МТУСИ

ФУМО ВО ИБ

ТЕОРИЯ И ПРАКТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сборник научных трудов
по материалам всероссийской
научно-практической конференции

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики» (МТУСИ)

Федеральное учебно-методическое объединение в системе высшего образования по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» (ФУМО ВО ИБ)

2 ноября 2022 г.

II ВСЕРОССИЙСКАЯ НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

ТЕОРИЯ И ПРАКТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СБОРНИК ТРУДОВ

Москва - 2022

УДК 004.056(82)
ББК 16.8я43
В74

Организационный коммитет

1. Леохин Ю.Л., д.т.н., профессор, проректор по научной работе МТУСИ – председатель;
2. Белов Е.Б., заместитель председателя ФУМО ВО ИБ – заместитель председателя;
3. Шелухин О.И., д.т.н., профессор, заведующий кафедрой «Информационная безопасность» МТУСИ;
4. Кубанков А.Н., д.в.н., профессор, заведующий кафедрой «Безопасность телекоммуникаций» МТУСИ;
5. Лось В.П., д.в.н., профессор, президент МОО «Ассоциация защиты информации»;
6. Новиков С.Н., д.т.н., доцент, заведующий кафедрой «Безопасность и управление в телекоммуникациях» СибГУТИ;
7. Крылов Г.О., д.ф.-м.н., профессор кафедры «Безопасность телекоммуникаций» МТУСИ;
8. Панков К.Н., к.ф.-м.н., врио заведующего кафедрой «Теория вероятностей и прикладная математика» МТУСИ;
9. Киреева Н.В., к.т.н., доцент, декан факультета «Телекоммуникации и радиотехника» ПГУТИ;
10. Красов А.В., к.т.н., доцент, заведующий кафедрой «Защищенные системы связи» СПбГУТ;
11. Безумнов Д.Н., начальник ОРОП МТУСИ – секретарь.

ISBN 978-5-905376-24-5

9 785905 376245

УДК 004.056(82)
ББК 16.8я43
В74

Оглавление

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

ТЕХНИКИ ЗАКРЕПЛЕНИЯ В ОС WINDOWS 5

НАУЧНАЯ СЕКЦИЯ «КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ И СЕТЕВАЯ БЕЗОПАСНОСТЬ»

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ СТЕГАНОГРАФИИ В ЗВУКЕ 14

МЕТОД АНАЛИЗА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 22

МЕХАНИЗМЫ ИСКУССТВЕННОЙ ИММУНИЗАЦИИ 30

ДЛЯ РЕШЕНИЯ ЗАДАЧ КИБЕРБЕЗОПАСНОСТИ 30

ПРИМЕНЕНИЕ ОБРАТНОГО СИМВОЛЬНОГО ВЫПОЛНЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ ОШИБОК В ИСПОЛНЯЕМОМ БИНАРНОМ КОДЕ 39

НАУЧНАЯ СЕКЦИЯ «ОРГАНИЗАЦИОННО-ПРАВОВЫЕ И ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ»

ПЕРСОНАЛЬНЫЕ ДАННЫЕ: ЗАЩИЩЕНЫ ИЛИ НЕТ? 49

ПРИМЕНЕНИЕ МОДЕЛЕЙ ЗРЕЛОСТИ ПРИ ОЦЕНКЕ ЭФФЕКТИВНОСТИ ПРОЦЕССОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 57

ЗАЩИТА ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ 67

ИДЕНТИФИКАЦИЯ ЛИЧНОСТИ ПО РАДУЖНОЙ ОБОЛОЧКЕ ГЛАЗА С ИСПОЛЬЗОВАНИЕМ МЕТОДА ЛОКАЛЬНЫХ БИНАРНЫХ ШАБЛОНОВ 75

«СОВЕРШЕНСТВОВАНИЕ СПОСОБОВ ОБНАРУЖЕНИЯ И ЗАЩИТЫ ОНЛАЙН АТАК НА КОМПЬЮТЕРНУЮ СЕТЬ» 83

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЛИЧНОСТИ: ЗАЩИТА ДАННЫХ ЦИФРОВОГО ПРОФИЛЯ И ЦИФРОВОЙ РЕПУТАЦИИ 89

ТРЕБОВАНИЯ К ЗАЩИТЕ ПРИЛОЖЕНИЙ, ОСНОВАННЫХ НА ТЕХНОЛОГИИ КОНТЕЙНЕРИЗАЦИИ 96

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ИЗМЕНЕНИЯ В ПРОЦЕССАХ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В СВЯЗИ С ИЗМЕНЕНИЯМИ ЗАКОНОДАТЕЛЬСТВА, ВСТУПАЮЩИМИ В СИЛУ С 1 СЕНТЯБРЯ 2022 ГОДА 105

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В РЕШЕНИЯХ ПО ЗАЩИТЕ ИНФОРМАЦИИ ПРЕДПРИЯТИЯ И ОБЕСПЕЧЕНИЮ ЕГО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 114

НАУЧНАЯ СЕКЦИЯ «ПРОБЛЕМЫ ЦИФРОВОГО СУВЕРЕНИТЕТА И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ»

ОРГАНИЗАЦИЯ ЗАЩИЩЕННОЙ ВИДЕОКОНФЕРЕНЦСВЯЗИ С ИСПОЛЬЗОВАНИЕМ КВАНТОВОГО КАНАЛА СВЯЗИ 125

ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ ТЕСТИРОВАНИЯ WEB-ПРИЛОЖЕНИЙ НА УЯЗВИМОСТИ 133

ПРОБЛЕМА НЕКОРРЕКТНОЙ ВАЛИДАЦИИ СЕРТИФИКАТОВ (IMPROPER CERTIFICATE VALIDATION) ПРИ УСТАНОВЛЕНИИ ДОВЕРЕННЫХ СОЕДИНЕНИЙ 139

ПОДГОТОВКА СОТРУДНИКОВ ДЛЯ МОНИТОРИНГА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОТИ 146

ПОМЕХОЗАЩИЩЕННОСТЬ И УЯЗВИМОСТЬ ПРОВОДА ВИТОЙ ПАРЫ КАК СРЕДЫ РАСПРОСТРАНЕНИЯ СИГНАЛА НА ФИЗИЧЕСКОМ УРОВНЕ МОДЕЛИ OSI 156

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ С МОРСКОГО СУДНА НА БЕРЕГ В УСЛОВИЯХ ОГРАНИЧЕННОГО КАНАЛА СВЯЗИ 170

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДИК ТЕСТИРОВАНИЯ БЕЗОПАСНОСТИ ПРОЕКТОВ 176

НАУЧНАЯ СЕКЦИЯ «КИБЕРБЕЗОПАСНОСТЬ»

ПРОБЛЕМЫ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА 186

РАЗРАБОТКА МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ПОПЫТОК КИБЕРАТАК НА СЕРВЕРЫ БАЗ ДАННЫХ 194

ИСПОЛЬЗОВАНИЕ СЕТЕВОЙ СТЕГАНОГРАФИИ В СЕТЯХ NGN 199

ВИДЫ КИБЕРУГРОЗ В СУДОВОЖДЕНИИ 206

СРАВНЕНИЕ ВОЗМОЖНОСТЕЙ НЕЙРОННОЙ СЕТИ И СИСТЕМЫ ПРЕДТВРАЩЕНИЯ ВТОРЖЕНИЙ ПРИ ОБНАРУЖЕНИИ СЕТЕВОЙ СТЕГАНОГРАФИИ В ПРОТОКОЛЕ TCP 213

ПРОГНОЗИРОВАНИЕ ПРОФИЛЯ ФУНКЦИОНИРОВАНИЯ КОМПЬЮТЕРНОЙ СИСТЕМЫ С ПРИМЕНЕНИЕМ АППАРАТА ТОЧЕЧНО-МНОЖЕСТВЕННЫХ ОТОБРАЖЕНИЙ 222

ШИФРАТОРЫ, ДЕШИФРАТОРЫ И ИХ ЗНАЧЕНИЕ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 232

ИССЛЕДОВАНИЯ РАЗВИТИЯ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ В РАМКАХ КОНЦЕПЦИИ РАЗВИТИЯ ЧЕТВЕРТОЙ ПРОМЫШЛЕННОЙ РЕВОЛЮЦИИ «ИНДУСТРИЯ 4.0» 238

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

Кравец В.В.
Акционерное общество «Перспективный мониторинг»,
Начальник отдела,
Vasily.Kravets@amonitoring.ru
Иванов О.А.
Акционерное общество «Перспективный мониторинг»,
Руководитель направления
Oleg.Ivanov@amonitoring.ru
Морин А.А.
Акционерное общество «Перспективный мониторинг»,
Специалист
Aleksey.Morin@amonitoring.ru

ТЕХНИКИ ЗАКРЕПЛЕНИЯ В ОС WINDOWS

Аннотация: При проведении работ по пентесту, анализу уязвимостей и аудиту информационной безопасности часто возникают ситуации, когда в ходе выполнения работ был получен доступ к некоторому объекту, который может и не иметь самостоятельной ценности в рамках исследования, но может быть хорошей точкой, с которой будут проводиться дальнейшие исследования. Для таких точек особенно важно иметь возможность обеспечить обратную связь, транспорт для исследователей. Набор действий, который предназначен для сохранения доступа к этой системе, для поддержки и помощи в обеспечении связи, называют «закреплением» (английский термин: «persistence»). Необходимо подчеркнуть, что данные техники не касаются транспорта как такового, а только обеспечивают работу любого вида транспорта. Программное обеспечение для транспорта,

например, reverse shell, рассматривается как полезная нагрузка. В данной статье рассматриваются техники закрепления на машине под управлением ОС Windows.

Типовые ситуации закрепления

Типовыми ситуациями для необходимости закрепления можно рассмотреть такие ситуации:

1) В рамках проведения работ по пентесту была обнаружена уязвимость, которая привела к исполнению кода внутри периметра. Уязвимость может быть оперативно закрыта вместе с установленным подключением, а рабочее место, где был исполнен код, перезагружено – все выполненные действия приведут к тому, что работа исследователя будет прерваны и для продолжения работ необходимо было закрепиться на системе.

2) Возможное однократное исполнение специально подготовленного ПО на объекте исследования – как в результате фишинговых действий или, например, социальной инженерии. В таком случае необходимо воспользоваться возможностью, чтобы вместо однократного действия иметь возможность выполнять серии команд в удобное время.

3) Ситуация, близкая к предыдущей, но которую стоит отдельно рассматривать: запуск кода с повышенными правами в рамках одного рабочего места. Например, к пользователю без прав администратора приходит работник службы IT-поддержки и запускает какое-то действие с высокими правами для рабочей задачи.

Виды техник закрепления

Техники закрепления можно делить и сравнивать между собой по разным критериям, которые позволят выбрать наиболее подходящий для тех условий, что есть у исследователя. Рассмотрим основные классификации, которые стоит учитывать.

1. По расположению полезной нагрузки

Полезная нагрузка закрепления может располагаться в оперативной памяти, в файлах на диске и в реестре. При расположении в ОЗУ, полезную нагрузку сложнее обнаружить, но такие методы могут не пережить перезагрузку ОС. Файлы же наоборот – при корректных настройках независимы от перезагрузок, но и их легче обнаружить и обезвредить. При расположении в реестре, действует много ограничений – туда нельзя поместить полную полезную нагрузку, а только какие-то начальные операции, но и найти все места в реестре обычно непросто.

2. По сложности обнаружения

Поиск и обезвреживание артефактов от техник закрепления может происходить и в ручном режиме, и в автоматическом. Противодействие ручному анализу обычно проходив в двух вариантах: использование слабоизученных мест, куда человек не сможет посмотреть, и использование техник, которые маскируют полезную нагрузку под легальные ПО.

В автоматизированном варианте чаще всего необходимо защититься от утилиты SysInternals Autoruns, которая может выдать один из трех вариантов: утилита не видит автозагрузку, утилита показывает запуск полезной нагрузки и утилита показывает запуск полезной нагрузки только в режиме усиленного поиска.

3. По специальным условиям активации

Некоторые методы закрепления требуют специальных действий от пользователя. Спектр действий может быть широким: от простого включения или перезагрузки компьютера, до более экзотических, типа запуска ПО, поддерживающего криптографию или запуск .net приложений. Некоторые из таких условий работаю по сути автоматически, поскольку, например, сейчас почти любое приложение поддерживает работу с криптографией в том или ином смысле.

4. По условиям использования

Не все методы доступны одинаково для любых систем. На доступность техник может оказывать влияние разрядность ОС, версия и редакция ОС, установленное ПО. Чем меньше условий накладывает метод, тем он проще в использовании. Но, с другой стороны, чем более «узкоспециализированный» метод, тем сложнее его обнаружить.

Дополнительно стоит рассмотреть вопрос, связанный с обнаружением persistence методик. Выше упоминалось, что часто используется обфускация. В качестве примеров можно привести использование параметра –e (-enc или -EncodedCommand) для powershell. Например, так: *powershell –e QzpcdGVzdC5wczEK*. Или использование мусорных символов для командной оболочки cmd, таких как ^, *“;* (циркумфлекс, запятая, двойная кавычка, точка с запятой) – такие символы будут игнорироваться при исполнении. Использование переменных окружения еще один действенный метод составления строк и запутывания исполнения. Помимо техник обфускации, стоит обратить внимание и на использование LOLBAS (Living Off The Land Binaries, Scripts and Libraries). LOLBAS – это список из большого количества программ и библиотек, которые позволяют выполнить особые действия, такие как чтение, запись и исполнение файлов, при этом эти файлы широко распространены и входят, например, в состав типовой ОС Windows. Один из примеров будет разобран ниже по тексту.

Рассмотрим некоторые из классических примеров методик обеспечения закрепления.

1. Автозагрузка (реестр)

Одно из самых частых местоположений для закрепления – разделы в реестре, отвечающие за автозагрузку при входе в ОС. Для пользователей это будет ветка в пользовательском разделе:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run Once

Общесистемные:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

Такие настройки легко переживают перезагрузку, старт обеспечивается операционной системой, легко обнаруживаются и в ручном, и в автоматическом режиме, не требуют специальных условий активации. Из плюсов можно отметить тот факт, что бум вирусов, использующих эти ветки, уже давно прошел, а, значит, все реже записи в этих ветках вызывают подозрения. Но из минусов – такие настройки весьма капризны к режимам работы: ветки *RunOnce* запускаются не всегда, а в некоторых ситуациях игнорируются и системные записи.

2. Автозагрузка (файлы)

Помимо реестра, автозагрузка для пользователей осуществляется из папок, например, *:\Users\%username%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup* или *C:\ProgramData\Microsoft\Windows\Start Menu\Programs* (тут обычно лежат ярлыки на программы, которым нужна автозагрузка).

Свойства этого метода, по сути, повторяют свойства предыдущего пункта.

3. Сервисы

Системные сервисы – очень удобный способ не только закрепиться в системе, но и действовать при этом с максимальными правами в ОС. Из плюсов: переживает перезагрузку, имеет ряд возможностей для обфускации запускаемой нагрузки, пользователь без прав администратора не сможет отключить сервис. Минусы: очень «шумная» технология – список сервисов довольно легко проверяется и человеком, и утилитами.

4. Интересные разделы реестра

В реестре хранится большое количество системных настроек, связанных с автоматическим запуском ПО или загрузкой dll. Например, в ветке *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs* расположен список dll, которые будут загружаться практически к каждому запускаемому приложению. Ветка *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\<имя файла>\Debugger* позволяет задать программу, которая будет запускать вместо указанной в имени файла. В ветке *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID* можно задать dll для работы с криптографией. По свойствам здесь все примерно стандартное – переживает перезагрузку, легко обнаруживается, работает почти везде, но есть разные специфичные условия для работы, которые по факту почти всегда выполняются.

Вышеперечисленные методы широко известны, поэтому применяются не так часто. Теперь можно рассмотреть некоторые современные методы.

1. COM hijacking

В реестре Windows в специальном разделе HKEY_CURRNET_USER\Software\Classes\CLSID\ хранится большое количество настроек связанных с загрузкой COM-объектов. Некоторые из них в своих настройках содержат возможность указать загружаемую dll. Такой метод хорошо переживает перезагрузку, почти не требует ничего специального для активации. Его очень сложно обнаружить как утилитами, так и вручную – только очень долгое и внимательное изучение работы ПО может выдать наличие закрепления.

2. scrobj.dll

Среди списка LOLBAS есть утилита *regsvr*, которая позволяет вызывать различные библиотеки, например, легитимную *scrobj.dll* (от

Microsoft с подписью). Можно передать дополнительные параметры, среди которых будет скрипт на специальном языке, который даже не обязательно должен быть расположен локально. Пример: *regsvr /s /n /u /i:http://evil.com/script.sct scrobj.dll*. Такой метод может расположен как в реестре, так и в файловой системе, его сложно обнаружить поскольку и regsvr и scrobj.dll являются легитимными файлами от Microsoft и не имеет особых условий по активации или использованию.

3. Профилировщик .net

Если в переменных среду установить две переменные: COR_ENABLE_PROFILING в 1, а COR_PROFILER в строковое значения заведомосозданного CLSID с библиотекой, то эта библиотека будет загружена во все стартующие .net приложения. Хоть это условие активации и ограничивает применимость метода, но в реальных условиях встречается очень часто и по факту скорее всего выполнятся всегда.

В завершении стоит упомянуть и несколько несерьезных и теоретических методов, которые тем не менее, имеют право на существование.

1. Горячие клавиши

У ярлыков на рабочем столе есть особая возможность – можно задать комбинацию клавиш, которая запустит ПО. Можно поменять (или создать новый) ярлык, убрать его подальше и назначить ему какую-то частую комбинацию. Данный метод сложно оценить с точки зрения обнаружения: его одновременно и сложно найти (вручную такое никто не проверяет, а утилиты редко собирают такую информацию) и легко – он же лежит прямо на рабочем столе. С условиями активации тоже все сложно – вовсе не факт, что выбранная комбинация клавиш будет наживаться пользователем.

2. edgegdi.dll

Специально или нет, но несколько лет назад почти все приложения в ОС Windows, использующие графический интерфейс, пытались загрузить

библиотеку edgegdi.dll из системной папки (*C:\Windows\system32* или *C:\Windows\SysWOW64*). Но в этих файлах не было такого файла и при наличии прав его можно было легко создать. Единственная серьезная сложность с этим методом – эта dll пытается загрузиться в том числе и в защищенные системные процессы, что при типовых настройках приводит к синему экрану смерти.

Заключение

В статье были рассмотрены различные способы и методы закрепления в ОС Windows, рассмотрены и приведены примеры классификации технологий закрепления ОС Windows. Стоит отметить, что знание таких методов может помочь одновременно и исследователям в их работе, и специалистам по реагированию на инциденты в защите.

СПИСОК ЛИТЕРАТУРЫ

3. Общие уязвимости и риски [Электронный ресурс]: - CVE 2018 г.
4. Башлы П.Н., Баранова Е.К. Информационная безопасность: учебно-практическое пособие.
5. Барсуков В.В., Водолазкий В.В. Современные технологии безопасности. Интегральный подход. - М .: Нолидж, 2015.
6. Андрианов В.В., Зефиров С.Л., Голованов В.Б., Колдуев Н.А. Обеспече-информационная безопасность бизнеса / 2-е издание перераб. и доп. - М .: Альпина Паблишерз, 2014.
7. Репин Д.С. Разработка алгоритмов и безопасности обнаружения и предотвращения угроз информации, повторного отказа в обслуживании с.48 2017г
8. Амрит Т. Уильямс, Марк Николетт, Повысьте ИТ-безопасность с помощью управления уязвимостями.

НАУЧНАЯ СЕКЦИЯ

«КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ И АНАЛИЗ СЕТЕВОГО ТРАФИКА»

Руководитель: **Панков Константин Николаевич**,
Московский технический университет связи и информатики,
врио заведующего кафедрой «Теория вероятностей и прикладная математика»
кандидат физико-математических наук

Караулова О.А.
ФГБОУ ВО ПГУТИ, старший преподаватель кафедры Информационной безопасности,
olya4369@yandex.ru
Шакурский М.В.
ФГБОУ ВО СамГТУ, доцент кафедры Теоретическая и общая электротехника
ФБОУ ВО ПГУТИ, доцент кафедры Информационной безопасности
к.т.н., доцент,
m.shakurskiy@gmail.com

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ СТЕГАНОГРАФИИ В ЗВУКЕ

В настоящее время проблема надежной защиты от несанкционированного доступа (НСД) остается одной из не решенных до конца проблем. Причины и способы сокрытия секретных сообщений известны с древних времен. Всем этим занимается стеганография. Стеганография – это способ хранения и передачи информации с учетом сохранения в тайне самого факта передачи.

Стеганография существует достаточно давно. Понятие «стеганография» с греческого означает «тайнопись», которая включает в себя большое разнообразие средств тайной связи, таких как невидимые чернила, микроизображения, секретные каналы и т. д. Стеганография занимает свое место в безопасности: она не заменяет шифрование, а дополняет его. Сокрытие сообщения с помощью стеганографии значительно снижает возможность обнаружения факта отправки самого сообщения [1]. А если это сообщение еще и зашифровано, оно будет иметь один дополнительный уровень защиты. Обобщенная модель стегосистемы представлена на (Рис. 1).

Достижения в области компьютерных технологий дали новый толчок стеганографии, в результате чего появилось новое направление – компьютерная стеганография (КС).

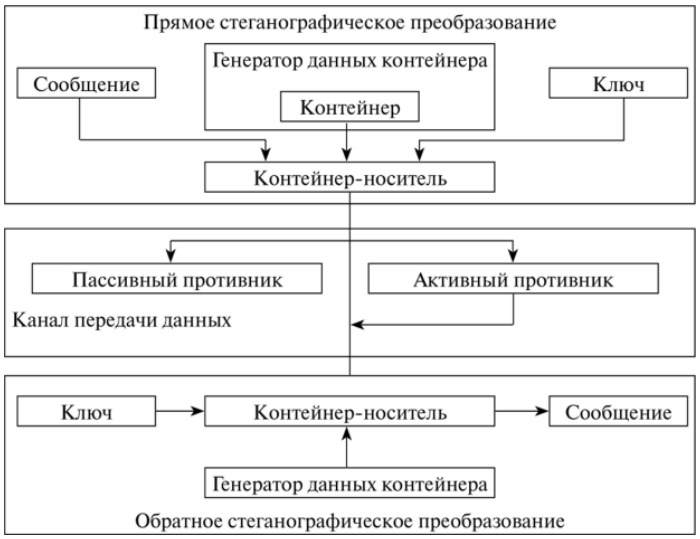


Рис. 1. Обобщенная модель стегосистемы

Развитие глобальных компьютерных сетей и мультимедиа технологий позволило разработать новые методы стеганографии, которые предназначены для защиты передаваемых данных по открытым каналам связи [2, 3]. Эти методы позволяют скрывать сообщения в компьютерных файлах (контейнерах) и данных, передаваемых в реальном времени. Стеганографический алгоритм использует информационную избыточность в передаваемых аудио- и видеоданных, а также не используемые зарезервированные поля файлов.

Наибольшее распространение стеганография получила в графических изображениях, в частности в формате JPEG. Однако сокрытие данных в аудиосигналах на сегодняшний день является актуальным в связи с широким распространением программ видеосвязи (Viber, Skype, WhatsApp, Telegram, Zoom).

На сегодняшний день распространение получили следующие форматы аудиофайлов:

– формат без сжатия (WAVE, AIFF);

– формат со сжатие без потерь (FLAC, APE, TTA, TTE, LA, ALAC и другие);

– формат со сжатием с потерями (MP3, AAC, AAC+, WMA и другие).

Помимо этого, существуют форматы для передачи звука в реальном времени (кодеки): SILC, Opus и другие.

Простейшим и наиболее часто используемым аудиоформатом является WAVE, структура файла которого приведена на (Рис. 2). Он нужен для хранения несжатой цифровой аудиоинформации.

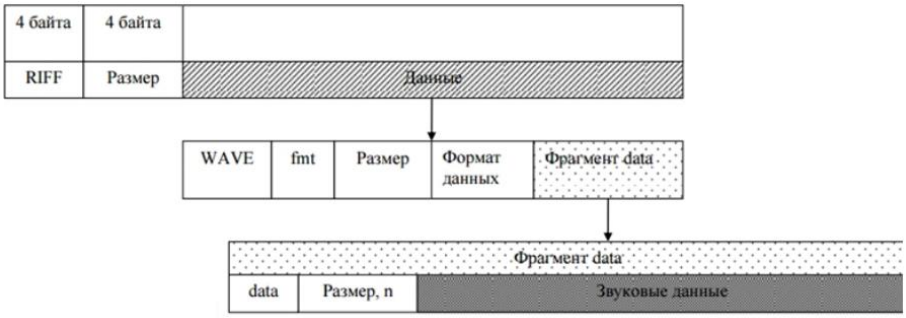


Рис. 2. Структура WAVE файла

Выбор формата основан на его избыточности и позволяет анализировать его с помощью метода замены младших значащих бит (LSB–метод). Аудиофайлы WAVE представляют собой несжатые данные, которые получены из аналого-цифровых преобразователей.

LSB–метод позволяет эффективно встраивать срытую информацию. Однако при встраивании в реальном времени невозможно заранее проанализировать весь аудиопоток [4].

Рассмотрим реализацию LSB – метода для формата WAVE в среде Python.

Для начала необходимо для заданного файла WAVE присвоить частоту дискретизации (samplerate) и данные файла (cover), после чего его необходимо его прочитать. После чего в заданном диапазоне данных файла строим каналы (0 – левый канал, 1 – правый канал) (Рис. 3).

```
from scipy.io import wavfile
samplerate, Cover = wavfile.read('./samples/cover1.wav')
plt.plot(range(-32766,32767,1),Cover[range(-32766,32767,1),0])
plt.plot(range(-32766,32767,1),Cover[range(-32766,32767,1),1])
plt.grid(color='black')
plt.savefig('./graphics/CoverSignal.pdf')
```

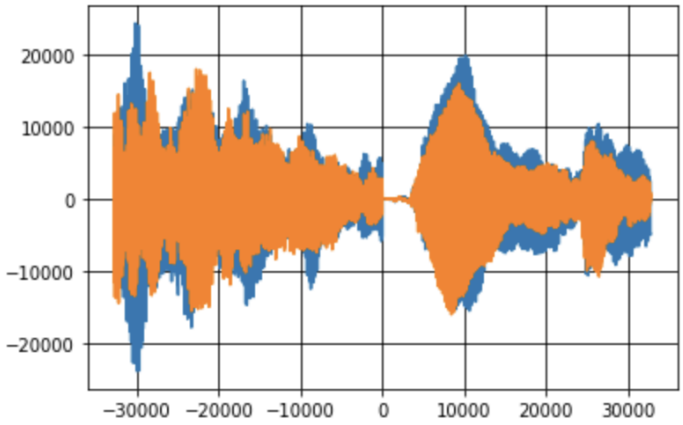


Рис. 3. Графическое представление данных в каналах

Следующим шагом идет формирование матриц левого и правого каналов с выделением знака. Для этого необходимо определить длину cover, чтобы понять сколько всего отсчетов всего. Далее необходимо сформировать пустые массивы данных конкретной длины. Это необходимо для формирования каждого отсчета. В Cover1 записываются значения по модулю, а Cover1Sign записывается знак. После чего организуется цикл длиной n для каждого канала (Рис. 4).

```
n=len(Cover)
Cover1=np.empty([n],dtype=int)
Cover1Sign=np.empty([n],dtype=int)
Cover2=np.empty([n],dtype=int)
Cover2Sign=np.empty([n],dtype=int)
for i in range(n):
    Cover1[i]=np.abs(Cover[i,0])
    if Cover[i,0]>=0:
        Cover1Sign[i]=1
    else:
        Cover1Sign[i]=-1

    Cover2[i]=np.abs(Cover[i,1])
    if Cover[i,1]>=0:
        Cover2Sign[i]=1
    else:
        Cover2Sign[i]=-1
```

Рис. 4. Формирование матриц левого и правого каналов с выделением знака

После необходимо разбить контейнер на слои с помощью следующего кода, так как в отсчете всего 16 бит, один бит уходит на знак, поэтому

остается 15 слоев. Далее формируется матрица, которая имеет массив прямоугольного типа (Рис. 5).

```
C1=np.empty([n,16],dtype=int)
C2=np.empty([n,16],dtype=int)
temp1=0;temp2=0

for i in range(n):
    for k in range(16):
        if Cover1[i]-temp1>=2**(15-k):
            C1[i,k]=1
        else:
            C1[i,k]=0

        if Cover2[i]-temp2>=2**(15-k):
            C2[i,k]=1
        else:
            C2[i,k]=0

        temp1=temp1+C1[i,k]*2**(15-k)
        temp2=temp2+C2[i,k]*2**(15-k)
    temp1=0; temp2=0
```

Рис. 5. Разбиение контейнера на слои

После этого сформируем сообщения messageL и messageR, чтобы встроить массив данных и применяем классический LSB – метод. Разбивая на слои файл, встраиваем данные по этому методу, записывая в младший битный слой скрытую информацию и далее собираем слои вместе, записывая их в файл StegoLSB (Рис. 6).

```
C1LSB=C1
C2LSB=C2
for i in range(n):
    C1LSB[i,15]=MessageL[i]
    C2LSB[i,15]=MessageR[i]
```

```
#Сборка слоёв
Cover1LSB=np.zeros([n],dtype=int)
Cover2LSB=np.zeros([n],dtype=int)
StegoLSB=np.zeros([n,2],dtype=int)
for i in range(n):
    for k in range(16):
        Cover1LSB[i]=Cover1LSB[i]+C1LSB[i,k]*(2**(15-k))
        Cover2LSB[i]=Cover2LSB[i]+C2LSB[i,k]*(2**(15-k))
    Cover1LSB[i]=Cover1LSB[i]*Cover1Sign[i]
    Cover2LSB[i]=Cover2LSB[i]*Cover2Sign[i]
    StegoLSB[i,0]=Cover1LSB[i]
    StegoLSB[i,1]=Cover2LSB[i]
```

Рис. 6. Сбор слоев с использованием LSB – метода

После выполнения всех этих шагов записываем файл со скрытой информацией. Необходимо открыть файл и прочитать всю информацию,

которая записана в нем, после чего разбиваем его на слои и извлекаем младший битный слой. Эта процедура необходима для вычисления ошибки извлечения. Данная ошибка позволяет сравнить в каналах сообщение до кодирования и сообщение после извлечения ошибки. Если в результате они равны между собой, то ошибка равна нулю.

В Python можно провести статистический анализ контейнеров с распределением значений (Рис. 7 – 9). По полученным гистограммам видно, что нулевых значений больше всего, а с увеличением амплитуды значений становится меньше.

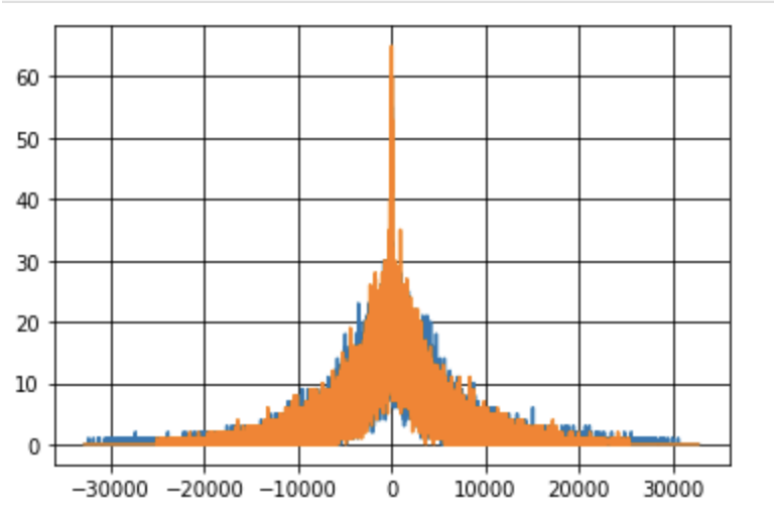


Рис. 7. Гистограмма распределения значений контейнера

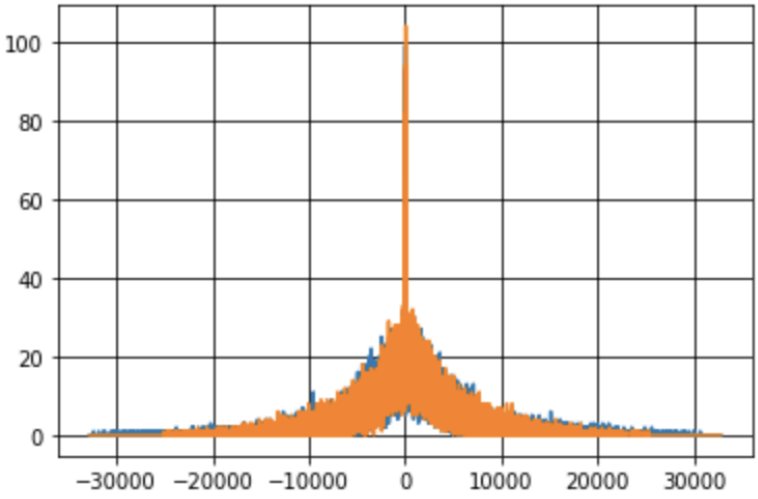


Рис.8. Гистограмма заполненного контейнера

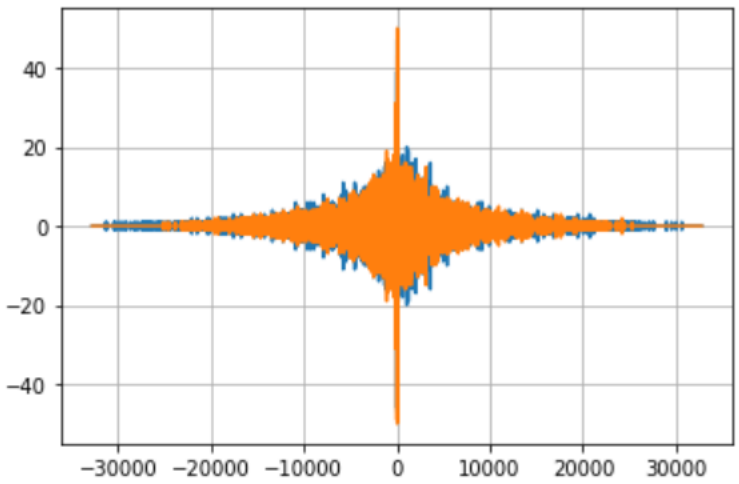


Рис. 9. Разность гистограмм пустого и заполненного контейнеров

Таким образом, проведено моделирование стеганографической системы на основе метода наименьших значащих бит в среде Python. При этом открытым является вопрос оценки качества маскировки информации. В случае аудио системы, работающей в реальном времени, использование известных стегоаналитических методов ограниченно их фактическим отсутствием. Поэтому остаётся статистический анализ. В качестве статистического показателя удобно использовать анализ распределения в сравнении с распределением покрывающего объекта на основе корреляции. Для этой цели выбран коэффициент корреляции Пирсона, вести оценку по которому удобно, так как он ограничен диапазоном единицы. Помимо этого он широко используется и включён в стандартный функционал всех математических программ. Для предлагаемой системы коэффициент корреляции определяется встроенной функцией (рис. 10).

Разработка данной модели позволяет проводить исследование формата WAVE для различных алгоритмов встраивания сообщений и осуществлять их статистическое сравнение, как на отдельных участках встраивания, так и для всего файла.

```
CorPL=np.corrcoef(CoverLH[0],StegoLH[0])
CorPR=np.corrcoef(CoverRH[0],StegoRH[0])
print(CorPL[1,0])
print(CorPR[1,0])

✓ 0.4s
```

```
0.8737441399147382
0.8903803551375169
```

Рис. 10. Коэффициент корреляции Пирсона

Помимо этого, модель позволяет исследовать статистические распределения самих покрывающих объектов, как существующих в общем доступе, так и записанных с реальных микрофонов, встроенных и внешних, для получения базы для исследования данного формата.

СПИСОК ЛИТЕРАТУРЫ

1. Википедия – свободная энциклопедия [Электронный ресурс]. - https://ru.wikipedia.org/ – (дата обращения: 17.09.2022).

2. Конахович, Г.Ф. Компьютерная стеганография. Теория и практика/ Г.Ф. Конахович, А.Ю. Пузыренко // - К.: «МК-пресс», 2006 – 288 с.

3. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев // - М.: Солон-Пресс, 2009 – 272 с.

4. Садов, В.С. Компьютерная стеганография (Конспект лекций) / В.С. Садов // Минск: ВГУ, 2010 – 220 с.

5. Хеллман, Д. Стандартная библиотека Python 3. Справочник с примерами / Д. Хеллман // Вильямс, 2-е издание, 2018 – 1376 с.

6. Лутц, М. Изучаем Python. Авторский курс объектно-ориентированного программирования / М. Лутц // Диалектика, 5-е издание, 2019, 832 с.

Зефиров С.Л.
Зав. кафедрой, ФГБОУ ВО «Пензенский государственный университет»
к.т.н., доцент,
sergeizefirov@mail.ru
Аккуратнов А.Н.
аспирант, ФГБОУ ВО «Пензенский государственный университет»
akkalexnick@yandex.ru

МЕТОД АНАЛИЗА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Одним из компонентов современных систем мониторинга информационной безопасности является модуль корреляции событий, предназначенный для поиска общих значений атрибутов связи событий между собой. Корреляция событий используется в сигнатурных методах анализа, которые отражают накопленные знания о сценариях вторжений, атак, сбоях в правилах корреляции. Для получения знаний используются моделирование, поведенческий анализ, данные реальных атак и т.д. Зафиксированный набор событий в журнале событий изучается, нормализуется, определяется набор параметров для корреляции и реализуется в форме набора правил [1]. Правила анализа представляют собой описание последовательностей событий ИБ с условиями корреляции, а также условий, выполнение которых характеризует наличие инцидента информационной безопасности (ИБ). Фактически, правило корреляции описывает ситуацию, которую можно охарактеризовать, как «случилось что-то конкретное, что не должно было случиться». На рис. 1 показан пример правила сигнатурного анализа SIEM ArcSight ESM [2].

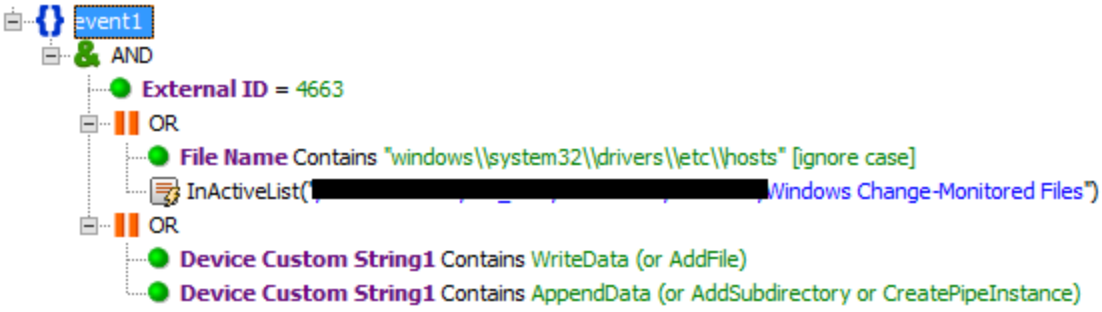


Рис. 1. Пример правила сигнатурного анализа из ArcSight ESM

Такой подход не позволяет выявлять инциденты ИБ, которые находятся вне области накопленных знаний.

Выявление таких инцидентов частично позволяет применение цифровых профилей. Цифровой профиль – это поведенческая модель, построенная на статистических закономерностях хронологических данных о количестве событий в единицу времени. Сигналом о возможном инциденте ИБ является превышение количества событий за текущую единицу времени определенных и установленных пороговых значений. Превышение пороговых значений, установленных в цифровом профиле, рассматривается как отклонение от найденных закономерностей при построении профиля. Для построения цифрового профиля не требуется предварительная нормализация, требуется только один параметр – время возникновения события. Этот метод позволяет выявлять инциденты автоматизированным способом, основываясь на закономерностях, найденных в исторических данных мониторинга и не используя базу знаний сигнатурного анализа. Но цифровой профиль не сработает, если инцидент ИБ характеризуется небольшим количеством событий, не превышающим пороговых значений.

Для выявления таких инцидентов автоматизированным способом предлагается объединить возможности сигнатурного анализа и цифровых профилей. Смысл применения такого подхода заключается в выявлении закономерностей или зависимостей появления нормализованных событий ИБ. В качестве исходных данных используются журналы событий. На

первом этапе закономерности устанавливаются по последовательности или порядку появления событий, а также по относительным (интервал времени между появлениями) временным параметрам событий. По найденным закономерностям создается модель данных (аналогичная эталонной модели цифрового профиля, но со своими характеристиками). На втором этапе проводится анализ на предмет выявления отклонений от характеристик модели. Предполагается, что возможные инциденты ИБ, а точнее последовательности событий их составляющих содержатся в перечне найденных отклонений.

На первом шаге реализации предлагаемого метода следует провести категоризацию событий [3], т.е. определить набор параметров, которые отвечают за соответствие события определенной категории. Каждая категория соответствует уникальному набору значений параметров события и составляет так называемый алфавит типов событий (A, B, C и т.д.).

На втором шаге осуществляется создание основы модели данных. Для этого весь журнал событий преобразовывается в последовательность типов событий вида, например, ABCEAEADE. Вся последовательность разбивается на пары по принципу (по номеру события) 1-2, 2-3, 3-4 и т.д. Из вышеуказанной последовательности рассмотрим пары событий AB, BC, CE и т.д. В качестве структуры данных выбрана структура данных ориентированного графа [4]. Пример визуализации модели показан на рис.2, где вершинами графа являются множество типов событий, а ребра графа указывают на наличие присутствия пары событий в исходных данных. Направления ребер указывают последовательность появления событий.

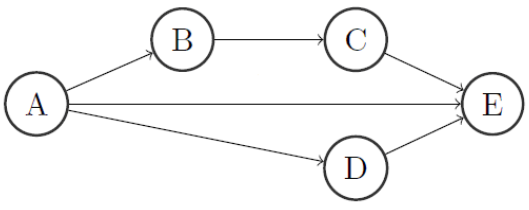


Рис 2. Пример визуализации модели.

На третьем шаге осуществляется подсчет количественных характеристик модели. Для каждой вершины определяется количество появлений события данного типа в исходном журнале. Для каждого ребра определяется количество появлений пар событий в исходной последовательности. На рис. 3 представлен пример модели с количественными характеристиками. Видно, что количество событий типа A составляет 10. Количество пар событий AB и AE по 3.

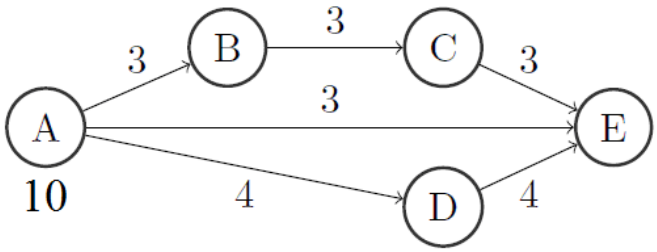


Рис 3. Пример визуализации модели с количественными характеристиками.

На четвертом шаге осуществляется расчет частот [5] появления пар событий относительно общего количества появления первого события из пары. Например, для событий A и B частота рассчитывается по формуле:

$$t_{AB} = \frac{N_{AB}}{N_A}, \quad (1)$$

где N_{AB} - количество пар событий AB, N_A - количество событий типа A.

Расчет частот производится для каждой пары (каждого ребра графа).

Результаты расчетов добавляются в данные ребер модели. На рис. 4 показан пример модели с частотными характеристиками.

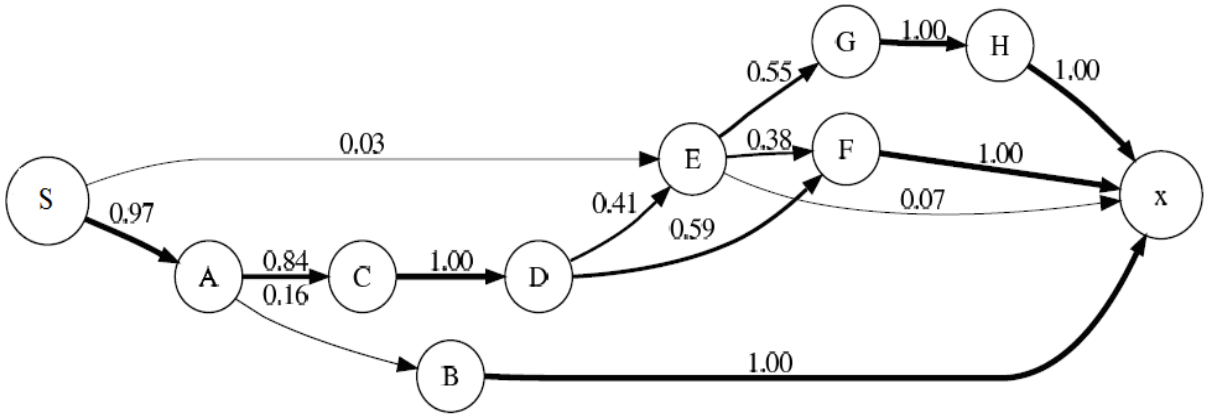


Рис 4. Пример визуализации модели с частотными характеристиками выходов из вершины предшествующего события.

Аналогичным способом вычисляются частоты появления пар событий относительно общего количества появления второго события из пары.

Кроме частотных характеристик предлагается использовать коэффициент зависимости событий, который вычисляется эвристическим методом технологии интеллектуального анализа процессов (ProcessMining)[6,7]. Описание эвристического метода приведено в [8]. Коэффициент отражает долю появления пары событий AB, относительно появления пары событий BA. Коэффициент для пары разнотипных событий вычисляется следующим образом:

$$a \Rightarrow w_b = \left(\frac{|a > w_b| - |b > w_a|}{|a > w_b| + |b > w_a| + 1} \right), \quad (2)$$

где $|a > w_b|$ - количество появлений пары событий *ab*, а $|b > w_a|$ - количество появлений пары событий *ba*.

Коэффициент для пары однотипных событий вычисляется так:

$$a \Rightarrow w_a = \left(\frac{|a > w_a|}{|a > w_a| + 1} \right), \quad (3)$$

где $|a > w_a|$ - количество повторений события *a*.

На рис.5 изображен пример модели с рассчитанным коэффициентом зависимости событий.

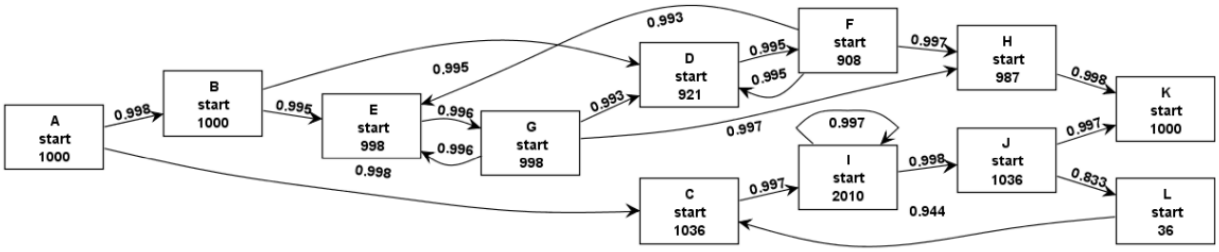


Рис 5. Пример модели с рассчитанным коэффициентом зависимости событий.

Пятым шагом является фильтрация модели. Фильтрация модели осуществляется установкой нижних пределов количества появлений событий, пар событий, частот и коэффициента зависимости событий. Пределы устанавливаются экспертным путем. Если частоты в ребре и коэффициент зависимости ниже установленных пределов, то ребро удаляется из графа. Вершины, у которых удалены все ребра также удаляются из графа модели. Например, на рис.5 таким ребром является ребро S-E (частота 0,03).

Шестым шагом является установление относительных временных зависимостей или закономерностей. Для этого вычисляются интервалы времени для каждой пары событий, полученных на шаге 2. Дальнейший анализ сводится к анализу числовых рядов [9]. Сначала числовой ряд анализируется на предмет выбросов. Способ обнаружения выбросов основан на межквартильном расстоянии [10]. Из числового ряда удаляются значения, не попадающие в диапазон:

$$\left[(x_{25} - 1{,}5(x_{75} - x_{25})), (x_{75} + 1{,}5(x_{75} - x_{25}))\right], \quad (4)$$

где x_{75} и x_{25} - значения третьего и первого квартиля соответственно.

Так для числового ряда 2,3,2,4,90,2,4,3 значение 90 будет удалено.

Из оставшихся значений выбирается минимальное и максимальное значение в качестве допустимого интервала между появлением пары событий и добавляется в модель.

В итоге модель представляет собой набор правил-закономерностей, характеризующих последовательность и временные зависимости появления событий. Самый простой пример такого правила: «после события A должно появиться событие B». Следующее правило для события B: «после появления событий B должно появиться событие C или D» и т.д. Применительно к временным характеристикам правило звучит как «после события A должно появиться событие B в течение 5 минут» и т.д.

Седьмым шагом является поиск отклонений от модели данных. Для этого исходную последовательность разбивают на пары событий, аналогично шага 2 предлагаемого метода. Далее проводится поиск в модели данных ребра графа, соединяющего вершины, составляющие пару событий. Если такое ребро отсутствует фиксируется отклонение несоответствия модели. Также используется счетчик текущего времени для выявления отсутствующих событий (не соответствующих интервалу). Выявленные отклонения изучаются экспертами на предмет наличия инцидентов ИБ.

Предлагаемый метод анализа событий ИБ позволяет построить модель для выявления инцидентов ИБ. Представление модели в виде графа позволяет компактно отобразить найденные закономерности независимо от размера исходного журнала событий. Поэтому модель можно использовать для получения знаний об изучаемой системе, что невозможно при визуальном анализе самого журнала. Также анализ модели позволяет выявлять и фильтровать спам-события, не имеющие ценности для анализа, что существенно снижает нагрузку на систему мониторинга. Построенную модель данных можно в дальнейшем использовать для выявления инцидентов ИБ в реальном времени. Причем для поиска отклонений как по появлению, так и отсутствию событий с использованием счетчика реального времени.

СПИСОК ЛИТЕРАТУРЫ

1. Олеся Шелестова. Корреляция SIEM. Сигнатурные методы //исследовательский центр Positive Research [Электронный ресурс] 2012 URL:http:// www.securitylab.ru/analytics/431459.php
2. ArcSight ESM. http://www.arcsight.com/products/products–esm/
3. Заводцев И.В. Разработка механизмов сбора и преобразования формата представления исходной информации для систем мониторинга событий информационной безопасности. / Заводцев И.В., Гайнов А.Е./ "Программные системы и вычислительные методы" – 2015 - №1 – стр.21-31
4. Харари Ф. Теория графов. — М.: УРСС, 2003. — 300 с. — ISBN 5-354-00301-6.
5. Р.Ш. Хуснутдинов. Теория вероятностей. Учебник. - Инфра-М, 2013 – 175 с. – ISBN 978-5-16-005312-7
6. W.M.P. van der Aalst, A.J.M.M. Weijters, and L. Maruster. Workflow Mining: Discovering Process Models from Event Logs. IEEE Transactions on Knowledge and Data Engineering, 16(9):1128–1142, 2004.
7. Wil van der Aalst: Process Mining. Data Science in Action. Second Edition. Springer-Verlag Berlin Heidelberg, 2016
8. A.J.M.M. Weijters and J.T.S. Ribeiro. Flexible Heuristics Miner (FHM). BETA Working Paper Series, WP 334, Eindhoven University of Technology, Eindhoven, 2010.
9. Майков Е.В. Математический анализ. Числовые ряды/Е.В. Майков. – 1999
10. Сальникова К.В. Анализ массива данных с помощью инструмента визуализации «ящик с усами» / «Математические и инструментальные методы экономики» - 2021г. - №6.

Павленко Е.Ю.
ФГАОУ ВО «СПбПУ»,
Институт кибербезопасности
и защиты информации,
доцент, к.т.н.,
pavlenko@ibks.spbstu.ru

МЕХАНИЗМЫ ИСКУССТВЕННОЙ ИММУНИЗАЦИИ ДЛЯ РЕШЕНИЯ ЗАДАЧ КИБЕРБЕЗОПАСНОСТИ

Исследование выполнено в рамках гранта Президента РФ для государственной поддержки молодых российских ученых - кандидатов наук МК-3861.2022.1.6.

Цифровизация технологической инфраструктуры реализуется высокими темпами, и ключевым препятствием для вывода всех отраслей деятельности на новый технический уровень является широкий спектр нерешенных задач кибербезопасности современных цифровых систем. Такие системы представляют собой конгломерат информационных систем, баз и хранилищ данных, систем обработки информации, SCADA-систем и так далее. Также они осуществляют взаимодействие с другими подобными системами и со средствами защиты. Для таких объектов характерна угроза реализации целенаправленных кибератак, поэтому актуальной задачей является создание подхода, обеспечивающего отражение соответствующих киберугроз и целенаправленных атак [1, 2]. Перечисленные объекты имеют гетерогенный состав компонентов. динамически изменяющийся функционал (в зависимости от совокупности внешних и внутренних факторов), отсутствие избыточности или взаимозаменяемости узлов, а также наличие

критических узлов, деструктивное воздействие на которые может привести к компрометации и краху всей системы.

Для решения проблем кибербезопасности предлагается подход, состоящий в применении иммунизации, направленной на защиту критических узлов цифровых систем путем разработки набора временно применяемых структур и функциональных узлов для снижения риска реализации атаки. Предлагаемая иммунизация направлена не на восстановление всех возможных функций системы, а на разработку мер, защищающих систему от заданного набора угроз и снижающих риск поражения критичных узлов от новых угроз. Направленность на заданный перечень атак является особенностью подхода и одновременно его достоинством, так как позволяет защитить критические узлы от сложных таргетированных атак, типичных для систем подобного вида.

Предлагаемый подход обладает новизной, поскольку анализ научно-технических источников [3-6] показал, что имеющиеся исследования сосредоточены лишь на противодействии компьютерным вирусам и не учитывают особенности киберугроз в сложных системах.

Ключевая идея иммунного подхода состоит в защите критических узлов и наращивании иммунитета. Иммунитет узла – это сложность (алгоритмическая, вычислительная, организационная) реализации злоумышленником атаки на него.

Основываясь на работах [7-9], предлагается использовать моделирование цифровой системы в виде ориентированного графа, где узлами являются компоненты системы, а ребра или направленные дуги отражают связи между ними, выражаемые как обменом данных, так и согласованностью работы (логическая взаимосвязь).

При реализации иммунного подхода необходимо определить, какие именно узлы должны в первую очередь подвергаться иммунизациа.

Поэтому ряд экспериментов был связан с проверкой того, насколько корректно система сможет реализовывать свою целевую функцию в условиях кибератак. Здесь использован подход, представленный в работах [7-10], в рамках которого целевая функция системы выражается в виде маршрута на графе, с последовательным или параллельным посещением вершин. При моделировании были рассмотрены графы со следующими параметрами: число узлов N = 50; вероятность появления связи между парой вершин p = 0.2, 0.5 (использовалась модель Эрдеша Реньи); длина функциональной последовательности (маршрута целевой функции) len = 5, 7.

На каждый граф было проведено два типа атак: последовательное удаление узлов и удаление связей. В таблицах 1, 2 представлены результаты экспериментов. В первых трех столбцах указаны параметры графа (число узлов, вероятность появления связи, длина маршрута). В столбцах (10%, 20% и т.д.) указано число маршрутов, которое осталось после удаления процента узлов/связей. В последнем столбце указано количество удаленных узлов/связей, после которого число маршрутов, которыми можно реализовать целевую функцию, стало равно 0.

Табл. 1. Атака путем удаления узлов

N	**P**	**Len**	**Число маршрутов**	**20%**	**50%**	**70%**	**100 %**
50	0.2	5	183	90	2	0	26
50	0.2	7	237	88	0	0	22
50	0.5	5	3535	1135	118	0	29
50	0.5	7	114705	28417	174	0	34
150	0.2	5	30742	8769	997	22	115

Табл. 2. Атака путем удаления ребер

N	**E**	**Len**	**Число маршрутов**	**20%**	**50%**	**70%**	**100 %**
50	0.2	5	183	81	24	6	248
50	0.2	7	237	42	0	0	116
50	0.5	5	3535	1130	99	21	492
50	0.5	7	114705	28754	1461	28	445
150	0.2	5	30742	13942	2141	268	1974

По результатам экспериментов можно сделать вывод о том, что удаление узлов, особенно критических, быстрее приводит к деградации системы и потере ей способности реализовывать свою целевую функцию разными способами (маршрутами), чем потеря связей. Это можно объяснить тем, что для многих цифровых систем характерна сильная связность между компонентами различного типа. Например, для цифровых систем, чья сетевая инфраструктура базируется на одноранговых сетях, такие атаки будут менее критичными, чем атаки на узлы, наиболее мощные с точки зрения приема и передачи сигнала.

Также была проведена серия экспериментов над графом, моделирующим поведение распределенной цифровой системы, направленная уже на оценку эффективности подхода иммунизации. Процесс функционирования системы описывается оказанием на нее двух типов воздействий: атакующего (характеризующего деструктивное влияние внешней среды) и восстанавливающего. Например, за один промежуток времени на систему может проводиться атака (моделируемая в виде удаления нескольких ребер), а также восстанавливающее воздействие (моделируемая в виде добавления нескольких ребер), которое, по сути, и является эволюцией и способностью системы приспосабливаться к внешним условиям среды.

Для формализации таких процессов введем понятие интенсивности атакующего и восстанавливающего воздействий. Рассмотрим простейший

пуассоновский поток. Сгенерируем последовательность случайных величин, подчиняющихся распределению Пуассона с интенсивностью, равной 2 (в момент времени происходит в среднем 2 события) (1.1):

$$\text{Poisson random variable} = [1,1,4,5,1,0,1,1,1,1] \quad (1.1)$$

Каждый i-ый элемент последовательности — это количество событий, которые произойдут в i-ый момент времени.

Например, есть атака, реализуемая в терминах графовой модели путем удаления ребер с постоянной интенсивностью, равной 2. Первый элемент последовательности Poisson random variable равен 1. Это означает, что в начальный момент времени произойдет удаление одного ребра.

Такой же подход можно применить и к моделированию восстанавливающего воздействия.

С точки зрения поведения системы и ее эволюционного процесса? интересно рассмотреть различные соотношения интенсивностей восстановительного и атакующего воздействий. В рамках текущего эксперимента предлагается рассматривать следующие соотношения:

1. Интенсивность восстановления в 2 раза меньше интенсивности атакующего воздействия.

2. Интенсивность восстановления равна интенсивности атакующего воздействия.

3. Интенсивность восстановления в 2 раза больше интенсивность атакующего воздействия.

Помимо интенсивности восстанавливающего и атакующего воздействия важен тип атаки. В рамках экспериментов рассматриваются следующие типы атак:

1. Атака отказа в обслуживании, моделируемая как удаление вершины графа. Восстанавливающее воздействие для такой атаки – добавление новой

вершины произвольного типа, а также произвольных ребер, количество которых равно степени удаленной вершины.

2. Атака нарушения коммуникации между компонентами системы, выражаемая как удаление ребра или дуги из графа. В результате этой атаки удаляется только ребро, вершины, которые инцидентны этому ребру, остаются. Восстанавливающее воздействие для такой атаки – добавление произвольного ребра.

3. Атака типа «человек посередине», Man-in-the-Middle. В терминах графа она выражается как подразбиение ребра. Восстанавливающее воздействие – добавление одной вершины произвольного типа и одного ребра.

Наибольший интерес представляет ситуация, когда интенсивность восстановления примерно равна интенсивности атаки, поскольку целью эффективной защиты от кибервоздействий является выработка не только эффективного по своим мерам, но и оперативного по степени генерации ответа на действия злоумышленника.

Рассмотрим результаты экспериментов, представленные в виде графиков поверхностей (Рис. 1 – 3).

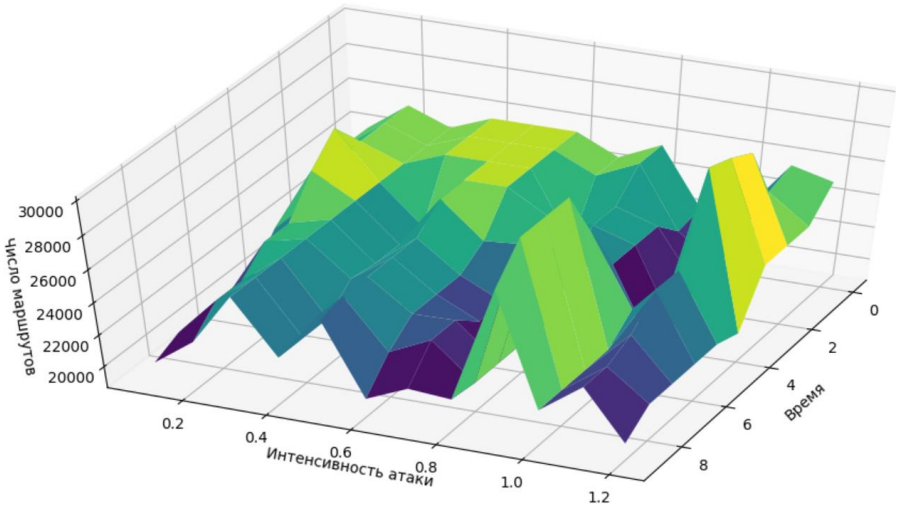


Рис. 1. Атака путем удаления вершины

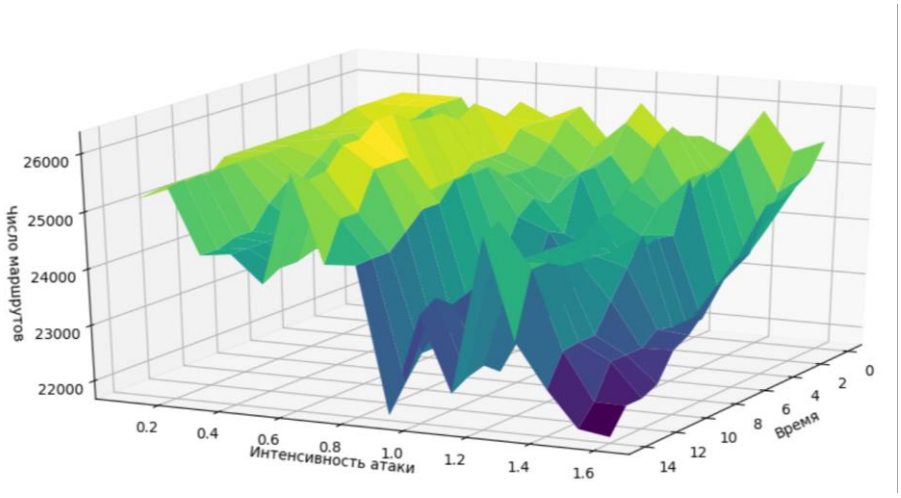


Рис. 2. Атака путем удаления ребра

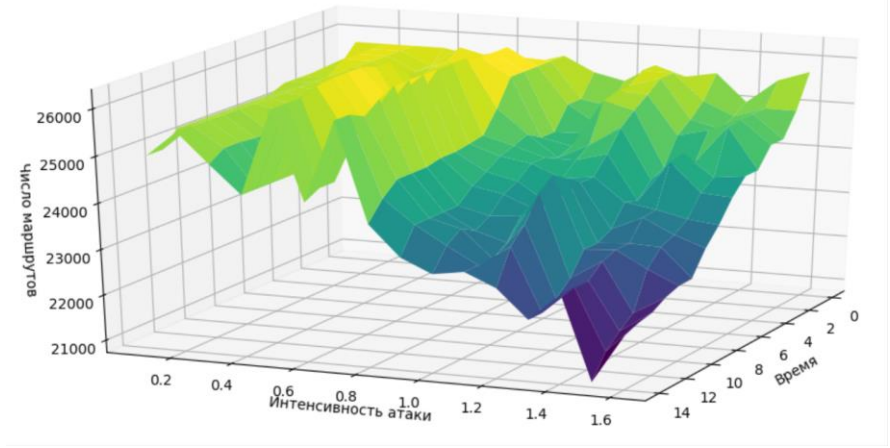


Рис. 3. Атака путем подразбиения ребра

По итогам экспериментальных результатов можно сделать следующие выводы: реализация атаки любого типа на систему приводила к достаточно заметной деградации системы, на гарфиках они выражены как «провалы» поверхностей. Однако применение иммунизации, в частности, спектра соответствующих восстанавливающих действий для каждой атаки, позволило с течением времени вернуть систему практически к начальному уровню работоспособности. Наименее критичной, судя по рисункам, оказалась атака отказа в обслуживании, связанная с удалением вершины из графа – для нее потребовалось меньше времени для восстановления системы, особенно это заметно в случаях малой интенсивности атак. При увеличении

интенсивности «провалы» становятся глубже, но тем не менее, применение иммунизации исправляет ситуацию.

Таким образом, представленный в данной работе иммуноподобный подход наиболее эффективен будет для атак, направленных на удаление узлов (вывод из строя компонентов системы). При этом, интеграция такого подхода на практике с распознаванием типа реализуемой кибератаки позволит в ходе иммунизации применить наиболее адекватный спектр ответных действий, реализующих наиболее эффективную иммунизацию системы и восстанавливающих ее исходный функционал.

СПИСОК ЛИТЕРАТУРЫ

1. Choraś, M. Cyber threats impacting critical infrastructures / M. Choraś, R. Kozik, A. Flizikowski, W. Hołubowicz, and R. Renk // In Managing the Complexity of Critical Infrastructures. Springer, Cham. – 2016. – Pp. 139-161.

2. Bécue, A. Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities / A. Bécue, I. Praça, and J. Gama // Artificial Intelligence Review. - 2021. – №54(5) – Pp.3849-3886.

3. Wang, C. On computer viral infection and the effect of immunization / C. Wang, J.C. Knight, M.C. Elder // In Proceedings 16th Annual Computer Security Applications Conference (ACSAC'00). – 2000. – Pp. 246-256.

4. Bahashwan, W.S. Modeling the Effect of External Computers and Removable Devices on a Computer Network with Heterogeneous Immunity / W.S. Bahashwan and S.M. Al-Tuwairqi // International Journal of Differential Equations. – 2021.

5. Cohen, R. Efficient immunization strategies for computer networks and populations / R. Cohen, S. Havlin, and D. Ben-Avraham // Physical review letters. – 2003. – №91(24). – P.247901.

6. Fagan, B. On the Immunization of Small Computer Networks / B. Fagan // [Электронный ресурс]. — Режим доступа :

https://www.siam.org/Portals/0/Publications/SIURO/Volume%2010/1.%20ON%20THE%20IMMUNIZATION%20OF%20SMALL%20COMPUTER%20NETWORKS.pdf?ver=2018-01-19-101500-827.

7. Зайцева, Е.А. Нейтрализация последствий деструктивных воздействий путём применения теории графов для переконфигурирования структуры системы / Е.А. Зайцева, Д.С. Лаврова, Д.П. Зегжда // Методы и технические средства обеспечения безопасности информации. – 2019. – № 28. – С. 7–8.

8. Зегжда, Д.П. Подход к созданию критерия устойчивого функционирования киберфизических систем / Д.П. Зегжда, Е.Ю. Павленко, Д.С. Лаврова, А.А. Штыркина // Проблемы информационной безопасности. Компьютерные системы. – СПб., 2019. – № 2. – С. 156–163.

9. Pavlenko, E.Yu. Homeostatic approach to assessing digital manufacturing security / Pavlenko E.Yu., Zegzhda D.P. // SHS Web of Conf. CC-TESC2018 - 2018. - Vol. 44. – Pp. 00066.

10. Зегжда, П.Д., Гомеостатическая стратегия управления безопасностью киберфизических систем / П.Д. Зегжда, Д.П. Зегжда, Е.Ю. Павленко // Материалы 26-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». - СПб., 2017. - С. 51-52.

Самарин Н.Н.
ФГУП «НИИ «Квант», начальник научно-исследовательского отделения, к.т.н,
samarin_nik@mail.ru
Сирота А.А.
СПбПУ, студент,
sirota.aa@edu.spbstu.ru

ПРИМЕНЕНИЕ ОБРАТНОГО СИМВОЛЬНОГО ВЫПОЛНЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ ОШИБОК В ИСПОЛНЯЕМОМ БИНАРНОМ КОДЕ

В настоящее время программное обеспечение (ПО) разрабатывается путем сложной комбинации множества различных технологий, а его функционирование выполняется в разнородной среде, включающей большое число устройств разного типа. Объем отдельных программных модулей в составе информационной системы крайне велик даже с учетом высокоуровневых языков программирования – свыше миллионов строк кода, следовательно, бинарные коды таких файлов занимают еще больше пространства [1].

Задача анализа безопасности таких файлов является технически сложной – как для ручного тестирования, так и для специальных программ-анализаторов: рассмотреть все возможные пути выполнения образца ПО практически невозможно, так как такая задача сводится к полному перебору [2]. Следовательно, актуальной задачей является разработка специальных методов, которые бы использовали эвристики, сокращающие этот перебор до такой степени, чтобы осуществление анализа безопасности стало реализуемо за приемлемое время.

В работе используется метод символьного выполнения [3-6] с обратным распространением – ОСВ (обратное символьное выполнение).

Объектом

анализа является отдельно взятый путь из графа управления, цель анализа состоит в проверке достижимости. Основная идея метода состоит в следующем:

1. Первоначально методом статического анализа производится поиск потенциально уязвимых участков бинарного кода.

2. Затем фиксируется путь выполнения *p*.

3. Производится символьное выполнение заданного пути *p* в обратном порядке.

Модель метода представлена на Рис. 1.

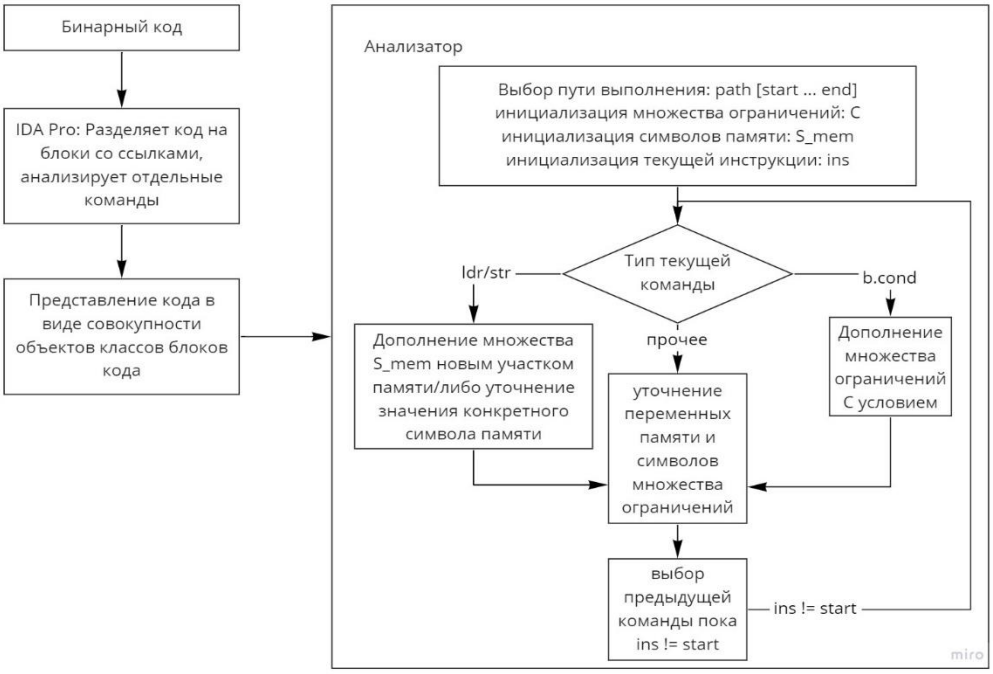


Рис. 1. Модель метода обратного символьного выполнения

Изначально все параметры образца ПО представляются в виде некоторых символьных переменных. Учитывая, что анализируются бинарные файлы, в качестве переменных выступают регистры и отдельно взятые участки памяти. Изначально на переменные накладывается ряд условий, при которых может сработать исключение в коде. Затем на каждом шаге анализа множество ограничений дополняется новыми в точках ветвления (команды

условного перехода), а значения переменных преобразуются в соответствие с выполняемой командой. Такую процедуру далее будем называть уточнением.

Основные компоненты, используемые при вычислении, это – символьное множество памяти S_{mem}, представленное как набор индексируемых переменных *mem*, и набор ограничений *C*.

Операция уточнения по операции *o* будем называть операцией перевода описания текущего состояния *S* системы к описанию возможных состояний системы до выполнения операции *o*. Уточнением конкретных переменных системы является замена этих переменных на некоторые выражения, полученные путем применения текущей операции *o* к её аргументам.

При обработке прямых ветвлений вида «условный переход», система не дублируется с различными условиями, как происходит при прямом выполнении. В данном случае изначально существует две копии системы, пришедшие к этому условию с различных веток. То есть, эти копии изначально могли быть запущены параллельно с различными начальными условиями.

Как только система доходит до начала функции, производится синхронизация переменных из набора ограничений с локальными переменными на стеке. После чего выполняется финальное решение системы ограничений. В результате получается множество ограничений на входные параметры для конкретной функции.

Метод обратного символьного выполнения обладает следующими преимуществами:

1. Сокращение роста ветвлений внутри кода, поскольку в большинстве случаев экспоненциальный рост ветвлений появляется в ходе анализа при прямом выполнении.

2. Возможность дополнения отдельных функций своими наборами ограничений. путем применения какого-либо внешнего анализа.

3. Более точное предсказание вида исходного числа при проведении операции взятия остатка от деления.

Однако у данного метода есть существенный недостаток: он заключается в сложности обращения некоторых функций, в том числе, функции умножения. Учитывая большое количество таких функций (умножение, хеш-функции, большинство битовых операций, в частности, XOR), при неизвестных входных параметрах обратный анализ данных функций станет вычислительно сложной задачей, и единственным оптимальным вариантом будет откладывание вычисления таких функций до момента уточнения входных параметров. А это в итоге может свести метод обратного выполнения к методу прямого символьного выполнения.

Также стоит отметить такие недостатки метода, как сильное ветвление при сортировке и неоднозначность переменных (как правило, такая проблема возникает при обращении к одному участку памяти с использованием разных регистров) [7].

Для устранения вышеописанных проблем предлагается следующее решение: использовать метод ОСВ в совокупности с методом прямого символьного выполнения. Так как метод ОСВ представляет из себя в большей степени метод проверки достижимости отдельных участков кода, чем метод поиска уязвимостей, его можно применить на последнем шаге метода прямого символьного выполнения. Возможен также вариант, при котором реализуется двусторонний анализ, в ходе которого код выполняется от начала методом прямого выполнения и от некоторой точки кода методом ОСВ. Затем, в некоторой средней точке, анализатор сопоставляет множества ограничений обоих методов и делает вывод о достижимости. Это позволит исключить некоторые ветви выполнения для прямого анализатора, повысив, тем самым, эффективность анализа.

Приведем формальное представление алгоритмов классического и обратного символьного выполнения, на основе которых предлагаются возможные способы комбинирования алгоритмов.

Метод прямого символьного выполнения сводится к тому, чтобы по некоторым входным данным построить множества возможных выходных данных. Если представить процесс выполнения кода в виде графа передачи управления, то любая машинная команда ветвления будет иметь только два адреса перехода (при истинном и ложном условии перехода). Блоки кода без условных переходов будем считать вершинами графа. Тогда граф будет состоять из подграфов вида, представленного на Рис. 2.

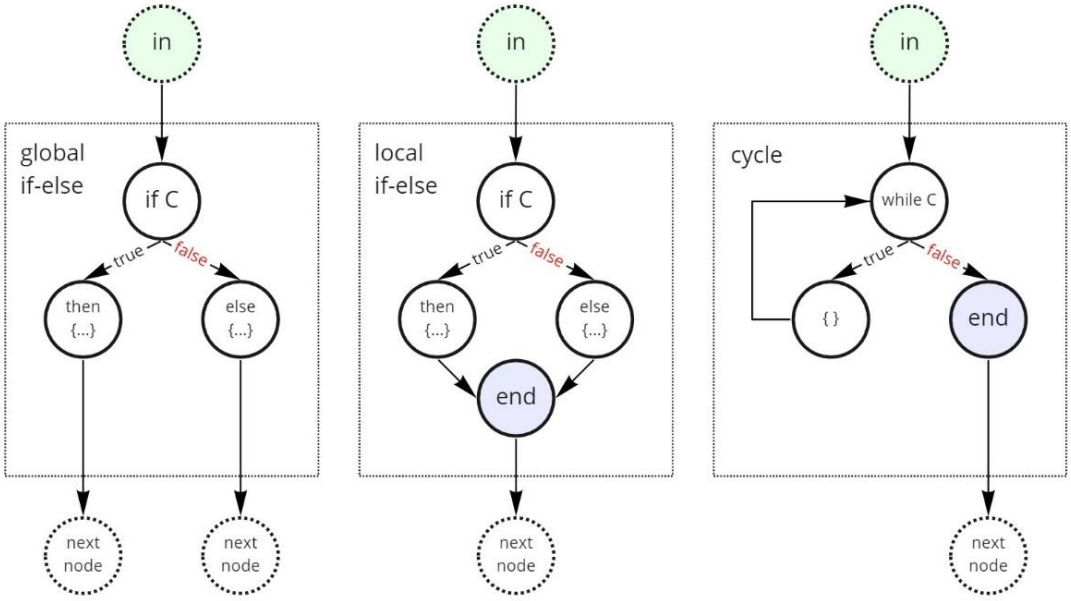


Рис. 2. Виды ветвлений кода

Формальное представление метода прямого символьного выполнения *SE* можно представить в виде отображения представленного в формуле (1.1).

$$SE:(X,C(X))\to\{(Y,C_i(X))\,|\,i\in M\subseteq[0,2^{h-1}-1]\},\qquad(1.1)$$

где C – начальное множество ограничений, X – входные данные, M – некоторый диапазон значений, h – высота дерева переходов.

Для метода ОСВ множества ограничений C_i считаются изначально заданными. Далее анализатор поднимается по дереву ветвления кода, которое при изначальном покрытии всех веток кода совпадает с деревом ветвлений для прямого символьного исполнителя. В точках ветвления анализатор объединяет множества ограничений и условия в них, тем самым восстанавливая исходный вид множества ограничений до ветвления. Ниже представлен формальный пример обработки участка кода с ветвлением (1.2).

$$c_{\overline{a_n \ldots a_0}}(X) = c_{\overline{0a_n \ldots a_0}} f_0(X_0) \cup c_{\overline{1a_n \ldots a_0}} f_1(X_1), \quad (1.2)$$

где X_0, X_1 – восстановленный вид входных данных на ветвях ложного и истинного условия ветвления соответственно, f_0 и f_1 – производимые операции над входными данными на этих ветвях, $a_i \in \{0,1\}$.

После объединения ограничений итоговое множество отправляется решателю, где оно так же анализируется и выдается результат в виде упрощенного множества ограничений и восстановленных входных данных. Формальное описание отображения для метода обратного символьного выполнения RSE представлено ниже (1.3).

$$RSE : \{(Y, C_i'(X)) \mid i \in M \subseteq [0, 2^{h-1} - 1]\} \to (X', C'(X)) \quad (1.3)$$

Пример последовательности действий обратного символьного исполнителя на графе ветвлений кода представлен на Рис. 3.

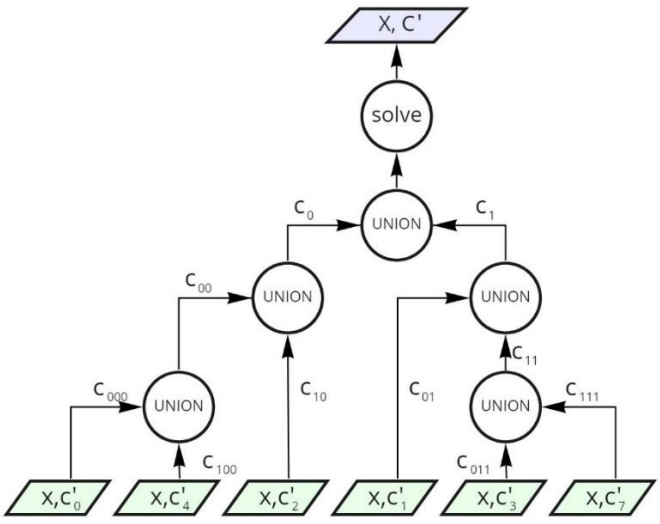


Рис. 3. Пример работы ОСВ на графе ветвлений кода

Для объединения методов требуется сопоставить результаты работы обоих алгоритмов. Объединять методы предлагается путем последовательного их соединения по множеству ограничений и множеству данных на графе выполнения программы. Формат результата одного из методов сопоставим с форматом выходных данных другого метода, равно как и для входных данных. То есть, выходные данные прямого метода выполнения $\{(Y, C_i(X))\}_{i \in M}$ сопоставимы с выходными данными обратного метода выполнения $(X', C'(X))$, при его выполнении далее на той же ветви графа. Одновременно с этим, входные данные метода обратного символьного выполнения $\{(Y, C_i'(X'))\}_{i \in M}$ также можно использовать в качестве входных данных для прямого символьного выполнения $(X, C(X))$, выделяя по копии прямого символьного исполнителя на каждую начальную ветвь обратного выполнения. Таким образом, методы могут быть объединены друг с другом.

В рамках практической апробации предложенной модели был реализован вариант зеркального объединения, состоящий в сокращении промежуточного множества ограничений путем его объединения с результатами работы метода ОСВ на отдельно взятых участках кода. Оценка эффективности предложенной модели проводилась на реализованном экспериментальном макете с использованием набора исходных данных Software Assurance Reference Dataset [10] от NIST (National Institute of Standards and Technology). В качестве результатов тестирования оценивалось время работы классического алгоритма символьного выполнения и алгоритма оптимизированного с помощью метода обратного символьного выполнения по логике зеркального объединения на определенных ветвях.

По результатам тестирования, время работы алгоритма с предложенным методом оптимизации при обнаружении программных ошибок и уязвимостей, порожденных вычислительными ошибками или

отсутствием инициализации переменных, в среднем сократилось на 2.1%, что говорит о практической применимости разработанной модели.

СПИСОК ЛИТЕРАТУРЫ

1. Balakrishnan, G. Fast library identification and recognition technology / G. Balakrishnan, T. Reps // [Электронный ресурс]. — Режим доступа : http://www.datarescue.com/idabase/flirt.htm.

2. Balakrishnan, G. Analyzing Memory Accesses in x86 Executables / G. Balakrishnan, T. Reps // [Электронный ресурс]. — Режим доступа : https://research.cs.wisc.edu/wpis/papers/cc04.pdf.

3. Baldoni, R. A survey of symbolic execution techniques / R. Baldoni, E. Coppa, D. C. D'elia, C. Demetrescu, I. Finocchi // ACM Computing Surveys (CSUR). – 2018. – 51(3). – P. 1-39.

4. Daniel, L. A. Binsec/rel: Efficient relational symbolic execution for constant-time at binary-level / L. A. Daniel, S. Bardin, T. Rezk // In 2020 IEEE Symposium on Security and Privacy (SP). – 2020. – P. 1021-1038.

5. Бородин, А. Е. Внутрипроцедурный анализ для поиска ошибок на основе символьного выполнения / А. Е. Бородин, И. А. Дудина // Труды Института системного программирования РАН. – 2020. – №32(6). – С. 87-100.

6. Борисов, П. Д. О характеристиках символьного исполнения в задаче оценки качества обфусцирующих преобразований / П. Д. Борисов, Ю. В. Косолапов // Моделирование и анализ информационных систем. – 2021. – №28(1). – С. 38-51.

7. Caballero, J. Input generation via decomposition and re-stitching: Finding bugs in malware / J. Caballero, P. Poosankam, S. McCamant, D. Babic, and D. Song // Security, Chicago, IL. – 2010.

8. Sparks, S. Automated vulnerability analysis: Leveraging control flow for evolutionary input crafting / S. Sparks, S. Embleton, R. Cunningham, C. Zou // In

Twenty-Third Annual Computer Security Applications Conference (ACSAC 2007). – 2007. – Pp. 477-486.

9. Nandi, A., Mandal, A., Atreja, S., Dasgupta, G. B., & Bhattacharya, S. Anomaly detection using program control flow graph mining from execution logs / A. Nandi, A. Mandal, S. Atreja, G. B. Dasgupta, S. Bhattacharya // In Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. – 2016. - Pp. 215-224.

10. NIST's Software Assurance Reference Dataset. [Электронный ресурс]. — Режим доступа: https://samate.nist.gov/SRD/view.php.

НАУЧНАЯ СЕКЦИЯ

«ОРГАНИЗАЦИОННО-ПРАВОВЫЕ И ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ»

Руководитель: **Кубанков Александр Николаевич**,
Московского технического университета связи и информатики, доктор военных наук, профессор, заведующий кафедрой «Безопасность телекоммуникаций»

Секретарь: **Булгакова Елена Валерьевна**,
Московский технический университет связи и информатики, кандидат юридических наук, доцент

Гришина Н.В.
Российский государственный
гуманитарный университет, доцент,
Московский государственный
лингвистический университет, доцент,
к.т.н., доцент,
grnat@rambler.ru

ПЕРСОНАЛЬНЫЕ ДАННЫЕ: ЗАЩИЩЕНЫ ИЛИ НЕТ?

Реализация национальных проектов России в области цифровой экономики [2,3,4] открывает новые горизонты для внедрения цифровых технологий в социальную и экономическую сферу, предоставляет условия для высокотехнологичного бизнеса. Как следствие – повышение конкурентоспособности страны, укрепление национальной безопасности и качества жизни людей.

Особое место занимает проблема обеспечения информационной безопасности. Этот фактор является системообразующим для успешной реализации всего проекта: если не обеспечить целостность циркулирующей информации, ее доступность, достоверность и, в случае необходимости, ее конфиденциальность, то вся остальная деятельность будет нецелесообразной.

Реализация программы цифровая экономика позволила сформировать принципиально новые возможности для каждого гражданина. Внедрено огромное количество новых сервисов. Если раньше для того, что бы получить рядовую справку, людям приходилось отстаивать огромные очереди, а в сложных ситуациях на это необходимо было потратить несколько дней, то теперь получить многие документы и заказать услуги можно не выходя из дома.

В этих условиях важная роль отводится обеспечению защиты персональных данных. Граждане доверяют «цифре» свои документы, пользуются онлайн - банками для управления своими денежными средствами, обмениваются сообщениями с помощью различных мессенджеров и т.д.

Еще в 2006 году был принят Федеральный закон «О персональных данных» [1], но до сих пор проблема защиты персональных данных стоит очень остро.

В России существует «черный рынок» персональных данных. Лидерами этого рынка являются финансовые организации и интернет - провайдеры. Этот рынок растет год от года. Не секрет, что причиной «утечки» персональных данных чаще всего являются собственно сотрудники компаний.

15 августа 2022 был опубликован очередной отчет по утечке данных их структуре и динамике Экспертно-аналитического центра ГК InfoWatch [10].

Опираясь на данные Экспертно-аналитического центра ГК InfoWatch за последние годы, можно проследить динамику по ряду вопросов, касающихся утечки данных вообще и персональных в частности.

Рис 1. Объем утечки персональных данных в России в структуре различных данных

Если рассматривать структуру всех данных, подвергшихся утечке, то «львиную» долю среди них занимают именно персональные данные. Причем, с каждым годом эта доля увеличивается все больше (Рис.1). Таким образом, говоря об утечке информации, можно с высокой долей вероятности говорить, что речь идет именно о персональных данных

Описанный факт можно достаточно легко объяснить: именно персональные данные «востребованы» в большей мере на «черном» рынке.

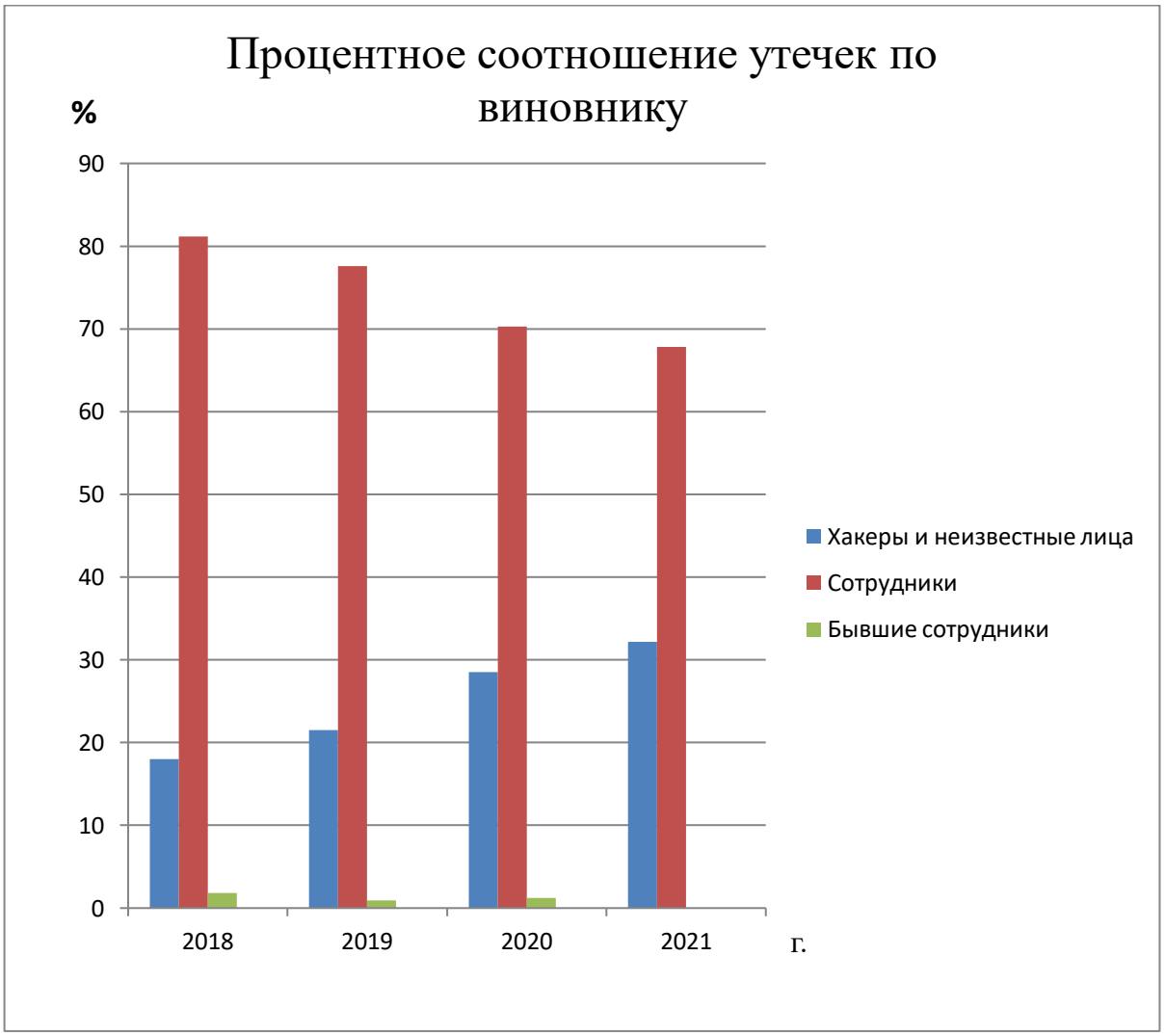


Рис. 2. Процентное соотношение утечек информации по виновнику

На Рис. 2 показано соотношение виновных в утечке информации. Все сотрудники предприятия объединены в одну группу: включая руководителей, системных администраторов и т.д. На рисунке прослеживается явная тенденция: доля сотрудников и бывших сотрудников уменьшается, а хакеров и неизвестных соответственно, увеличивается. Эта тенденция подтверждается и Рис.3.

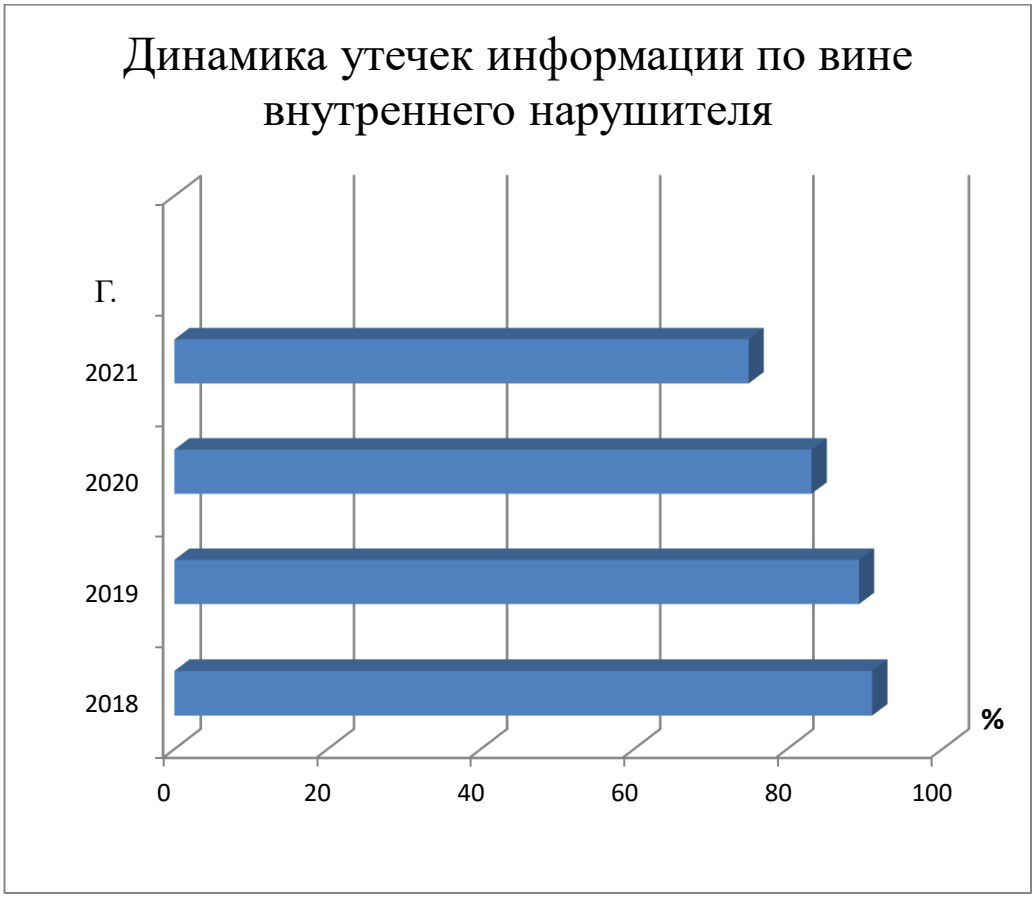


Рис. 3. Динамика утечек информации по вине внутреннего нарушителя

Еще одна интересная тенденция показана на Рис.4. По сравнению с 2018 годом произошли качественные изменения: существенно уменьшился объем утечек на бумажных носителях.

На Рис.5 можно посмотреть динамику доли умышленных утечек. Достаточно очевидно, что принципиальных изменений здесь нет.

Рис. 4 . Бумажные носители в общем объеме носителей утечек

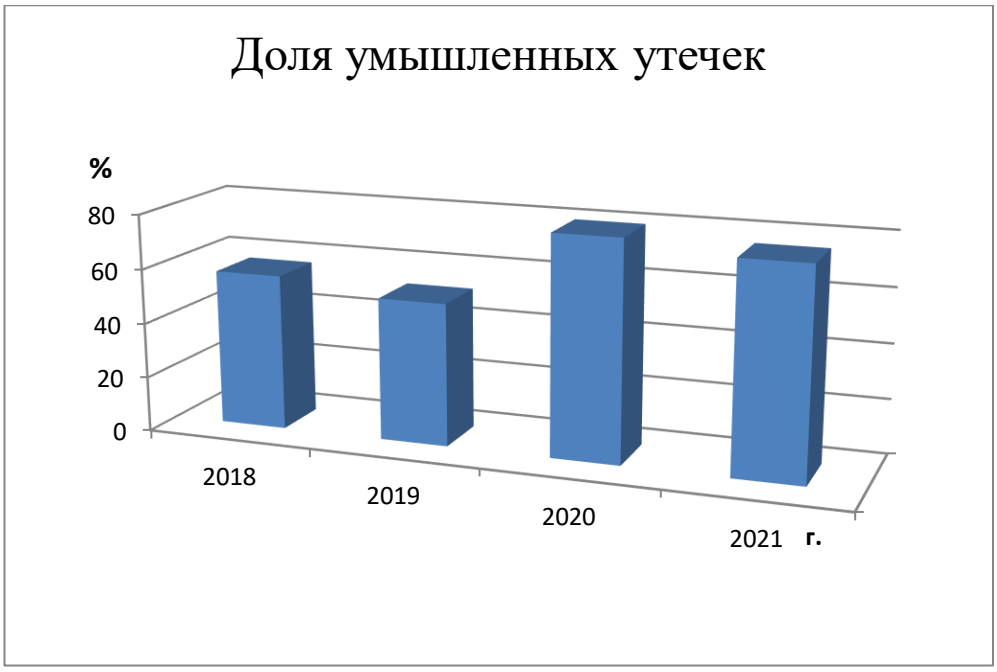


Рис. 5. Доля умышленных утечек

Не смотря на то, что в России действует целый ряд нормативных актов относительно защиты персональных данных, ситуацию сложно назвать стабильной. В чем же дело? Почему законы «не работают»?

Причин можно назвать много, например:

- действующие нормативные и правовые документы не учитывают «нюансы» конкретных противоправных действий относительно персональных данных;

- несущественная ответственность организаций, связанная с утечкой персональных данных;

- субъекты скомпрометированных персональных данных не обращаются с исковыми заявлениями в суд;

- невозможность построения полностью защищенной информационной инфраструктуры и т.п.

Заключение

Определить какой-либо конкретный перечень последствий утечки персональных данных практически невозможно. Этот перечень может существенно меняться в зависимости от ряда факторов:

- содержания скомпрометированных персональных данных;
- изобретательности мошенников, которые эти данные получили;
- поведения лица, чьи данные скомпрометированы.

Конечно, понимание того, что персональные данные попали в чужие руки неприятно. В то же время надо помнить, что паспортные данные, фотография паспорта не могут быть использованы, например, для получения кредита. А для организации атаки на субъекта с использованием средств социальной инженерии этой информации может быть достаточно для введения человека в заблуждение, запугивания и отнятия денежных средств.

СПИСОК ЛИТЕРАТУРЫ

1.Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ

2.Указ Президента Российской Федерации от 07.07.2011 № 899 "Об утверждении приоритетных направлений развития науки, технологий и техники в Российской Федерации и перечня критических технологий Российской Федерации" (в ред. Указа Президента Российской Федерации от 16.12.2015 № 623)

3.Указ Президента РФ от 7 мая 2018 г. N 204 "О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года"

4.Указ Президента Российской Федерации от 09.05.2017 № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы"

5.Гришина, Н.В. Деловая разведка как разновидность информационной работы /Н.В. Гришина, С.А. Емельянов // Прикладная информатика. —2006. — № 3(3). — С. 34-41.

6.Гришина, Н.В. Проблемы обеспечения информационной безопасности при использовании облачных технологий / Н.В. Гришина, О.В. 7.Маленкова, И.Н. Бычков // Международная научно-практическая конференция "Современные проблемы и задачи обеспечения информационной безопасности" Москва, 18 апреля 2017 года. — 2017. — С.

8.Гавриленко, А.В. Дистанционное обучение и информационная безопасность/А.В. Гавриленко // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». —2021. —№ 1. —С. 51–65. DOI: 10.28995/2686-679X-2021-1-51-65

9.Карпов, Д.С. Меры нейтрализации воздействия нарушителя информационной безопасности на подсистему биометрической аутентификации специальной информационной системы / Д.С. Карпов, А.А. Раковенко // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». —2019. — № 4. — С. 42–52.

10.Скрынникова А. Побочное явление цифровизации: как в России крадут и продают персональные данные https://www.forbes.ru/tehnologii/433651-pobochnoe-yavlenie-cifrovizacii-kak-v-rossii-kradut-i-prodayut-personalnye-dannye
11.Отчёт об исследовании утечек информации ограниченного доступа в I половине 2022 года. Экспертно-аналитический центр InfoWatch. 2022 г.

Ефимова К.А.
Студентка 1 курса магистратуры
Направления «Цифровая трансформация систем безопасности»
ИГЗ ФГБОУ ВО «УдГУ»
efimova_ka@mfc.udmr.ru
Колчерина Ж.Н.
Старший преподаватель кафедры
информационной безопасности в управлении
ИПСУБ ФГБОУ ВО «УдГУ»
zhulya@jf.uni.udm.ru

ПРИМЕНЕНИЕ МОДЕЛЕЙ ЗРЕЛОСТИ ПРИ ОЦЕНКЕ ЭФФЕКТИВНОСТИ ПРОЦЕССОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Организации, деятельность которых во многом зависит от информационной сферы, для достижения целей деятельности должны обеспечивать эффективное функционирование процессов информационной безопасности [1]. Для понимания того насколько эффективно функционируют процессы информационной безопасности и на сколько эффективны вложения организации в информационную безопасность применяется оценка эффективности процессов информационной безопасности. При оценке эффективности можно выявить слабые стороны защиты информации в организации, недостатки в функционировании процессов, и на основании оценки также можно разработать предложения по устранению недостатков процессов и по совершенствованию системы обеспечения информационной безопасности [2].

Одним из способов оценки эффективности процессов информационной безопасности могут быть модели зрелости. Модели зрелости процессов

информационной безопасности – это концепция, используемая для оценки процессов информационной безопасности в организации, позволяющая оценить прогресс, достигнутый в обеспечении безопасности в повседневных и стратегических задачах, выявить недостатки в процессах информационной безопасности и, отталкиваясь от результатов, позволяет разработать пути совершенствования процессов [3].

Модель зрелости используется как инструмент измерения состояния процесса на основе набора метрик, которые представляют собой определенные характеристики. Оценка этих метрик по оговоренной шкале позволяет понять состояние процессов организации, которая и будет характеризовать уровень зрелости. После получения оценки зрелости можно выработать необходимые мероприятия для повышения зрелости процессов и организации в целом [4].

Существует множество моделей оценки зрелости такие как:

1. Control Objectives for Information and related Technology (COBIT);
2. Information Security Maturity Model (ISMM);
3. Cybersecurity Capability Maturity Model – National Institute of Standards and Technology (CSF – NIST);
4. Community Cyber Security Maturity Model, CCSMM; и др.

Для оценки зрелости процессов в организации используются метрики информационной безопасности или показатели. Метрики информационной безопасности - это KPI, ключевые показатели эффективности (англ. - Key Performance Indicators), которые позволяют количественно оценить работу персонала и систем, обеспечивающих информационную безопасность. Для визуализации показателей предлагается использовать графическое отображение в виде дашбордов [5].

Для примера используем процесс оценки зрелости на основании модели зрелости возможностей (SSE-CMM), описанную в ГОСТ Р ИСО/МЭК 21827-2010.

Оценка процессов информационной безопасности [6], основывается на следующих принципах:

- процессы информационной безопасности оценивается по 5 уровням: от первого (минимального) до пятого (максимального), причем каждый следующий уровень включает полностью реализацию предыдущих уровней;

- каждый уровень описывается определенным набором показателей и их значениями.

Для оценки возьмем один из критичных процессов любой организации, это процесс реагирования на инциденты. Процесс реагирования на инциденты может серьезно повлиять на бизнес-процессы организации. Успешная реализация процесса управления инцидентами позволяет определять и разрешать события в области ИБ и инциденты, сокращать продолжительность и последствия простоев в работе.

Для оценки задаем следующие KPI, подходящие под данный процесс. Пример возможных оцениваемых метрик приведен ниже (Табл. 1) [7].

Табл. 1. KPI для оценки процесса реагирования на инциденты

Количество инцидентов	**Общее количество инцидентов за год**
Процент обработанных инцидентов	(Количество обработанных инцидентов в год/ Общее количество инцидентов) * 100%
Среднее время обнаружения инцидента	Время, за которое был обнаружен инцидент
Среднее время реагирования на инциденты	Средний период времени от момента получения обращения об инциденте службой технической поддержки

Для оценки метрик процесса реагирования на инциденты используем документацию организации, либо системы, анализирующих данные KPI. Период анализа выбирается оценщиками. Анализируемые KPI в дальнейшем будут предоставляться экспертам, для выставления ими обоснованных оценок.

Для оценки создается экспертная комиссия, обладающая необходимыми компетенциями в данной области. Методы экспертных оценок являются частью обширной области теории принятия решений, а само экспертное оценивание — процедура получения оценки проблемы на основе мнения специалистов (экспертов) с целью последующего принятия решения (выбора) [8].

Компетентность экспертов зависит от уровня их образования, опыта и др. факторов [9]. К примеру компетентность экспертов может быть проанализирована по таблице, приведенной ниже (Табл. 2).

Табл. 2. Профессиональная компетентность эксперта

Факторы	**Значение весового коэффициента**		
Уровень образования	Среднее	Среднее специальное	Высшее
	0,2	0,3	0,5
Стаж работы	от 1 до 5 лет	от 5 до 10 лет	свыше 10 лет
	0,2	0,3	0,5
Опыт работы по профилю проведения экспертизы	Отсутствует	от 1 до 5 лет	свыше 5 лет
	0	0,4	0,6
Научная квалификация	без ученой степени	ученая степень кандидата наук	ученая степень доктора наук
	0	0,4	0,6
Наличие научных трудов последние 5 лет.	Отсутствуют	до 5 статей	свыше 5 статей
	0	0,4	0,6

Компетентность рассчитывается по следующим формулам. Вычисляется сумма SumXi баллов набранных i – м экспертом по всем факторам, применяя следующую формулу (1.1):

$$SumX_i = \sum_{j=1}^{n} a_{ij} \ . \qquad (1.1)$$

Вычисляется сумма баллов SumФ j – го фактора по всем экспертам, применяя следующую формулу (1.2):

$$SumФ_j = \sum_{i=1}^{m} a_{ij} \ . \qquad (1.2)$$

Вычисляется весовой коэффициент экспертов по всем факторам, применяя следующую формулу (1.3):

$$W_i = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}}{\sum_{j=1}^{n} a_{ij}}, \qquad \sum_{i=1}^{m} W_i = 1 \ . \qquad (1.3)$$

На основании определенных вычислений, проставляется вес оценки каждого эксперта. В дальнейшем к оценкам, проставленным экспертами при анализе метрик, будет еще добавляться их весовой коэффициент для получения более точного результата оценки.

Для оценки зрелости на основании мнения экспертов разрабатывается анкета оценивания групповых показателей ИБ [10]. Так пример анкеты для оценивания процесса реагирования на инциденты приведен в таблице ниже (Табл. 3).

Табл. 3. Анкета для оценки метрик процесса реагирования на инциденты

Показатель оценки	**Оценки экспертов**
Существуют ли в организации документы, регламентирующие процедуры обнаружения инцидентов ИБ?	
Существуют ли в организации документы, регламентирующие процедуры реагирования на инцидент?	
Сформирована и поддерживается ли в актуальном состоянии централизованная база инцидентов ИБ?	

Назначены ли ответственные за выполнение ролей по обнаружению, классификации, реагированию, анализу и расследованию инцидентов ИБ?	

Оценки экспертами также выставляются по определенной шкале, приведенной ниже (Табл. 4). При проставлении оценок экспертами тщательно анализируются документация по ИБ, данные в информационных системах, а также используя различные инструменты, проводится анализ состояния процесса ИБ.

Табл. 4. Критерии оценивания метрик процесса

Оценка частного показателя ИБ	Критерий выставления оценки частного показателя ИБ
0	Требования не установлены; либо установлены частично во внутренних нормативных документах проверяемой организации и не выполняются
0,25	Требования полностью установлены в нормативных документах проверяемой организации, но не выполняются; либо не установлены во внутренних нормативных документах проверяемой организации и выполняются в неполном объеме;
0,5	Требования полностью установлены во внутренних нормативных документах проверяемой организации и выполняются в неполном объеме;
0,75	Требования частично установлены во внутренних нормативных документах проверяемой организации, но выполняются в полном объеме
1	Требования полностью установлены во внутренних нормативных документах проверяемой организации и выполняются в полном объеме

Выставление общего уровня зрелости процессу ИБ происходит исходя из таблицы, приведенной ниже (Табл. 5), уровень зрелости сопоставляется с выставленными экспертами оценками.

Для удобства расчетов анкетирование можно проводить в таблице Excel. Там эксперты могут выставлять каждому показателю свои оценки и все остальные значения будут считаться автоматически. После выставления оценок экспертами, к каждой их оценке автоматически приравнивается

весовой коэффициент каждого эксперта и на основании этого выводится уровень зрелости процесса. А также в Excel можно настроить автоматическое выведение дашбордов, отражающих результаты оценки.

Табл. 5. Присвоение процессу ИБ уровня зрелости

Уровень зрелости	Итоговая оценка
Первый уровень	от 0 до 0,0832
Второй уровень	от 0,0833 до 0,16666
Третий уровень	от 0,16667 до 0,24
Четвертый уровень	от 0,25 до 0,332
Пятый уровень	0,333

Полученные результаты визуализируем в виде дашборда, позволяющего наглядно показать результаты проведенной оценки зрелости процессов информационной безопасности (Рис. 1).

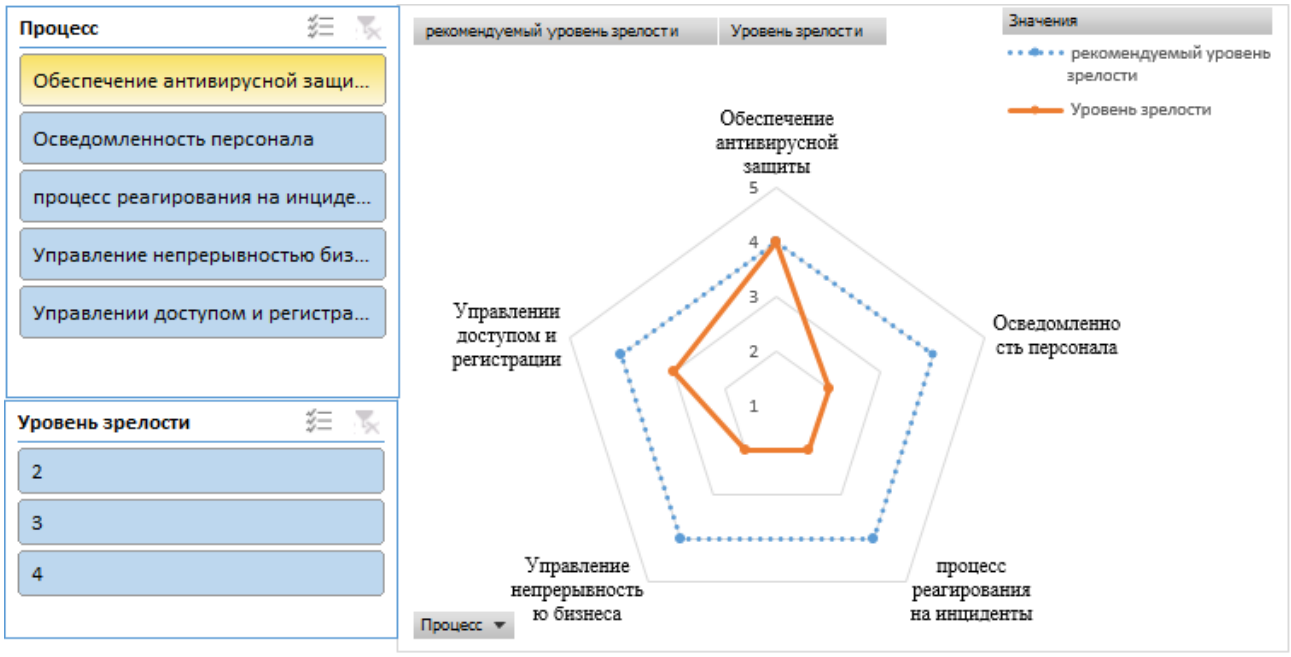


Рис.1. Уровни зрелости процессов ИБ

Также для удобства анализа, все KPI можно проиллюстрировать в виде дашбордов, приведенных ниже (Рис.2 – Рис. 3). По дашбордам можно легко увидеть KPI, которые реализованы не в полной мере, а также на основании

них можно предложить рекомендации по повышению уровня зрелости процесса ИБ.

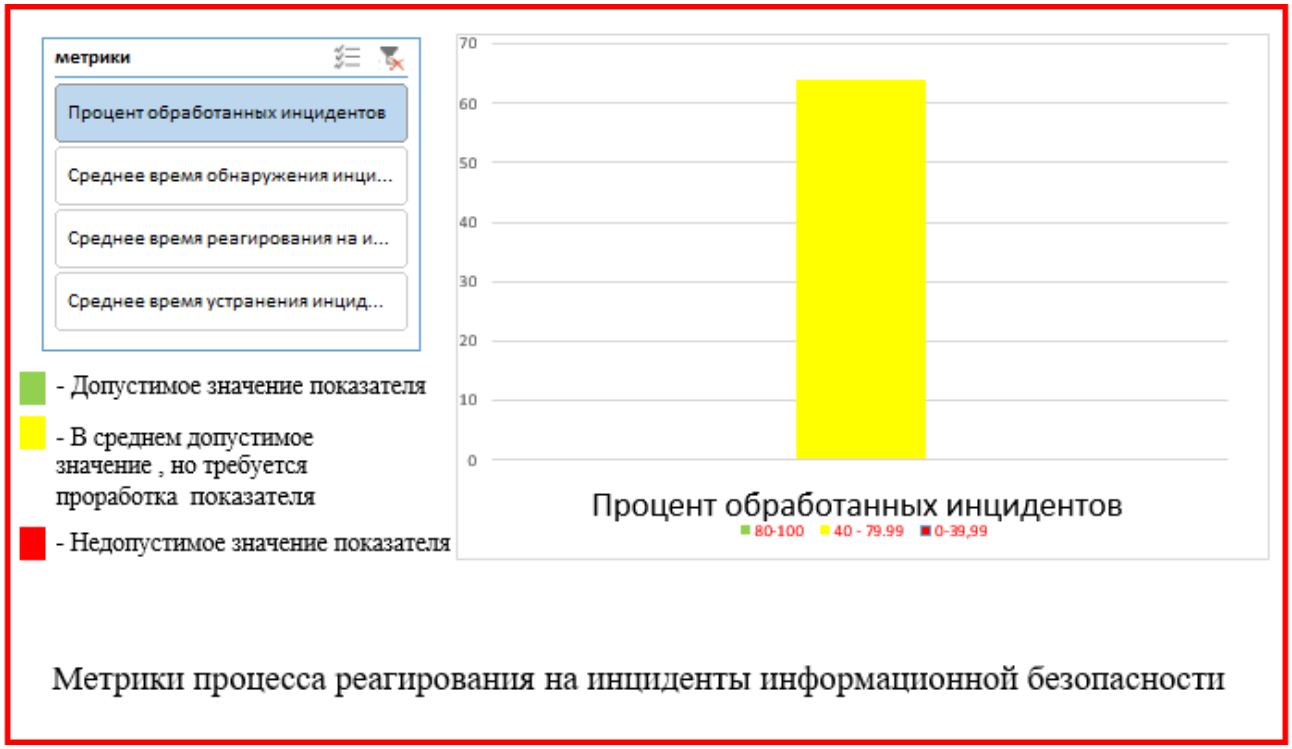


Рис. 2. Дашборд, оценивающий метрики ИБ

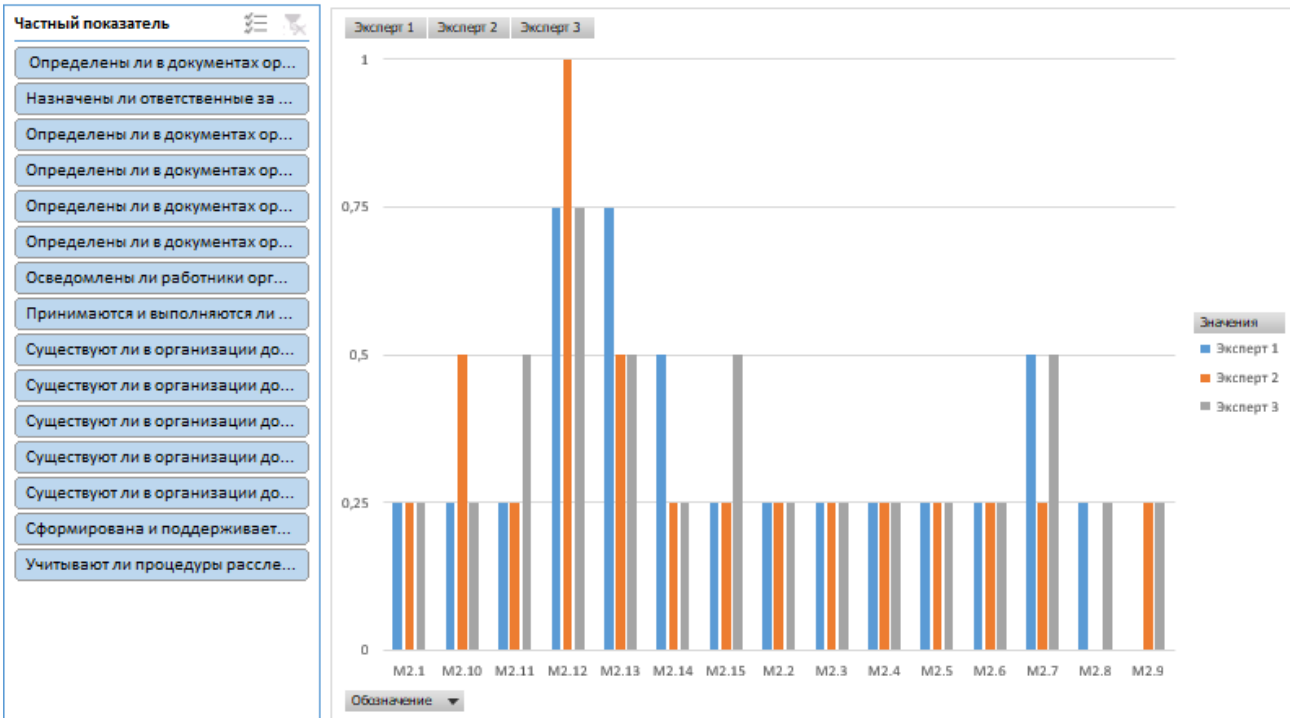


Рис. 3. Дашборд с оценками экспертов

Приведенный алгоритм с легкостью может помочь при оценке зрелости процессов ИБ в организации. Так, на основании моделей зрелости можно проанализировать эффективность процессов информационной безопасности, охарактеризовать полноту, адекватность, результативность процессов ИБ организации, а также позволит разработать рекомендации для повышения зрелости и эффективности процессов.

СПИСОК ЛИТЕРАТУРЫ

1) Головина, Э. С. Критерии оценки эффективности управления деятельностью предприятия / Э. С. Головина, Ю. А. Анищенко. — Текст : непосредственный // ЭКОНОМИКА И БИЗНЕС. — 2012. — № 338. — С. 21-22.

2) Курило А.П., Зефиров С.Л., Голованов В.Б. и др. Аудит информационной безопасности. — М.: Издательская группа «БДЦ-пресс», 2006. — 304с.

3) Коптелов А.К. Оценка зрелости процессного управления. Обзор методик оценки зрелости [Электронный ресурс]. – URL: https://koptelov.info/wp-content/uploads/2019/06/HSBI_Zrelost.pdf (дата обращения: 05.09.2021)

4) Баскаков А.В. Модель зрелости как инструмент развития процесса безопасности в организации процессов [Электронный ресурс]. – URL: http://journal.itmane.ru/node/913 (дата обращения: 24.09.2022).

5) COBIT. — Текст : электронный // isaca.org : [сайт]. — URL: https://www.isaca.org/en/resources/cobit (дата обращения: 01.10.2022).

6) ГОСТ Р ИСО/МЭК 21827-2010. Информационная технология. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Проектирование систем безопасности. Модель зрелости процесса. – М.: Стандартинформ, 2010. – 124 с.

7) Шаго, Ф. Н. Методика оценки эффективности системы менеджмента информационной безопасности по времени реакции системы на

инциденты информационной безопасности / Ф. Н. Шаго. — Текст : непосредственный // Научно-технический вестник информационных технологий, механики и оптики . — 2014. — № 4(92). — С. 115-122.

8) Постановление Правительства РФ от 29 ноября 2021 г. N 2080 "О порядке подтверждения компетентности эксперта-аудитора и требованиях к экспертам-аудиторам" //Консультант Плюс. [Электронный ресурс]. URL: http://www.consultant.ru/ (дата обращения 20.04.2022)

9) Петриченко, Г. С. МЕТОДИКА ОЦЕНКИ КОМПЕТЕНТНОСТИ ЭКСПЕРТОВ / Г. С. Петриченко, В. Г. Петриченко. — Текст : непосредственный // Научный журнал КубГАУ. — 2015. — № 109(05). — С. 8-19.

10) Измерение эффективности процессов кибербезопасности. Часть 1. // securityvision.ru : [сайт]. — URL: https://www.securityvision.ru/blog/izmerenie-effektivnosti-protsessov-kiberbezopasnosti-metriki-ib-chast-1/ (дата обращения: 17.09.2022).

Зорин А.Е.
ЮРГПУ(НПИ) им. Платова, студент
screen.1999.14@gmail.com

ЗАЩИТА ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Аннотация

Целью работы является понятие определения телекоммуникационной сети. Рассмотрение видов и классификаций телекоммуникационных систем связи, типы сетей, линий и каналов связи.

В ходе работы рассматривается защита информации в телекоммуникационных сетях и задачи направленные на защиту информации в телекоммуникационных сетях.

В соответствии с определёнными требованиями предложены необходимые организационные, инженерно-технические и программно-аппаратные методы и средства защиты информации.

Итогом работы являются средства и методы защиты информации в телекоммуникационных сетях.

Телекоммуникационная сеть - это узлы либо группа узлов, объединенные телекоммуникационными каналами, которые применяются с целью обмена сообщениями между ними. Каналы связи могут применять разнообразные технологии, основанные на методиках коммутации каналов, сообщений либо пакетов, с целью передачи сообщений а также сигналов.

Образцами телекоммуникационных сетей считаются компьютерные сети, интернет, коммутируемая телефонная сеть общего пользования (ТСОП), глобальная сеть телекса, беспроводные радиосети сотовых телекоммуникационных провайдеров а также авиационная сеть ACARS.

Узлы могут взаимодействовать от начального узла, с целью передачи сообщения, к узлу назначения посредством несколько сетевых переходов.

Для данной функции маршрутизации каждому узлу в сети присваивается сетевой адрес с целью идентификации а также определения его местоположения в сети. Совокупность адресов в сети именуется адресным пространством сети.

Виды и классификация телекоммуникационных систем связи.

Нынешние телекоммуникационные системы соединяются по нескольким основным признакам.

В зависимости от технического обеспечения, которое применяется с целью передачи информации, выделяются традиционные кабельные коммуникационные системы, наиболее совершенные – оптоволоконные, а также эфирные и спутниковые.

В зависимости от назначения, различаются системы телевизионного вещания, персональной связи, а также компьютерные сети.

В зависимости от способа кодировки массива информации выделяются аналоговые каналы коммуникации а также цифровые. Завершающий тип приобрел повсеместное распространение, в то время равно как аналоговые каналы коммуникации становятся все без исключения менее востребованными в настоящий период.

Типы сетей, линий и каналов связи.

В ТВС используются сети связи — телефонные, телеграфные, телевизионные, спутниковые. В качестве линий связи используются: кабельные (простые телефонные линии связи, витая пара, коаксиальный кабель, волоконно-оптические линии связи (ВОЛС), либо световоды), радиорелейные а также радиолинии.

Из числа кабельных линий связи оптимальные показатели имеют световоды. Главные их достоинства: высокая пропускная способность (сотни мбит в секунду), обусловленная отсутствием собственных электромагнитных излучений, невысокая трудоемкость прокладки оптического кабеля

применением электромагнитных волн оптического диапазона а так же нечувствительность к внешним электромагнитным полям; искро -, взрыво - а также пожаробезопасность; высокая устойчивость к агрессивным средам; незначительная удельная масса (отношение погонной массы к полосе пропускания); разнообразные области использования.

Недостатки ВОЛС: передача сигналов осуществляется только лишь в одном направлении, подключение к световоду дополнительных ЭВМ значительно обессиливает сигнал, требуемые для световодов высокоскоростные модемы до тех пор пока еще дороги, световоды, связывающие ЭВМ, должны снабжаться преобразователями электрических сигналов в световые а также обратно.

В ТВС нашли применение следующие типы каналов связи :

• симплексные;

• полудуплексные;

• дуплексные.

Защита информации в телекоммуникационных сетях

Устранение утечки информации ориентировано на предотвращение разглашения конфиденциальной информации, несанкционированного доступа к ним. Защита информации кроме того направлена на защиту от искажения конфиденциальной информации, ее уничтожения, блокирования доступа а также подобных операций с носителей информации.

Самое большое количество угроз формируются компьютерными вирусами, которые принадлежат как традиционные файловые, загрузочные, маквирусы, вредоносные программы, так и троянские программы а также т.д.

Разрушительные действия с информацией в телекоммуникационных сетях могут осуществляться со злым замыслом а также без него.

На обстоятельствах активного формирования телекоммуникационной инфраструктуры в нашем государстве проблема защиты информации становится острее. На данный момент в проблеме стандартизации методов, а

также способов обеспечения информативной безопасности в телекоммуникационных сетях отмечается значительная интернациональная активность. В российском законодательстве этот вопрос рассматривается в Федеральном законе с 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Защита информации в телекоммуникационных сетях считается одним из основных направлений деятельности каждой организации.

Необходимо сперва определить, что под термином «телекоммуникационные сети» подразумевают совокупность технических средств, обменивающихся между собой информацией и подключенных к одной коммуникационной среде.

Существуют конкретные факторы, которые вызывают трудности защиты информации в сетях связи:

– внедрение мер защиты может быть не успевать за формированием сетей, так как они динамичны;

– сети а также связанные вместе с ними процессы раскрыты для возможных злоумышленников;

– определенные виды связи, применяемые в сетях, комфортны для прослушивания;

– в сетях применяются иностранное спецоборудование;

– существует огромное количество протоколов связи, которые применяются в сетях;

– в сетях используется спецоборудование, которое никак не предусматривает реализацию мер защиты информации;

– отсутствует политика а также общая система управления доступом к сетям связи.

В телекоммуникационных сетях защищенность информации можно обеспечить вместе с поддержкой комплекса методов, а именно: организационные, технические а также криптографические методы.

При этом следует отметить, то что данные методы подойдут к абсолютно всем системам, требующим обеспечения информационной безопасности. Организационные методы заключаются в:

– подборе персонала, допускаемого к обрабатыванию конфиденциальной информации;

– активном исследовании а также использовании нормативно-законодательной базы по обеспечению безопасности в телекоммуникационных сетях;

– организации охранного а также контрольно-пропускного режима;

– организации хранения документов а также доступа к ним;

– исключении вероятного воздействия стихийных бедствий на защищенность хранимой информации а также т.п.

Задачи нацеленные на защиту информации в телекоммуникационных сетях:

1. Осуществление непрерывного обучения штатных сотрудников;
2. Осуществление анализа угроз конфиденциальной информации а также уязвимых зон автоматизированной системы и их предотвращение;
3. Обучения работе с защитными средствами, контролю за соблюдением правил их использования;
4. Организация системы защиты данных – установка требуемого программного обеспечения, его профилактика а также обслуживание;
5. Осуществление непрерывного обучения штатных сотрудников;
6. Помощь постоянной деятельности автоматизированной системы а также создание плана восстановительных мероприятий при необходимости.
7. Создание плана действий по внезапным ситуациям;

Средства и методы защиты информации в телекоммуникационных сетях:

1. Криптографические средства.

2. Антивирусная защита станций, файловых а также почтовых сервисов, средств борьбы со спамом.

3. Межсетевой экран либо система выявления атак.

4. Средства “Прозрачного” шифрования логических дисков пользователей, которые применяются с целью хранения секретных данных.

5.Программно-аппаратное средство формирования защищенных корпоративных сетей.

6. Аппаратные средства аутентификации.

7. Средства защиты от несанкционированного доступа.

8. Программы для резервного копирования.

9. Организация разграничения доступа пользователей к секретным данным с помощью штатных механизмов защиты информации.

10. Организация разграничения доступа к операционным системам, прикладным программам, маршрутизаторам а также т. п.

11. Программные криптографические средства а также средства формирования электронной цифровой подписи с целью обмена секретными данными посредством открытые каналы связи.

12. Средства ликвидирования неприменяемых конфиденциальных данных.

Средства и методы защиты информации в телекоммуникационных сетях

Крипто графические средства.	Антивирусная защита станций, файловых а также почтовых сервисов, средств борьбы со спамом.	Межсетевой экран либо система выявления атак.	Средства “Прозрачного” шифрования логических дисков пользователей, которые применяются с целью хранения секретных данных.	Программно-аппаратное средство формирования защищенных корпоративных сетей.	Аппаратные средства аутентификации.	Средства защиты от несанкционированного доступа	и т.д.

Вывод :

Основываясь на информации, согласно статье, мы можем сделать вывод, что защита информации очень важный аспект в наше время. Рассмотрев задачи направленные на защиту информации в телекоммуникационных сетях стоит, не проявляя халатности, использовать все средства и методы защиты информации в телекоммуникационных сетях.

СПИСОК ЛИТЕРАТУРЫ

1. Ahlswede R., Cai N., Li S.R., Yeung R.W. Network information flow // IEEE Trans. Inform. Theory. — 2000. — V. 47, N 7. — P. 1204–1216.

2. Cai N., Yeung R.W. Secure network coding // IEEE Intern. Sympos. on Information Theory (ISIT’2002). Lausanne, Switzerland. June 30–July 5, 2002. — P. 323.

3. Silva D., Kschischang F. R., Koetter R. A Rank-Metric Approach to Error Control in Random Network Coding // IEEE Trans. Inform. Theory. — 2008. — V. 54, N 9. — P. 3951– 3967.

4. Fragouli C, Soljanin E. Network coding. Foundations and Trends // Networking. — 2007. — V. 2, N. 1. — P. 1–134.

5. Габидулин Э.М., Пилипчук Н.И., Колыбельников А.И., Уривский А.В., Владимиров С.М., Григорьев А.А. Сетевое кодирование // Труды МФТИ. — 2009. — Т. 1, № 2. — С. 3–28.
6. Shannon K.A. Mathematical Theory of Communications // Bell System Techn. J. — 1948. — V. 27. — P. 379–423, 623–656. Русский перевод: Шеннон К. Математическая теория связи // Работы по теории связи и кибернетике: сб. ст. – М.: ИЛ, 1963.
7. Белов Е.Б., Лось В.П. и др. Основы информационной безопасности. Учебное пособие для вузов. – М.: Горячая линия - Телеком, 2006. – 544 с.
8. Гатчин Ю.А., Климова Е.В. Ожиганов А.А. Основы информационной безопасности компьютерных систем и защиты государственной тайны: учебное пособие. - СПб: СПбГУ ИТМО, 2001. - 60 с.
9. Гатчин Ю.А., Климова Е.В. Основы информационной безопасности: учебное пособие. – СПб: СПбГУ ИТМО, 2009. – 84 с.
10. Алферов А.П., Зубов А.Ю. и др. Основы криптографии.: Гелиос АРВ, 2002. – 480 с.

Минакова Н.Н.

Алтайский государственный университет, профессор

Д.ф.м.н., профессор

minakova@asu.ru

Мансуров А.В.

Алтайский государственный университет, доцент

к.т.н, доцент

mansurov.alex@gmail.com

ИДЕНТИФИКАЦИЯ ЛИЧНОСТИ ПО РАДУЖНОЙ ОБОЛОЧКЕ ГЛАЗА С ИСПОЛЬЗОВАНИЕМ МЕТОДА ЛОКАЛЬНЫХ БИНАРНЫХ ШАБЛОНОВ

В условиях цифровой трансформации все шире применяются интеллектуальные системы. Широкий спектр интеллектуальных систем используется для задач информационной безопасности. Среди них биометрические системы распознавания личности, которые работают на основе различных признаков (рис. 1).

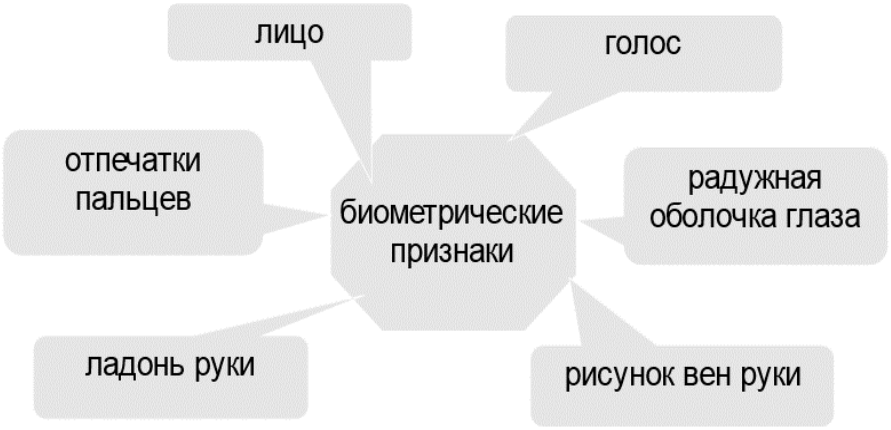


Рис. 1. Биометрические признаки идентификации личности в информационной системе

Составляющие процесса идентификации личности по биометрическому признаку во много одинаковы независимо от вида признака. Отличие, как правило, в механизмах реализации каждой стадии, которые зависят от структуры объекта [1,2].

К одному из надежных биометрических признаков относится радужная оболочка глаза (РОГ), структура которой практически не меняется в течение жизни. Для радужной оболочки глаза схему идентификации в системах контроля доступа можно представить следующим образом [3 - 5].

1. Предобработка изображения структуры.
2. Локализация.
3. Нормализация.
4. Параметризация - выделение характеристических особенностей структуры (кодов).
5. Сравнения кодов.
6. Вывод о корректной (некорректной) идентификации по результатам сравнения кодов

В условиях расширения областей применения биометрических систем защиты актуальна разработка новых методов и алгоритмов реализации указанных выше этапов распознавания личности для идентификации и контроля в системах информационной безопасности.

Этап параметризации структуры радужной оболочки глаза (способы выделения характерных признаков) во многом определяет точность и быстродействие работы биометрической системы защиты. Параметризация выполняется с помощью различных подходов. Для выделения характерных особенностей структуры используются фильтры Габора, операторы Лапласа, преобразование Эрмита, вейвлеты Хаара и т.д. [2, 3].

В работе исследуется подход к изучению структуры радужной оболочки глаза, применяемый к структурно-неоднородным средам: анализ текстурной картины [6].

Текстурная картина объекта формируется в том случае, если количество перепадов интенсивности на изображении достаточно велико. Интенсивности серых тонов (тонов другого цвета) элементов такого изображения имеют определенное статистическое распределение. Такое пространственное свойство объекта дает возможность по количественным оценкам выделить объект из ряда ему подобных. Основной количественной характеристикой текстуры служит автокорреляционная функция. Однако для разных структур экспериментально доказана эффективность других признаков [1, 3].

Радужная оболочка глаза имеет большое количество мелких деталей: коллагеновые нити, складки, области различной окраски, пятна, впадины и т.д. [2, 3]. Поэтому ее структура имеет определенную текстурную картину. Выявление характеристик взаимосвязи деталей структуры позволяет получить количественные параметры, которые могут быть использованы для классификации структур.

В работе оценивается возможность оценки структуры радужной оболочки глаза помощью метода локальных бинарных шаблонов (Local Binary Pattern или LBP) [7 - 9]. Локальный бинарный шаблон используется в компьютерном зрении для классификации текстуры полутоновых изображений [10,11]. Он сохраняет инвариантность, если яркость преобразуется в пределах порядка. Подход апробирован для распознавания лиц [12 - 14].

Расчет с использованием LBP может быть выполнен с помощью известных библиотек без специально разработанных программ.

Математическая модель вычисления локальных бинарных шаблонов согласно [7, 8]:

$$LBPp, c = \sum_{p=0}^{p-1} S(g_p - g_c)\, 2^p,$$

где C – точка, для которой вычисляется локальный бинарный шаблон; p = {0,..,P-1} – некая окрестность точки c; g_c и g_p – значения яркости в соответствующих точках; s – функция, которая возвращает 1, если значение в скобках больше нуля.

Среди методов локальных бинарных шаблонов выбран метод перечней. Алгоритм пересечений имеет следующие достоинства: не требует точного отделения объекта от фона, возможные перекрытия на переднем плане не вносят существенной ошибки в расчет. Рассматриваются окрестности пикселя изображения в двоичном представлении. Шаблон содержит информацию о соседних точках. Расчет в рамках метода пересечений выполнялся по формуле, представленной в [15]:

$$d_S\left(H_1, H_2\right) = \sum_i \min(H_1(t) \cdot H_2(t)),$$

где H_1 и H_2 – сравниваемые гистограммы; $H_1(i)$ и $H_2(i)$ – элементы соответствующих гистограмм с номером i.

Параметр ds может принимать значения от нуля до единицы. Приближение к единице соответствует уменьшению различий между гистограммами [15].

При расчетах базовый оператор локального бинарного шаблона применен для 8 пикселей окрестности. Величина интенсивности центрального пикселя является порогом при расчетах. Результат применения базового оператора – восьмиразрядный бинарный код, который включает характеристики окрестности этого пикселя [7].

Расчет выполнялся с помощью функций свободно распространяемой библиотеки opencv [16]. Рассматривались структуры радужной оболочки глаза из публично доступных баз данных CASIA-Iris.

На рис. 1 представлены результаты сравнения гистограмм изображений радужной оболочки глаза. Параметр ds метода пересечений, определяющих

степень сходства между изображениями структуры, определялся для изображений радужной оболочки глаза одного человека, полученных при разных условиях (1 на рис. 2) и разных людей (2 на рис. 2). Выполнялась статистическая обработка результатов измерений.

Эксперименты показали, что алгоритм расчета параметра d_s в рамках метода пересечений позволяет отделить характеристики радужной оболочки глаза одного человека от другого. Существенное отличие показателя d_s от единицы указывает на несовпадение гистограмм изображений по интенсивности пикселей. Для одного человека несовпадение гистограмм находится в рамах статистического разброса параметра: значение d_s близко к 1 (рис. 2).

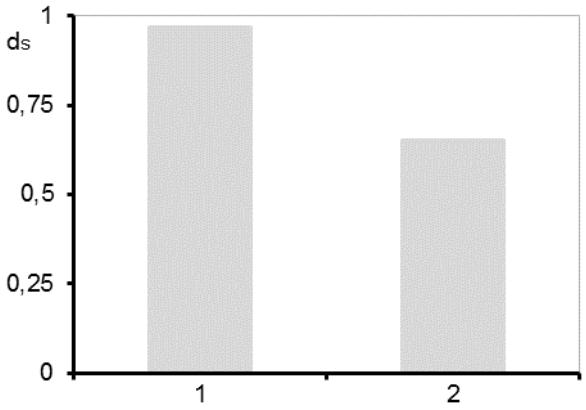


Рис. 2 Характеристики параметра d_s, определенного в рамках метода пересечений. Результаты сравнения гистограмм изображений: 1 для одного человека; 2 – для разных людей.

Таким образом, полученные результаты расчетов показали, что метод пересечений позволяет корректно классифицировать изображения структуры радужной оболочки глаза. Примененный подход, анализирующий изменение яркости на изображении, позволяет выделить характерные признаки текстуры и сравнивать по ним радужные оболочки глаза.

СПИСОК ЛИТЕРАТУРЫ

1. Кухарев, Г.А. Биометрические системы: методы и средства идентификации личности человека / Г.А. Кухарев. - С-П.:Изд-во Политехника, 2001. - 248 с.
2. Болл, Руд, Руководство по биометрии / М. Болл Руд, Х. Коннед Джонатан, Панканти Шарат, К. Ратха Налини, У. Сеньор Эндрю. – Москва: Техносфера, 2007. – 368с.
3. Минакова, Н.Н. Методы и средства защиты информации в коммерческой организации: монография / Н.Н. Минакова, В.В. Поляков, П.В. Плетнев. - Барнаул: Изд-во «Новый формат», 2016. – 158 с.
4. Минакова Н.Н., Информационная система идентификации личности по слабо различимым текстурам радужной оболочки глаза в видимом диапазоне излучения /Н.Н. Минакова., И.В. Петров // Доклады Томского государственного университета систем управления и радиоэлектроники. - 2014. - № 2 (32). - С. 105-107.
5. Третьяков И.Н. Алгоритм разграничения доступа по радужной облочке глаза для решения задач контроля доступа к информационным ресурсам /И.Н. Третьяков, Н.Н. Минакова // Доклады Томского государственного университета систем управления и радиоэлектроники. - 2010. - № 1-1 (21). - С. 100-102.
6. Минакова Н.Н. Расчетные модели прогноза свойств и анализа проводимости структурнонеоднородных композиционных материалов. /Н.Н. Минакова // Электротехника. – 2000. - № 9. - С. 26-30.

7. Shan C. Facial expression based on local binary patterns: a comprehensive study/ C. Shan, S. Gong // Image and Vision Computing. – 2009. – № 27 (6). – P. 803–816
8. Maenpaa, T. The local binary pattern approach to texture analysis – extensions and applications. – Oulu: Oulu University Press, 2003. – 80 p.
9. Фазылов Ш. Х. Биометрическая система контроля и управления доступом / Ш.Х. Фазылов, С.С. Раджабов, М.Х. Атаханов //Проблемы вычислительной и прикладной математики. – 2020. – №. 5. – С. 34-45.
10. Гонсалес, Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс. – М.: Техносфера, 2005. – 1072 с.
11. Статистический анализ данных, моделирование и исследование вероятностных закономерностей. Компьютерный подход : монография / Б. Ю. Лемешко, С. Б .Лемешко, С. Н. Постовалов, Е. В. Чимитова.— Новосибирск: Изд-во НГТУ, 2011.— 888 с.
12. Львович Я. Е. Некоторые особенности распознавания лиц //Перспективы развития технологий обработки и оборудования в машиностроении. – 2022. – С. 119-122.
13. Вахитов А. Р. Математическое и программное обеспечение идентификации личности по изображению лица //Прикладная математика и информатика: современные исследования в области естественных и технических наук. – 2020. – С. 766-770.
14. Семёнова А. П., Миненко А. С. Сравнительный анализ методов распознавания выражений лица по фотоизображениям //Информатика, управляющие системы, математическое и компьютерное моделирование (ИУСМКМ-2020). – 2020. – С. 389-393.

15. Xu M., Varshney P.K. Tighter performance bounds on image registration // Proc. IEEE Int. Conference on Acoustics Speech and Signal Processing (ICASSP 2006). – 2006. – P. 777–780.
16. .Histogram Comparison //OpenCV. URL: https://docs.opencv.org/3.4/d8/dc8/tutorial_histogram_comparison.html (дата обращения 10.09.2022).

Подъемов А. М.

ЮРГПУ(НПИ)

ЗИСа-о17 100502

Студент кафедры “Информационная безопасность”

podemov77@mail.ru

Научный руководитель:

Косиченко Н. В.

ЮРГПУ(НПИ)

Кандидат технических наук. Доцент кафедры ИБ

kosichenkov@mail.ru

«СОВЕРШЕНСТВОВАНИЕ СПОСОБОВ ОБНАРУЖЕНИЯ И ЗАЩИТЫ ОНЛАЙН АТАК НА КОМПЬЮТЕРНУЮ СЕТЬ»

Суть проблемы данной статьи сводится к совершенствованию способов обнаружения и защиты онлайн атак на компьютерную сеть. В реалиях нашего времени, прогресс любой сферы не стоит на месте. Каждая, любая компания или предприятие, стремится опережать своих конкурентов в развитии. Для этого они используют любые средства, возможности, технологии, чтобы иметь спрос на свою деятельность.

За частую конкуренты предпринимают попытки в нанесении ущерба и препятствия бесперебойной работы другой компании. Иногда люди в меру своей халатности, не уделяют должного внимания на незначительные угрозы, но как мы прекрасно знаем за маленькой проблемой следует большая.

Возьмем область “Информационной безопасности”. Любая компания которая ведет активную деятельность, с большой вероятностью использует персональные компьютеры и интернет.

Благодаря этим двум основам, любая организация имеет риск атаки на свою компьютерную сеть. В следствии успешного вторжения, будет нанесен ущерб, который за собой повлечет ряд других проблем.

Объектом исследования являются уязвимые и экономически невыгодные решения по защите сети.

Предметом исследования является схема построения сети с максимальным снижением затрат на ее реализацию.

В работе, автор, предлагает идеи, которые будут нацелены на совершенствование в предотвращение примитивных ошибок защиты и обнаружения атак на компьютерную сеть, а также будут экономически выгодны для компаний.

Многие малые организации не осознают серьезности онлайн атак. Необходимо по сегментно контролировать доступ. Также разделить серверы по функциональной роли.

Выделим 4 основные защиты от атак:

1. Межсетевой экран
2. IPS (СОВ)
3. Антивирус
4. Защита от APT (песочница)

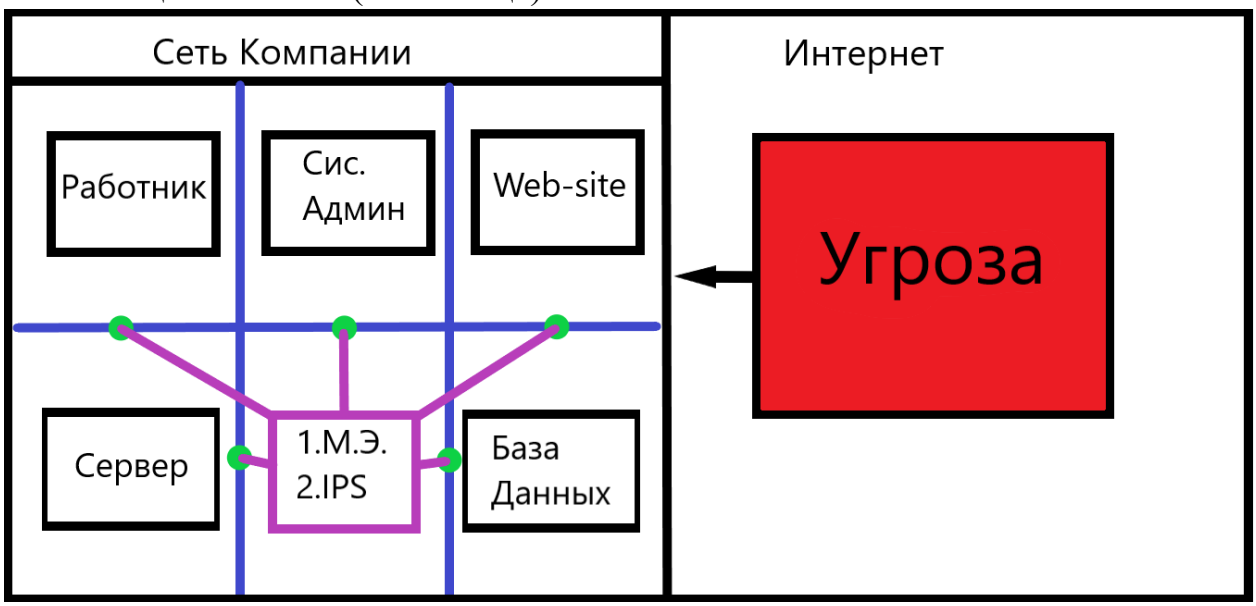


Рис. 1 Схема сети компании.

Многие компании используют по несколько межсетевых экранов для разграничения доступа к каждому сегменту, что в свою очередь оказывает финансовый удар. Это можно упростить (не теряя эффективность) с экономической выгодой. Одним межсетевым экраном, мы можем распределить информационные потоки, разделяя их разными политиками безопасности.

IPS так же как и межсетевой экран, в частности ставиться на периметре сети, но лучше ее разместить непосредственно внутри сети, для контроля информационных потоков и взаимодействия сегментов.

На рабочих местах и серверах обязательное условие – наличие Антивирусного программного обеспечения (ПО).

Самая главная проблема любой компьютерной сети – это неизвестная угроза.

Отличное решение по предотвращению угрозы данного типа – это создание Sandbox (песочниц).

В данной статье автор раскрывает актуальность и важность внедрения Sandbox.

Рассмотрение достоинств песочницы.

У песочницы много разных преимуществ при различном использовании сред. Дело в том, что использование песочницы позволяет организовать еще один уровень защиты к уже существующим решениям безопасности вшей сети. Поскольку большинство песочниц возможно запустить сразу, проведя настройку, это является большим плюсом в ее использовании. Этим обусловлена частота и актуальность применения.

Стандартные средства защиты периметра безопасности и решения могут различать и предотвращать только известные вредоносные программы и CVE, но они не справляются с новыми угрозами и уязвимостями нулевого дня.

В частности песочницы не используются в качестве защиты от угроз нулевого дня сами по себе, они могут ограничить угрозу от остальной сети. В большинстве случаев, это дает возможность анализировать и находить возможные уязвимости системы или сети. Изолируя их и вредоносное ПО, мы получаем новые данные об угрозах и атаках, которые ранее не были известны.

О других особенностях песочниц

Песочница очень хорошо действует в связке с антивирусов, так как после нахождения неизвестной угрозы, все данные об атаке будут предоставлены в реестр угроз. Это поможет в дальнейшем.

С песочницей при тестировании новейших приложений и внесении изменений в ПО, можно обнаружить любые проблемы в области, изолированной от производственной среды, и с ее помощью избежать многих проблем, которые могут возникнуть до и после её запуска.

Защита без дополнительных инвестиций

Песочницы применяются в любых отраслях: промышленности, медицине, торговле, финансовом и государственном секторе. Positive Technologies провели исследование о том, как именно компании используют песочницы. По его результатам, с их помощью:

- 64% респондентов проверяют файлы из интернета
- 57% проводят ручные проверки файлов
- 54% защищают электронную почту.

Новизна научной работы заключается в переосмыслении структурной схемы защиты сети в целях экономической выгоды и повышение значимости в использовании Sandbox.

Защита от целевых атак без увеличения бюджета

Обычно для эффективной защиты от целевых атак компании необходима мощная служба ИТ-безопасности, что зачастую требует увеличения штата ИБ-департамента и затрат на его содержание. Песочница же позволяет бороться со сложными комплексными угрозами без привлечения дополнительных специалистов и будет выгодна как для крупных компаний, так и для сегмента СМБ.

Опыт Softline в реализации ИБ-проектов показывает, что иногда для обеспечения информационной безопасности компании необходимо не одно, а несколько решений от разных производителей. Песочница защищает от целевых и массовых атак с применением вредоносного ПО. Однако для всесторонней защиты могут потребоваться как решения для обеспечения безопасности сетевого периметра, удаленного доступа и взаимодействия с ресурсами сети Интернет, так и агентские продукты для обеспечения безопасности рабочих станций. Дополняя друг друга, они обеспечат должный уровень защиты бизнеса от угроз в соответствии с концепцией построения эшелонированной системы безопасности.

Большинство коммерческих систем динамического анализа объектов построены по схожей схеме.

1. Файлы, поступающие на анализ, попадают в очередь на проверку.
2. Приложение, отвечающее за безопасность, вместе с анализатором выполняет предварительные операции: сигнатурную, эвристическую и иные проверки. Проверка объекта в виртуальной машине (ВМ) сама по себе не выгодна, по времени и ресурсам. В итоге определяется, нужно ли отправлять образец на анализ в песочницу, и конкретные параметры виртуальной машины (включая версию и разрядность ОС), а также метод анализа объекта.
3. Объект помещается в ВМ и исполняется. В ВМ нет никакого специализированного ПО — только стандартный набор программ обычного офисного сотрудника типичной компании; также имеется доступ в интернет (выявить сетевую активность угроз).

4. Все действия исследуемой программы внутри ВМ через гипервизор попадают в анализатор, который должен понять, происходит что-то вредоносное или нет, опираясь на вшитые в него шаблоны поведения.
5. Контекст и результаты анализа заносятся в базу данных для хранения, дальнейшего использования и обучения анализатора. Отсюда становится ясной основная фишка автоматизированных систем анализа объектов. Они действуют за областью виртуальной машины — на стороне гипервизора — и анализируют всю поступающую на него информацию. Именно поэтому вредоносной программе нецелесообразно искать специальные инструменты анализа на стороне ВМ.

Песочница может быть облачной, а может работать на стороне заказчика, сути это не меняет. Код запускается, его поведение отслеживается. Таким образом можно контролировать, что происходит на виртуальной машине и смотреть, какой ущерб мог нанести этот файл, если бы попал на нашу машину.

Проверка на вредоносность не должна идти первой в линии защиты. Сначала это могут быть межсетевое экранирование, антиспам, антифишинг, которые внедрены в почтовую систему, прокси-сервера, обнаружение вторжения на сетевом уровне, и только после прохождения файлом этих барьеров идет песочница – крайняя мера защиты. На этом этапе необходимо понимать, что оперативность проверки файла требует больших ресурсов, большой поток таких файлов повлечет за собой дополнительные затраты. Чтобы их сократить, необходимо сперва максимально эффективно использовать существующие средства защиты.

Вывод:

Следовательно, построение защищенной сети во главе с Песочницей – это один из лучших бюджетных методов защиты, который гарантирует, что каждый новый и неизвестный код, программа или файлы не могут свободно распространяться в используемой сети и потенциально устанавливать вредоносные программы или нарушать работу ваших служб.

СПИСОК ЛИТЕРАТУРЫ

1. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. — Рн/Д: Феникс, 2017. — 324 с.;

2. Бабаш А.В., Баранова Е.К., Ларин Д.А. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. ИСТОРИЯ ЗАЩИТЫ ИНФОРМАЦИИ В РОССИИ: Учебно-практическое пособие. - М.: Изд. центр ЕАОИ, 2012. - 736 с.;

3. Блинов А.М. Информационная безопасность: Учебное пособие. Часть 1. - СПб.: Изд-во СПбГУЭФ, 2010.-96с.;

4. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. — СПб.: Питер, 2012. — 960 с.: ил. ISBN 978-5-459-00342-0;

5. Фороузан, Б. А. Криптография и безопасность сетей : учеб.пособие / Б. А. Фороузан; пер. с англ. под ред. А. Н. Берлина. - М.:Интернет - ун-т информ. технологий : Бином, 2010. - 783 с.

6. Солонская, О. И. Алгоритмы и методика защиты пользовательской информации в мультисервисных сетях связи:дис канд. техн. наук :05.13.19 / О. И. Солонская. - Новосибирск, 2010. - 22 с.;

7. Петренко С.А., Курбатов В.А. Политики информационной безопасности / С. А. Петренко, В. А. Курбатов — М.: Компания АйТи, 20 0. — с.: ил. — (Информационные технологии для инженеров) ISBN 5-98453-024-4 SBN 5-98453-024-4 © С.А. Петренко, В.А. Курбатов © Компания АйТи, 2010 Издание ДМК Пресс, 2010;

8. Горбатов В.С., Полянская О.Ю. Г67 Основы технологии PKI. - М.: Горячая линия - Телеком, 2004. - 248 с.: ил. ISBN 5-93517-154-6.;

9. Олифер В., Олифер Н. 0-54 Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. — СПб.: Питер, 2016. — 992 с.: ил. — (Серия «Учебник для вузов»). ISBN 978-5-496-01967-5;

10. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. — СПб.: Питер, 2012. — 960 с.: ил. ISBN 978-5-459-00342-0;

Рудаков И.А
Студент МТУСИ
rudakov.ivan.ib@gmail.com

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЛИЧНОСТИ: ЗАЩИТА ДАННЫХ ЦИФРОВОГО ПРОФИЛЯ И ЦИФРОВОЙ РЕПУТАЦИИ

Пандемия 2020 года способствовала небывало быстрому погружению человека в новую цифровую реальность. После COVID-19 люди стали более зависимыми от социальных сетей со своими устройствами, чтобы развлекать себя, получать новости, а также пользоваться услугами, которые приобрели цифровую форму.

С огромным количеством информационных блогах, дискуссионными форумами и социальными сетями, Интернет в своей версии 2.0 является не просто замечательной витриной, инструментом для самовыражения, но и особым каналом для создания шума, который может создать или сломать репутацию человека.

Таким образом, идеология массовой, «ковровой» цифровизации», в ускоренном темпе, в том её виде, в каком она продвигается энтузиастами и проповедниками «цифры», представляет собой не только попытку легитимации происходящего в этой сфере, но и самостоятельную угрозу гражданскому и конституционному сознанию нашего общества.[1]

В июле 2019 года в российскую Госдуму был внесен законопроект о создании цифрового профиля гражданина.[2]

Цифровой профиль является совокупностью сведений о гражданах и юридических лицах, содержащихся в информационных системах государственных органов, органов местного самоуправления и организаций, осуществляющих в соответствии с федеральными законами отдельные

публичные полномочия, а также в единой системе идентификации и аутентификации. В законопроекте говорится, что

Социальный рейтинг – это система социальной оценки отдельных граждан по различным личным параметрам, значения которых получаются с помощью инструментов массового наблюдения, использующих технологию анализа больших данных; такая система автоматических оценок предполагает наделение граждан теми или иными правами или поражение в правах в зависимости уровня в рейтинге.

Формирование цифровой идентичности является вопросом личной, общественной и национальной безопасности! Человеку необходимо учиться формировать свою цифровую идентичность.

Риски

При таком большом объеме цифровизации и при недостаточной конфиденциальности данных, появляется огромный вектор атак на цифровую репутацию человека.

Уже сейчас при трудоустройстве в крупные компании будущие сотрудники заполняют анкеты для службы безопасности, которые в дальнейшем и проверяю все ваши цифровые следы, с целью минимизации риска причинения ущерба организации после приема на работу. О вас узнают буквально все, так еще и узнают о ваших ближайших родственниках. И все это влияет на решение о принятии вас на работу. И в случае обнаружения какой-либо негативной информации вы рискуете остаться на работе.

Система социального кредита» анализирует персональные данные жителей Поднебесной на предмет соблюдения законодательства и своевременности внесения обязательных платежей. Конечный итог анализа — присвоение баллов, которые будут учитываться при сумме возможного кредита, доступности медицинских услуг, возможности выезда за границу,

обучения в высших учебных заведениях и трудоустройства в государственные органы.[3]

Вы можете не иметь особых связей в интернете, но ваши родственники могут влиять на вашу цифровую репутацию. Мы всегда находим друзей по своим интересам, схожим политическим взглядам. И рейтинг вашего друга будет влиять, хоть и не так значительно, но и на ваш рейтинг.

В России создали нейросеть, способную оценивать тональность комментариев в соцсетях. Её назвали «Ольгой Станиславовной».[4] А раз можно оценить тональность то можно и оценить характер сообщений человека. И на основе этого сделать определенные выводы о человеке.

Прогресс цифровизации пришел и в учебные заведения. Теперь у ребенка в школе есть свой цифровой профиль (Рис.1). Где есть рейтинги в классе. И если ваш ребенок будет иметь низкий рейтинг, то в ваш цифровой профиль очень легко поставить заметку о том, что вы, как родитель, не уделяете должное внимание своему ребенку. При этом это создаст продвижения вам неких услуг, например репетиторства.

Рис.1 - Рейтинг ребенка в приложении Школьный портал.

Прогнозирование будущих вызовов нашей цифровой репутации

К чему же нас придет нас вся эта цифровизация и цифровая репутация?

Цифровая репутация окажет огромное влияние в будущем на то возьмут ли вас на работу в ту или иную компанию, доверят ли вам руководящие должности, дадут ли визу, кредит или ипотеку. Компании при трудоустройстве в описании вакансии будут просить определенную репутацию, цифровую репутацию.

Технология Face Pay появится не только в транспорте, но в магазинах для оплаты продуктов.

Fase ID не только на входе в метро, но и учебных заведениях, больницах, на проходной на работе граждан. Появится цифровая репутация у каждого работника любой организации. И взлом систем хранящих сведения о нас всегда добавляет новых рисков каждому гражданину.

До сих пор видео Deepfake[1] использовались в политических целях, но они все чаще используются для шантажа и мошенничества. Например, генеральный директор британской энергетической фирмы был обманут на 243 000 долларов голосом Deepfake главы его материнской компании с просьбой об экстренном переводе средств.[5] Кроме того, порнографические видеоролики Deepfake также использовались для шантажа женщин-репортеров и журналистов, таких как Рана Айюб в Индии, которая разоблачает злоупотребления властью.

А что дальше? Будем искать новых друзей оценивая их рейтинг, а не качества человека, и его богатый внутренний мир? Будем выбирать чиновников, президентов только по их цифровой репутации?

[1] Deep-fake – подделка изображения, видео, речи или документа с помощью нейронных сетей, позволяющая изготавливать неотличимые от реальности фальшивки. Например, изготовить видеоролик с известным политиком, где он говорит то, чего никогда не говорил, или подделать запись телефонного разговора.

По сути введение этого цифрового рейтинга ведет к еще большему влиянию на экономическую составляющую жизни человека, что способствует покупке той самой цифровой репутации человека.

Заключение

Ценность репутации не совсем нова для онлайн-мира. По мере того, как дни идут, и мы обращаемся к нашим электронным устройствам, чтобы справиться с превратностями новой нормальности, социальные и онлайн-СМИ не только усилят существующие проблемы конфиденциальности и репутации, но и создадут новые.

По своей сути цифровая репутация является аморфной концепцией. Он текучий и динамичный, и у каждого есть своя интерпретация того, что для них значит цифровая репутация.

Двигаясь вперед, важность экономики цифровой репутации станет еще более ценной, особенно с появлением Deepfakes и IoT. Это будет означать, что нам, как ненасытным потребителям контента, нужно будет научиться находить тонкий баланс между конфиденциальностью и кибербезопасностью.

Так же как раньше мы учились читать и писать, так сегодня мы должны учиться формировать свою цифровую идентичность.

Как защитить свою цифровую репутацию

1. Помните, что ваша цифровая репутация также связана с вашей личной репутацией. Все, что размещено в интернете, остается в интернете, включая суровые и радикальные суждения. Это может привести к неприятным объяснениям на рабочем месте или во время процессов найма.

2. Чтобы защитить свою цифровую репутацию, лучше быть более осторожным, чем раскрывать личную информацию о себе, особенно в социальных профилях. Никогда не разглашайте слишком много, придерживайтесь основ и делитесь только тем, что необходимо и нужно. Чем больше ваша доля, тем более привлекательным вы являетесь для

злоумышленника, который хочет украсть ваши личные данные или даже вашу личность.

3. Удаление учетных записей и данных — у всех нас есть десятки учетных записей, многие из которых едва используются или забываются. Многие из них сохраняются, и любой из них может слить вашу информацию.

4. Предотвращение злоупотребления личными данными - если приложения запрашивают конфиденциальные данные, взгляните на его политику конфиденциальности, в которой может открыто говорить, что ваши данные будут переданы сторонним компаниям. Не давайте приложениям больше информации, чем необходимо — тщательно подумайте о том, что им действительно нужно и без чего они могут обойтись. Помните, что любая информация, которую вы передаете приложениям, вряд ли останется полностью конфиденциальной.

5. Комбинированное решение продуктов безопасности и практических шагов может свести к минимуму угрозы и обеспечить безопасность ваших данных в Интернете.[6]

СПИСОК ЛИТЕРАТУРЫ

1. Доклад Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека- Цифровая трансформация и защита прав граждан в цифровом пространстве. Москва 2021г. [Электронный ресурс] //URL: https://ifap.ru/pr/2021/n211213a.pdf

2. Проект ФЕДЕРАЛЬНЫЙ ЗАКОН О внесении изменений в отдельные законодательные акты (в части уточнения процедур идентификации и аутентификации) [Электронный ресурс] //URL: https://sozd.duma.gov.ru/bill/747513-7

3. Цифровой профиль гражданина: перспективы внедрения систем удаленной идентификации - [Электронный ресурс] //URL:

https://drc.law/blog/tsifrovoy-profil-grazhdanina-perspektivy-vnedreniya-sistem-udalennoy-identifikatsii/

4. В России родилась «Ольга Станиславовна» — нейросеть для мониторинга комментариев [Электронный ресурс] //URL: https://ib-bank.ru/bisjournal/news/17676

5. Мошенники выманили у директора британской компании 243 тыс. долларов, подделав голос его немецкого руководителя. [Электронный ресурс] //URL: https://www.newsru.com/hitech/04sep2019/fake_voice.html

6. Осмысление нашего места в экономике цифровой репутации [Электронный ресурс] //URL: https://www.kaspersky.com/blog/digital-reputation-economy-report/

7. Жарова, А. К. Правовое обеспечение цифрового профилирования деятельности человека / А. К. Жарова // Вестник ЮУрГУ. Серия «Право». – 2020. – Т. 20, № 2. – С. 80–87. DOI: 10.14529/law200214

8. Мочалов А. Н. Цифровой профиль: основные риски для конституционных прав человека в условиях правовой неопределенности // Lex russica. — 2021. — Т. 74. — № 9. — С. 88–101. — DOI: 10.17803/1729-5920.2021.178.9.088-101.

9. Жарова А. К. Вопросы обеспечения безопасности цифрового профиля человека // Юрист. — 2020. — № 3. — С. 55–61.

10. Петров А. А. Китайский цифровой профиль или скоринговая система социального доверия // Chronos. — 2020. — № 8. — С. 11–24.

11. Зотов В.В. Демаркация публичного и приватного при взаимодействии государства и граждан на цифровых сетевых платформах//Цифровая социология. 2021. Т. 4, № 3. С. 16–26.

Селиверстов В.В.
СГТУ им. Гагарина, аспирант
Информатика и вычислительная техника, 2 курс
seliverstov_vitaly@mail.ru
Научный руководитель:
Корчагин С.А.
к.ф.-м.н., СГТУ им. Гагарина, доцент,
Финансовый университет при Правительстве Российской Федерации, доцент
korchaginser@gmail.com

ТРЕБОВАНИЯ К ЗАЩИТЕ ПРИЛОЖЕНИЙ, ОСНОВАННЫХ НА ТЕХНОЛОГИИ КОНТЕЙНЕРИЗАЦИИ

Контейнеризация стремительно повлияла на структуру современных приложений. Сочетание технологий Kubernetes и Docker зарекомендовало себя как решение для удовлетворения технических и бизнес-требований. Однако за такими изменениями последовал и целый ряд проблем в области информационной безопасности. Внедрение новых технологий всегда чревато ошибками и уязвимостями. Для защиты облачно-ориентированных технологий понадобились новые методики и инструменты [1].

Проанализировав известные инциденты с нарушением информационной безопасности, можно выделить следующие факторы уязвимостей контейнеризации: локальные уязвимости компонентов, сетевой трафик и человеческий фактор [2].

Эффективным инструментом выстраивания защиты для анализа возможных проблем, является, модель угроз (Рис 1).

Из модели угроз следует, что изначальный уровень конфигурации контейнеров чрезвычайно низок. Защита зависит от окружающей инфраструктуры, встроенных компонентов и конфигураций в runtime [3].

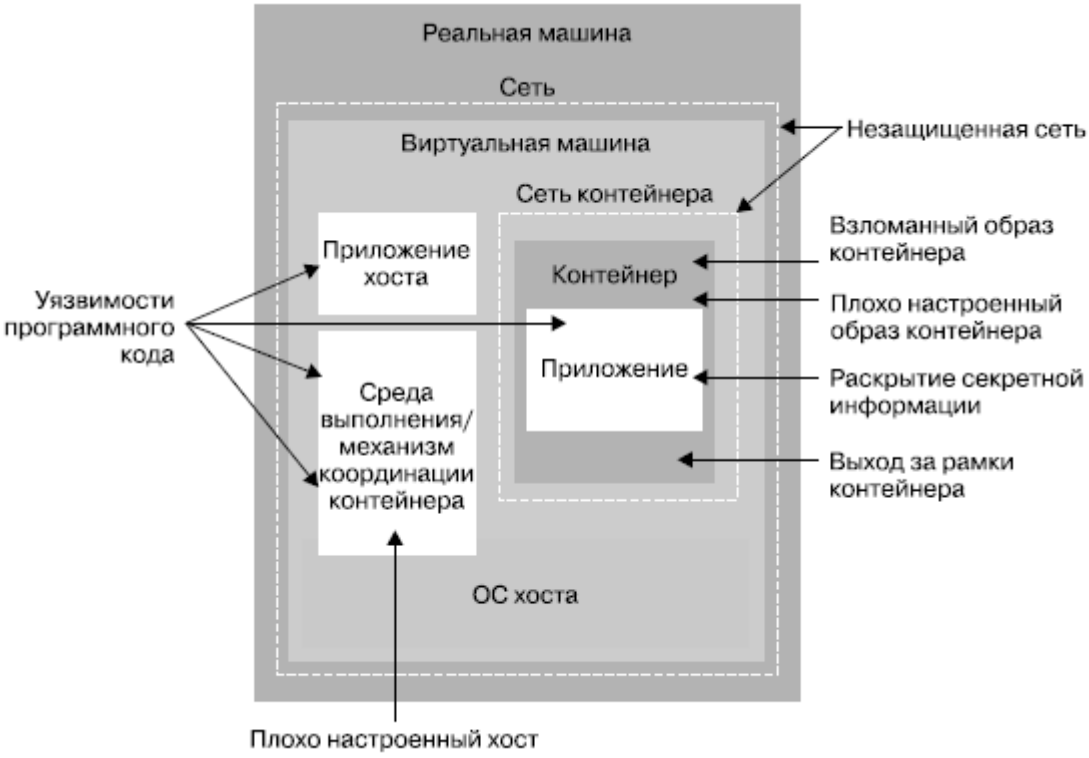


Рис. 1. Концептуальная модель угроз контейнеров

Требования безопасности для конфигурации контейнеров

Проблема №1: **повышение прав пользователя.**

Одна из основных форм неправильного конфигурирования в Docker связана с повышением прав пользователя. Практически все процессы в контейнере функционируют из-под root пользователя *(id =0)*, если конкретным способом его не указать. Такой вид настройки кажется весьма удобным, ведь у пользователя нет ограничений. Однако работать под root пользователем максимально некорректно с точки зрения безопасности. Существует целый ряд уязвимостей, который может позволить выбраться за контур контейнера и попасть в host-систему [4].

Требования.

Технология Docker поддерживает работу в режиме пользователя (*rootless/non-root)*, что позволяет значительно повысить уровень безопасности.

Для обеспечения принципа наименьших привилегий необходимо корректно сконфигурировать пользователя. Данный принцип достигается следующими способами:

- Указать конкретный идентификатор пользователя, которого нет в контейнере: *docker run -u 9999 <image>;*
- Заранее создать пользователя в Dockerfile;
- Запретить эскалацию привилегий, указав опцию при запуске: *--security-opt=no-new-privileges*.

Проблема №2: **раскрытие учетных данных и secrets.**

Обычно для нормального функционирования ПО нужны конфиденциальные данные: пароли пользователей, сертификаты, ключи шифрования и т. д.

Содержание учетных данных и secrets внутри конфигураций – еще одна популярная ошибка при создании контейнерной инфраструктуры [5].

```
version: '3'
services:
  postgres:
    image: postgres:13.1
    container_name: postgres13.1
    restart: always
    environment:
      - POSTGRES_DATABASE=posgres
      - POSTGRES_USER=postgres
      - POSTGRES_PASSWORD=root
    ports:
      - '5432:5432'
    volumes:
      - db:/var/lib/postgresql/data
volumes:
  db:
    driver: local
```

Рис. 2. Конфигурирование контейнера postgres

На рисунке 2 параметры настройки контейнера Docker перечисляются в виде обычного текста, включая пароли к базе данных, пути к данным и файлам. Данная конфигурация раскрывает практически всю информацию для проникновения в базу данных.

В таких случаях необходимо проверить не только надежность хранения файлов, но и то, что любая часть автоматизированных процессов развертывания не хранит конфиденциальных данные.

Кроме того, такие технологии, как *Ansible* или *Puppet* используют файлы конфигурации, в которых может содержаться, что и где должно быть выполнено.

Данные файлы могут использоваться для автоматизации задач, которые выполняются на большом количестве серверов [6].

Требования.

Для решения подобных проблем с конфигурацией следует знать о нескольких правилах:

- Конфигурации контейнеров должны быть вынесены в *Secrets* и *ConfigMaps*;
- Необходимо исключить использование паролей, установленных в контейнерах по умолчанию;
- Необходимо использовать централизованное решения для безопасного хранения всей закрытой информации: токенов, паролей, сертификатов, учетных записей и т.д.;
- Использовать различные сканеры безопасности для выявления утечек данных в конфигурационных файлах (например, *Hadolint*).

Следует помнить, что *stateless* – важное свойство для правильного функционирования контейнеров. Без сохранения состояния означает, что любое состояние (постоянные данные любого типа) хранится вне контейнера. Это внешнее хранилище может иметь несколько форм, в зависимости от того, что требуется. Используя это свойство, контейнер можно аккуратно закрыть и уничтожить в любое время, не опасаясь потери данных. Если создается новый контейнер для замены старого, просто следует подключить новый контейнер к тому же хранилищу данных или привязать его к тому же диску [7].

Проблема №3: уязвимости в образах контейнеров

Проблемы на этом уровне чаще всего возникают на этапе сборке образов. Контейнеры — это изолированные черные ящики. Контейнер может корректно функционировать с операционной точки зрения, при этом используя уязвимое ПО.

Основные проблемы этого уровня: уязвимости базового образа и системных пакетов; уязвимости в сторонних зависимостях, которые подтягиваются извне; проблемы и уязвимости в коде самих приложений.

Требования.

Конфигурирование контейнеров в виде неизменяемых атомарных блоков системы с точки зрения архитектуры максимально обоснованно, но для обеспечения безопасности их содержимое нужно всегда проверять [8].

Для получения свежих исправлений уязвимостей, необходимо регулярно обновлять и заново собирать свои образы. Однако, не стоит обновлять работающие контейнеры. Для корректного функционирования контейнеров они должны быть *immutable*.

Immutable означает, что контейнер не будет изменяться в течение его жизни: никаких обновлений, никаких исправлений, никаких изменений конфигурации. Если необходимо обновить код приложения или применить исправление, нужно создать новый образ и повторно развертывать его. Неизменяемость делает развертывание более безопасным и повторяемым. Если нужно откатиться, вы просто переустанавливаете старый образ.

Но прежде всего, стоит правильно выбирать базовый образ при выполнении команды – *docker pull image*. Всегда нужно эксплуатировать проверенный образ, предпочтительно из хранилища *Docker Official Images*, чтобы не допустить атаки на цепочки поставок (*supply-chain attacks*).

Хорошей практикой является использование отдельного программного обеспечения, которое регулярно получает обновления безопасности для установленных контейнеров.

Так же нужно обязательно помнить, что теги Docker работают от менее специфичных к более специфичным:

```
postgres: latest,

postgres: 14.5

postgres: 14.5-alpine

postgres: alpine
```

Рис. 3. Разновидность тегов Docker

Например, на рисунке 3 перечисленные теги относятся к одному и тому же образу. Если указывать и фиксировать более конкретную версию, можно получить защиту от будущих критических изменений (*breaking change*). С обратной стороны, эксплуатация последней версии гарантирует исправление свежих уязвимостей. Тут следует найти компромисс, однако хорошей практикой является привязка к стабильной версии.

Кроме того, необходимо использовать инструменты сканирования образов для поиска уязвимостей (например, *Quay*). Хорошим тоном является настройка сканирования безопасности обязательным этапом *CI/CD*-цепочки при разработке [9].

Проблема №4: незащищенное взаимодействие между контейнерами

Базовая сетевая модель контейнера *docker0* уязвима перед атаками типа *ARP-spoofing* и *MAC-flooding*. Это автоматически создаваемый сетевой мост, обычно использующийся для изоляции сети хоста от сети контейнера.

Контейнерам Docker требуется сетевой уровень для связи с внешним миром через сетевые интерфейсы на хосте. Сеть моста по умолчанию существует на всех хостах Docker — если не указать другую сеть, к ней автоматически подключатся новые контейнеры.

Требования.

Настоятельно рекомендуется не полагаться на сеть мостов по умолчанию. Необходимо использовать настраиваемые сети мостов, чтобы контролировать, какие контейнеры могут взаимодействовать между собой, и включать автоматическое преобразование DNS от имени контейнера к IP-адресу.

Еще одно решение – использовать технологию *Service mesh*, в данном случае *Istio. Service mesh* является сетью постоянных зашифрованных соединений с максимально производительными прокси-серверами вроде *Envoy* и *Linkerd*.

Istio – это настраиваемая оболочка для управления и конфигурации различного рода взаимодействия между сервисами. Так, например, данная технология отвечает за следующие операции: шифрование, маршрутизация, аутентификация, авторизация, трассировка, контроль доступа и многое другое.

Существует огромное количество готовых библиотек, которые могут реализовать эти функции непосредственно в коде сервиса. Однако с Istio достигается sidecar эффект и сам сервис остается без изменений [10].

Заключение

Переход на контейнерные приложения, которые используются повсеместно в организациях для обеспечения более простого управления, быстрого развертывания и эффективного масштабирования приложений, порождает определенные проблемы безопасности.

Приведенные в статье эксплуатируемые способы решения проблем, в большинстве случаев, помогают обеспечивать требования безопасности. Однако не стоит забыть о постоянном мониторинге современных тенденций и лучших практик.

Одна из лучших практик в этой области - быстрое поступательное улучшение безопасности. Данная практика достигается с подходом

Continuous Security, помогающий максимально оперативно находить и устранять вновь появляющиеся уязвимости и угрозы.

СПИСОК ЛИТЕРАТУРЫ

1. Combe T., Martin A., Di Pietro R. To docker or not to docker: A security perspective //IEEE Cloud Computing. – 2016. – Т. 3. – №. 5. – С. 54-62.
2. Brady K. et al. Docker container security in cloud computing //2020 10th Annual Computing and Communication Workshop and Conference (CCWC). – IEEE, 2020. – С. 0975-0980.
3. Manu A. R. et al. Docker container security via heuristics-based multilateral security-conceptual and pragmatic study //2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT). – IEEE, 2016. – С. 1-14.
4. MP A. R. et al. Enhancing security of docker using linux hardening techniques //2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT). – IEEE, 2016. – С. 94-99.
5. Manu A. R. et al. A study, analysis and deep dive on cloud PAAS security in terms of Docker container security //2016 international conference on circuit, power and computing technologies (ICCPCT). – IEEE, 2016. – С. 1-13.
6. Huang D. Et al. Security analysis and threats detection techniques on docker container //2019 IEEE 5th International Conference on Computer and Communications (ICCC). – IEEE, 2019. – С. 1214-1220.
7. Bacis E. et al. DockerPolicyModules: mandatory access control for docker containers //2015 IEEE Conference on Communications and Network Security (CNS). – IEEE, 2015. – С. 749-750.
8. Perrone G., Romano S. P. The docker security playground: A hands-on approach to the study of network security //2017 Principles, Systems and Applications of IP Telecommunications (IPTComm). – IEEE, 2017. – С. 1-8.

9. Loukidis-Andreou F. et al. Docker-sec: A fully automated container security enhancement mechanism //2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS). – IEEE, 2018. – С. 1561-1564.
10. Tomar A. et al. Docker security: A threat model, attack taxonomy and real-time attack scenario of dos //2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence). – IEEE, 2020. – С. 150-155.

Сиротский А.А.
ФГБОУ ВО НИУ МГСУ, доцент,
К.т.н., доцент,
Hotwater2009@yandex.ru

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ИЗМЕНЕНИЯ В ПРОЦЕССАХ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В СВЯЗИ С ИЗМЕНЕНИЯМИ ЗАКОНОДАТЕЛЬСТВА, ВСТУПАЮЩИМИ В СИЛУ С 1 СЕНТЯБРЯ 2022 ГОДА

6 июля 2022 года Государственной Думой РФ был окончательно принят Федеральный закон № 266-ФЗ "О внесении изменений в Федеральный закон "О персональных данных", отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона "О банках и банковской деятельности", который был официально опубликован 14 июля 2022 г.

Часть новых положений, устанавливаемых, и впервые вводимых данным законом, вступают в силу с 1 сентября 2022 года, а часть – с 1 марта 2023 года.

Поводом к принятию новых норм и положений в области защиты персональных данных стал анализ инцидентов последних лет, когда персональные данные граждан массово попадали в открытый доступ [1]. Риски несанкционированного распространения конфиденциальной информации увеличиваются в связи с развитием информационных сервисов в цифровой экономике [2].

Вопросы обеспечения персональной безопасности личности за последние годы только повышают свою актуальность и могут рассматриваться в различных концептуальных проблемах делового оборота

[3, 4]. Принятие новых норм направлено на повышение безопасности личности в современной информационной среде [5].

Новые законодательные нормы значительно усиливают государственный контроль за оборотом персональных данных, вводя ряд новых обязанностей для операторов персональных данных, заключающиеся прежде всего в необходимости непрерывного взаимодействия с государственными органами власти и уполномоченными структурами.

Всё это повлечёт необходимость в организациях-операторах персональных данных пересмотреть действующие процессы и внести коррективы в модели функционирования систем обеспечения информационной безопасности, приведя их к соответствию новым нормативным требованиям. Вполне вероятно, это потребует от операторов персональных данных провести внеочередной аудит безопасности своей инфраструктуры и бизнес-процессов [6].

По сравнению с законодательными требованиями и практикой защиты персональных данных в коммуникативной среде прошлого периода [7, 8], в настоящее время на операторов персональных данных накладываются гораздо большие обязанности и гораздо более высокая ответственность.

В данной работе проведём анализ некоторых наиболее принципиальных изменений законодательных требований к обработке персональных данных, вступающих в силу с 1 сентября 2022 года, и которые влекут за собой существенные изменения процессов обработки персональных данных в организациях, потребуют произвести корректировку и расширение применяемых операторами мер и средств обеспечения защищённости персональных данных.

Изменение 1.

Дополнена статья 11 Федерального Закона №152 «О персональных данных».

Ранее ситуация, когда организация (оператор) требовала от клиента дать согласие на обработку биометрических персональных данных, оставалась не до конца определённой. Хотя при этом, биометрические данные в большинстве случаев не являются необходимыми для установления деловых отношений между Оператором и субъектом (клиентом), выполнения работ и услуг.

Теперь, за исключением отдельных случаев, предоставление биометрических персональных данных не может быть обязательным. Закрепляется, что оператор не вправе отказывать в обслуживании в случае отказа субъекта персональных данных предоставить биометрические персональные данные и (или) дать согласие на обработку персональных данных, если в соответствии с федеральным законом получение оператором согласия на обработку персональных данных не является обязательным.

Таким образом, обособленно разграничивается категория биометрических персональных данных, уязвимость которых может иметь наиболее неблагоприятные последствия. Также однозначно определяется, что требование предоставления биометрических данных должно быть законодательно обосновано.

Изменение 2.

Дополнена сразу тремя пунктами, 12, 13 и 14 статья 19 Федерального Закона №152 «О персональных данных».

Ранее операторы персональных данных не были обязаны взаимодействовать с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГОССОПКА). В предыдущей редакции закона ГОССОПКА не упоминалась вообще. Взаимодействие с данной системой предусматривалось только для объектов критической информационной инфраструктуры (КИИ), что регламентируется другим законодательством.

Теперь операторам персональных данных будет необходимо наладить взаимодействие с системой ГОССОПКА и информировать о компьютерных инцидентах, повлекших нарушение режима конфиденциальности обработки персональных данных.

Таким образом, вводится совершенно новая процедура, которую предстоит освоить операторам персональных данных. В настоящий момент ожидается выход соответствующих регламентирующих документов, которые определят порядок взаимодействия операторов с системой ГОССОПКА.

Изменение 3.

Изменена статья 20 Федерального Закона №152 «О персональных данных».

Статья 20 Федерального Закона №152 «О персональных данных» устанавливала регламентные сроки реагирования оператора при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных.

Ранее по большинству обращений оператору отводился срок на подготовку ответа 30 дней. Теперь этот срок снижен до 10 рабочих дней с возможностью мотивированного продления ещё на 5 рабочих дней, т.е. максимально до 15 рабочих дней. Закреплена также возможность обращения субъекта с требованием о прекращении обработки персональных данных (Табл. 1).

Табл. 1. Сроки реагирования оператора на обращения

Источник обращения	**Повод обращения**	**Срок рассмотрения**	
		Было (до 01.09.2022)	**Стало (с 01.09.2022)**
Субъект	Ознакомление со своими персональными данными	30 дней	10 рабочих дней (+ 5 дней продление)
Субъект	Мотивированный отказ в предоставлении сведений	30 дней	10 рабочих дней (+ 5 дней продление)
Уполномоченный орган	Запрос	30 дней	10 рабочих дней (+ 5 дней продление)
Субъект	Требование прекратить обработку	Не определялось	10 рабочих дней (+ 5 дней продление)

Таким образом, срок ответов по всем штатным вопросам и обращениям снижается с 30 дней до максимум 15 рабочих дней.

Изменение 4.

Дополнена пунктом 3-1 статья 20 Федерального Закона №152 «О персональных данных».

Ранее оператор не был обязан сообщать о произошедших инцидентах, нарушивших безопасность персональных данных.

Теперь вводится новая процедура, предусматривающая обязательное уведомление уполномоченный орган по защите персональных данных как о

самих произошедших инцидентах, так и о результатах их внутреннего расследования. Кроме того, установлены очень жёсткие сроки для этого:

– 24 часа отводится на информирование о факте возникшего инцидента;

– 72 часа отводится на информирование о результатах проведённой внутренней проверки и расследования.

Таким образом, оператор персональных данных должен заранее проработать регламент действий на случай возникновения инцидентов, а также определить сотрудников, на которых будут возлагаться функции по расследованию. Сами расследования должны будут проводиться крайне оперативно в считанные часы.

Изменение 5.

Сокращены основания, по которым оператор может осуществлять обработку персональных данных без обязательного уведомления уполномоченного органа, которые изложены в статье 22 Федерального Закона №152 «О персональных данных».

До настоящего времени было 9 оснований, освобождающих оператора от обязанности подавать уведомление и, соответственно, вступать в реестр операторов персональных данных.

Теперь из 9 оснований остаются в силе только три:

- при обработке персональных данных включенных в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

- персональных данных, обрабатываемых исключительно без использования средств автоматизации;

- персональных данных, обрабатываемых в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности.

Таким образом, практически любая организация теперь обязана подавать уведомление и вступать в реестр операторов персональных данных.

Для рядовой коммерческой компании малого бизнеса, деятельность которых ориентировано на сектор массового потребления товаров или услуг, и не связанных ни с государственными информационными системами, ни с транспортной безопасностью, единственным основанием, чтобы не вступать в реестр, фактически остаётся переход на неавтоматизированную обработку персональных данных [9].

Автор данной статьи является разработчиком и спикером программы повышения квалификации «Защита персональных данных в организации», проводимой Институтом цифровых компетенций Финансового Университета при Правительстве РФ [10]. Также следует отметить, что одной из наиболее актуальных задач в настоящий период является не только подготовка специалистов по защите персональных данных, владеющих организационно-управленческим и аналитическим мышлением, но также и донесение знаний и пониманий важности осмысленного отношения к своим персональным данным до широких слоёв граждан, формирование культуры обращения с персональными данными и обеспечения персональной безопасности личности в информационной среде.

СПИСОК ЛИТЕРАТУРЫ

1. Иванова, А.П. Утечка персональных данных: большая проблема в цифровую эпоху. / А.П. Иванова // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Серия 4: Государство и право. – 2020. – №4. – с. 100 – 107.
2. Сиротский, А.А. Тенденции развития информационных сервисов в структуре цифровой экономики / А.А. Сиротский, А.Э. Самадуров // Сборник докладов XI Международной конференции "Современные информационные технологии в образовании, науке и промышленности", 3 ноября 2018 г., Региональное отделение международной академии информатизации, Факультет информационных технологий ФГБОУ ВО РГСУ. – 2018. – с. 169 – 172.

3. Сиротский, А.А. О некоторых угрозах безопасности персональной информации в современных условиях. / А.А. Сиротский // Социальное образование в условиях интеграции России в мировое образовательное пространство. Сборник материалов XII Всероссийского социально-педагогического конгресса. Министерство образования и науки РФ, Российский государственный социальный университет, Институт культурологии образования Российской академии образования. – 2012, – с. 247 – 252.

4. Сиротский, А.А. Личность – как объект информационных угроз в современном обществе / А.А. Сиротский // Информационная безопасность бизнеса и общества. Сборник избранных статей научно-педагогического состава кафедры информационных систем, сетей и безопасности. Российский Государственный Социальный Университет. – М.: Издательство «Перо», 2016. – 111 с. – с. 23 – 27.

5. Сиротский, А.А. Информационные и методические проблемы информационной безопасности личности в современном деловом обороте / А.А. Сиротский // «Системы безопасности – 2015». Материалы 24-й международной научно-технической конференции (26 ноября 2015 г, Москва). – М.: Академия ГПС МЧС России, 2015. – 482 с. – с. 104 – 107.

6. Сиротский, А.А. Формализованная модель аудита информационной безопасности организации на предмет соответствия требованиям стандартов. / А.А. Сиротский, С.А. Резниченко // Безопасность информационных технологий, [S.l.], т. 28. – 2021. – № 3, – с. 103–117.

7. Сиротский, А.А. Информационная безопасность личности и защита персональных данных в современной коммуникативной среде. / А.А. Сиротский // Технологии техносферной безопасности. Научный интернет-журнал. – 2013. – Выпуск 4(50). – с. 3 – 10.

8. Гнедков, А.В. Особенности распространения персональных данных в последней редакции законодательства о персональных данных / А.В. Гнедков, А.В. Нищик //Научно-методическое обеспечение оценки качества образования. – 2022. – № 1(15). – с. 49 – 52.

9. Грибанов, А.А. Определение персональных данных, разграничение операторов и обработчиков персональных данных / А.А. Грибанов // Судья. – 2021. – №4(124). – с. 30 – 34.

10. Сиротский, А.А. Опыт участия в программе «Персональные цифровые сертификаты 2020» в качестве разработчика и преподавателя курса по защите персональных данных / А.А. Сиротский // Преподавание информационных технологий в российской федерации. Сборник научных трудов Девятнадцатой открытой Всероссийской конференции. Москва, онлайн, 19-20 мая 2021. М.: ООО «1С-Паблишинг». – 2021. – 520 с. – с. 323 – 325.

Тивелев Н. А.,
Московский технический университет связи и информатики, студент
Булгакова Е. В.,
Московский технический университет связи и информатики, Доцент кафедры "Безопасность телекоммуникаций"

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В РЕШЕНИЯХ ПО ЗАЩИТЕ ИНФОРМАЦИИ ПРЕДПРИЯТИЯ И ОБЕСПЕЧЕНИЮ ЕГО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация

В докладе будет рассмотрено применение искусственного интеллекта (ИИ) для обеспечения информационной безопасности предприятия. Будут раскрыты основные понятия ИИ, описаны методы ИИ, применяемые для защиты информации. А также будет изучена необходимость его использования в современных средствах защиты.

21 век - век глобальной цифровизации. Развитие информационных технологий происходит во всех сферах жизни. Вследствие этого, каждый человек и каждая компания желают уменьшить вероятность кражи своих данных, а также любого негативного воздействия. Именно поэтому, информационная безопасность так важна в современном мире. Крупные компании интегрируют множество различных продуктов для обеспечения безопасности, однако этого бывает недостаточно. Всё это приводит к увеличению разнообразия атак на информационные системы, а в следствие и совершенствованию методов защиты от них.

Однако, с увеличением размера предприятия увеличивается количество информации, которую необходимо обрабатывать для своевременного ответа

на информационную угрозу. В крупнейших предприятиях существует огромное число сигналов, которые необходимо проанализировать для точного расчета риска. Такое количество информации может оказаться не под силу человеку. Требуются новые подходы в обеспечении информационной безопасности. Как итог, стали появляться инструменты на основе искусственного интеллекта. Они призваны увеличить защищенность информационных систем и уменьши время реагирования на различные инциденты.

Искусственный интеллект – это в первую очередь программное обеспечение, которое может понимать, учиться и действовать на основе полученной ранее информации. В контексте кибербезопасности искусственный интеллект – это программное обеспечение, способное распознавать события в информационной системе и самостоятельно реагировать на них. Его главное отличие от обычных программ – это способность самостоятельно обучаться в процессе анализа новой информации.

Есть два основных способа, которыми искусственный интеллект может помочь в информационной безопасности. Первый способ заключается в том, что искусственный интеллект помогает автоматизировать множество интеллектуально сложных задач. Это позволяет лучше распределять средства защиты. Искусственный интеллект позволяет анализировать огромные объёмы данных намного быстрее, чем это делает человек. Второй же способ заключается в способности искусственного интеллекта обнаруживать закономерности в больших объемах данных. Он может запоминать паттерны кода вредоносных файлов и распознавать их в будущем. Тем самым находя вирусы в исполняемых файлах еще до их активации.

Основные продукты информационной безопасности с использованием искусственного интеллекта:

– EDR (обнаружение и реагирование на атаки на конечных точках сети) — платформы обнаружения атак и реагирования на них на любых компьютерных. Данный продукт позволяет классифицировать и обнаруживать неизвестные ранее угрозы и самостоятельно принимать решения касательно их. Искусственный интеллект учиться определять угрозы на основе уже проанализированных данных. Также существует возможность поставить метки на файлы и проанализировать дальнейший пут файла во внутренней системе для выявления угрозы.

– NDR (обнаружения и реагирование на атаки в сети) — устройства, которые позволяют обнаружить атаки на сетевом уровне и оперативно на них реагировать. Используя накопленную базу знаний об угрозах, продукты данного типа выявляют угрозы в сетевом трафике и автоматически на них реагируют, изменяя конфигурацию сетевых устройств. Такие продукты применяют для защиты облачных сервисов. Также данные системы применяют для анализа почты на предмет фишинга.

– UEBA (анализ поведения пользователей и устройств) — системы поведенческого анализа пользователей. Данный продукт анализирует и запоминает поведение пользователя и обнаруживает отклонения, тем самым детектируя угрозы. Выявленные аномалии определяется искусственным интеллектом как угроза в системе. Аномальное поведение может обнаруживать мошенничество среди клиентов или сотрудников (антифрод), проверить соблюдение тех или иных регламентов и нормативных актов.

– TIP (платформа анализа угроз) — платформа детектирования угроз и реагирования на них. Применение искусственного интеллекта существенно повышает эффективность выявления неизвестных угроз. Данная модель похожа на SIEM-системы, но нацелена на внешние угрозы.

– SIEM (управление информацией и событий безопасности) — решения, которые в режиме реального времени анализируют события безопасности, поступающие от множества систем, и позволит эффективно

обнаруживать инциденты ИБ. В данных системах накапливается большой объём данных, что существенно уменьшает риск ложных срабатываний. Применение искусственного интеллекта в таких системах позволяет достигнуть высокого уровня автоматизации.

– SOAR (платформа оркестрации, автоматизации и реагирования на инциденты) — системы, выявляющие угрозы информационной безопасности и автоматизирующие реагирование на инциденты. Данные системы схожи с SIEM, только искусственный интеллект не только анализирует и выявляет угрозы, но также и реагирует на них надлежащим образом.

– Application Security (средства защиты приложений) — системы, позволяющие определять угрозы прикладных приложений и устраненять такие угрозы. Основной принцип работы таких систем – это сбор информации из открытых источников об угрозах, уязвимостях и заражениях, и дальнейшее автоматизированное выполнение защитных действий.

– Antifraud (антифрод-системы) — системы, позволяющие определять угрозы в бизнес-процессах и предотвращать в режиме реального времени. В таких системах технологии искусственного интеллекта применяются для нахождения отклонений от установленных процессов, тем самым помогая в кратчайшие сроки реагировать на финансовое преступление или уязвимость процессов.

Во всех этих продуктах используется множество методов искусственного интеллекта. Далее рассмотрим самые распространённые из них:

- **Противодействием угрозам.** Как уже говорилось выше, злоумышленники постоянно совершенствуются, тем самым увеличивая количество возможных атак. Для борьбы с этим предприятия используют искусственный интеллект. Он призван проанализировать большое

количество атак и просчитать, какие из них будут использованы против вашего предприятия с большей вероятностью.

- **Инвентаризация ИТ-Активов.** Искусственный интеллект может собрать информацию о всех устройствах и приложения внутри сети предприятия, для дальнейшего контроля возникновения уязвимостей.
- **Прогнозирование риска взлома.** Учитывая инвентаризацию и различные системы контроля, искусственный интеллект может просчитать слабые места системы, что позволит укрепить их безопасность.
- **Реагирование на инциденты.** Искусственный интеллект позволяет быстро отреагировать на предупреждение системы безопасности и выявить методы, для предотвращения похожих проблем в будущем

Все данные методы работают, основываясь на машинном обучении. Машинное обучение – наиболее широкий раздел искусственного интеллекта, использующий различные алгоритмы для самообучения, постепенно повышая точность. При помощи машинного обучения работает компьютерное зрение, обработка естественного языка, современные антивирусные программы и многое другое. Данный метод извлекает полезную информацию из больших объемов данных, используя алгоритмы для выявления закономерностей и обучения в процессе. Алгоритмы машинного обучения используют методы вычислений, чтобы учиться непосредственно на полученных данных, вместо заранее определенных уравнений. Точность и эффективность улучшаются с увеличением анализируемых данных.

На рисунке 1 показан метод обучения с учителем

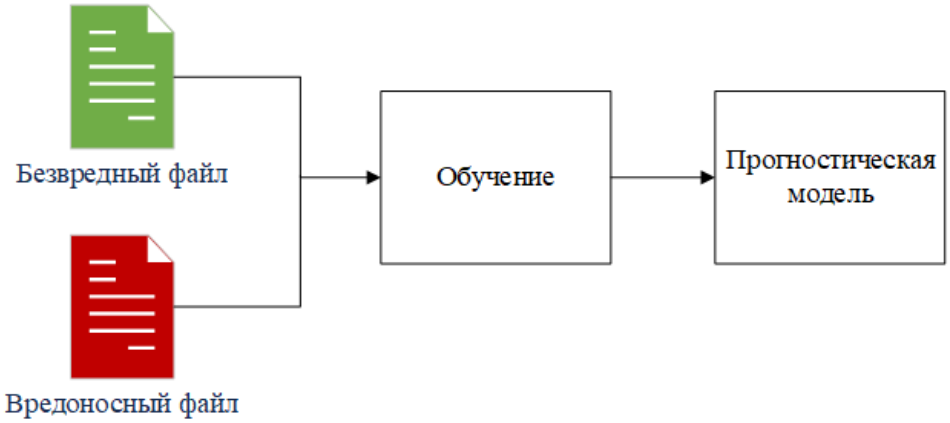


Рисунок 1. Обучения с учителем.

Данный метод включает в себя обучение на основе маркированного набора данных. В маркированном наборе уже сопоставлены входные и выходные данные, то есть машина заранее знает, какие признаки у вредоносных файлов, а какие у безопасных. Тем самым данная модель анализирует различные свойства файла, и на основе этой информации определяет его тип.

Общий вид работы такой системы показан на рисунке 2.

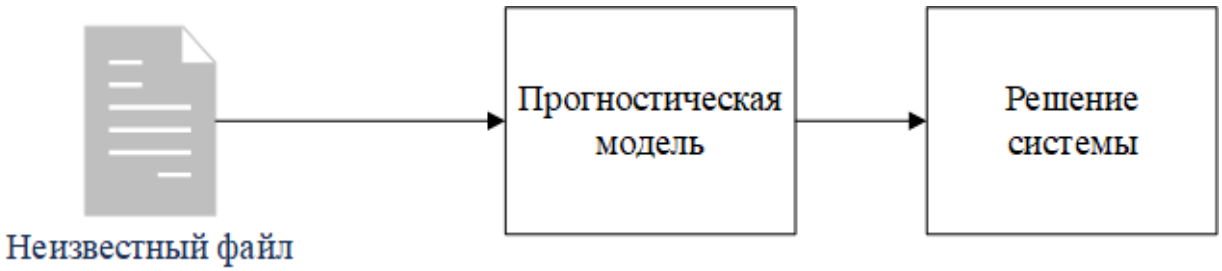


Рисунок 2. Пример работы машинного обучения.

Самыми важными технологиями искусственного интеллекта в области информационной безопасности являются:

1. **Локально-устойчивая свертка**. Представляет из себя метод эффективного обобщения на основе ортогональных проекций, для выбора наиболее важных свойств файла, по которым наиболее успешно будут найдены вредоносные файлы. Пример работы локально-устойчивой свертки показан на рисунке 3.

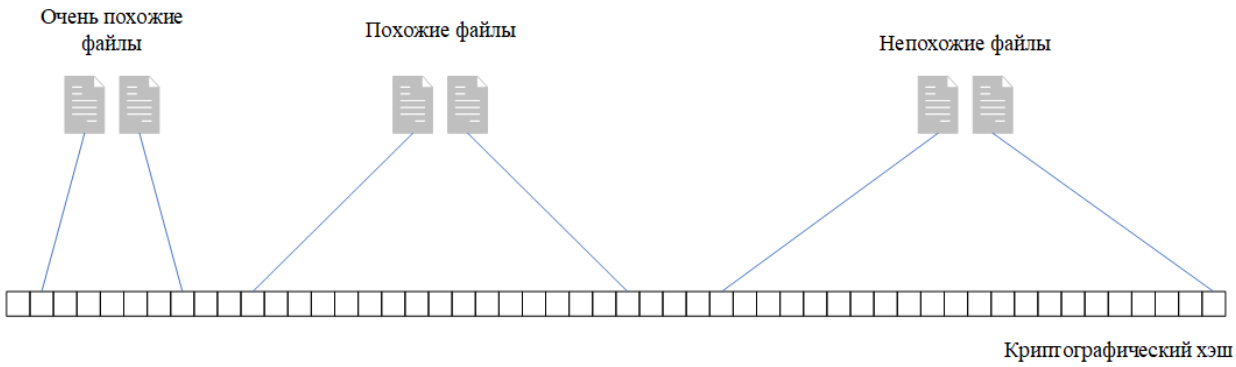


Рисунок 3. Пример локально-устойчивой свертки

2. **Ансамбль деревьев решений**. Данная модель основана на таком методе искусственного интеллекта, как дерево принятия решений. Пример такого дерева показан на рисунке 4.

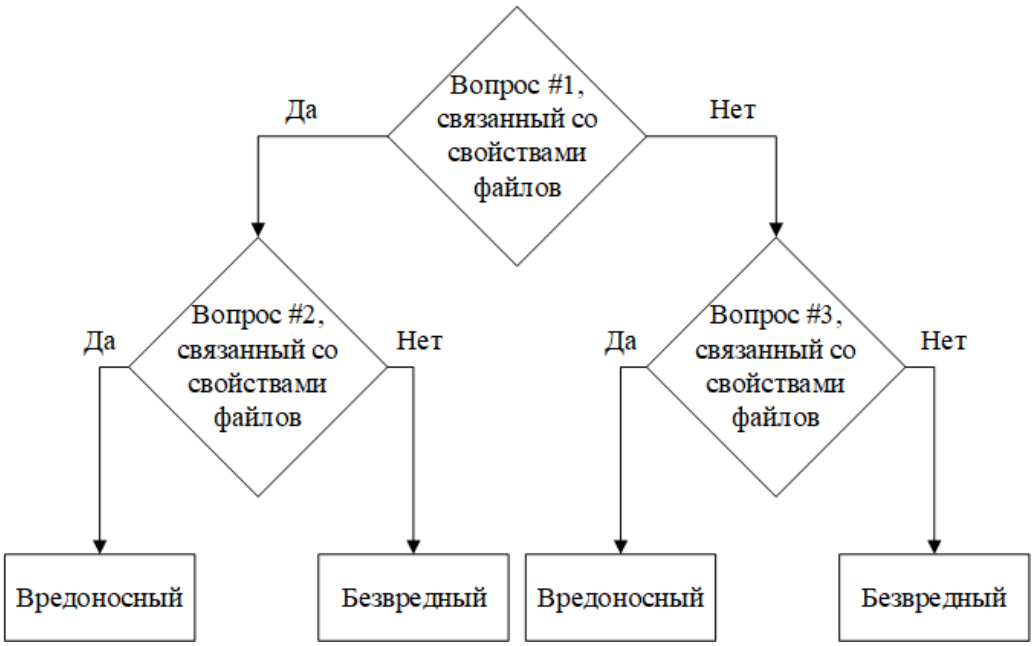


Рисунок 4. Простое дерево решений.

Ансамбль деревьев решений представляет модель, в которой используется множество деревьев решений. Тип файла решается выбором большинства деревьев. Принцип действия такой системы показан на рисунке 5.

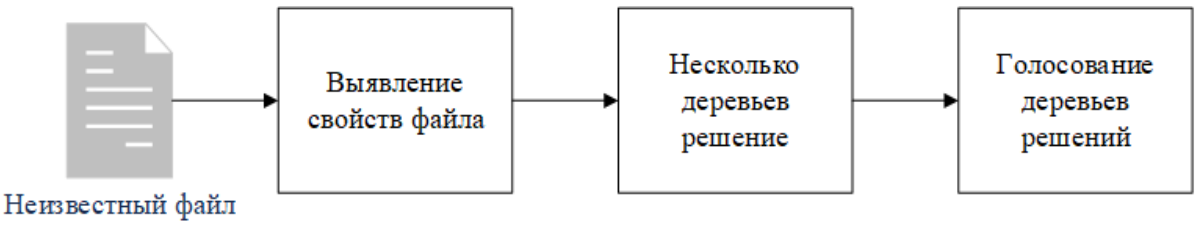


Рисунок 5. Принцип действия ансамбля деревьев решений.

3. **Поведенческая модель**. Принцип действия заключается в том, что компоненты системы составляют журнал действий пользователей и системы за определенный период времени и формируют паттерны поведения. Нейронная сеть обучается на основе этих данных и может распознавать опасную активность, тем самым предупредить атаку.

4. **Кластеризация входящего потока.** Данный метод разделяет большой объем данных по кластерам, которые автоматически обрабатываются в зависимости от классифицированных ранее объектах внутри.

Всё вышесказанное показывает, что искусственный интеллект просто необходим, если речь идет о современной информационной безопасности. Однако не стоит забывать, что злоумышленники всё чаще используют те же самые методы, тем самым создавая новые виды кибератак. Простейшим примером является обход так называемой “капчи”, которая представляет из себя защиту от скриптов и автоматизированных программ. Это уже не является проблемой для злоумышленников, поскольку искусственный интеллект крайне быстро обходит подобную защиту. Еще одним примером является подделка человеческого голоса с помощью искусственного интеллекта. Из-за данного вида атаки аутентификация по голосу не может считаться абсолютно надежной. Есть еще множество примеров использования технологий машинного обучения как со стороны защиты, так и со стороны нападения. Как итог, искусственный интеллект в

информационной безопасности просто незаменим, так как злоумышленники уже начинают его использовать в полную силу.

СПИСОК ЛИТЕРАТУРЫ

1. Машинной обучение в кибербезопасности [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/enterprise-security/wiki-section/products/machine-learning-in-cybersecurity

2. С. Рассел, П. Норвиг. Искусственный интеллект: современный подход, 4-е изд., том 1. Решение знания и рассуждения. : Пер. с англ. - СПб. : ООО "Диалектика", 2021. - 704 с

3. Джон Д. Келлехер. Глубокое обучение. Самый краткий и понятный курс, — Москва: Эксмо, 2022. – 160 с

4. Н.В. Гришина. Использование методов искусственного интеллекта для обеспечения информационной безопасности // Информационная безопасность: вчера, сегодня, завтра – Москва, 2020 – с 158-163

5. Грязнов С.А. Искусственный интеллект и кибербезопасность // Теоретические и прикладные вопросы комплексной безопасности – Москва, 2021 - 163-165

6. Как искусственный интеллект влияет на гонку вооружений в сфере кибербезопасности [Электронный ресурс]. –

Режим доступа: https://theconversation.com/how-ai-is-shaping-the-cybersecurity-arms-race-167017

7. Применение технологий искусственного интеллекта в информационной безопасности [Электронный ресурс]. –

Режим доступа:

https://www.anti-malware.ru/analytics/Technology_Analysis/using-artificial-intelligence-technologies-in-information-security

8. Антон Фишман. Искусственный интеллект: возможности и угрозы [Электронный ресурс]. –

Режим доступа: https://www.it-world.ru/cionews/security/175459.html

9. Джон Д. Келлехер. Глубокое обучение. Самый краткий и понятный курс, — Москва: Эксмо, 2022. – 160 с

10. Гарбук С.В задачи нормативно-технического регулирования интеллектуальных систем информационной безопасности // Вопросы кибербезопасности - Москва, 2021. - С. 83.

НАУЧНАЯ СЕКЦИЯ

«ПРОБЛЕМЫ ЦИФРОВОГО СУВЕРЕНИТЕТА И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ»

Руководитель: **Крылов Григорий Олегович**,
доктор физико-математических наук, профессор кафедры «Безопасность телекоммуникаций» Московского технического университета связи и информатики, профессор Финуниверситета, профессор Национального исследовательского ядерного университета «МИФИ»

Секретарь: **Закомолдин Семён Дмитриевич,**
Московский технический университет связи и информатики, студент кафедры «Безопасность телекоммуникаций»

Глозштейн Д.А.
ПГТУ, ст.преп. кафедры ИБ
GlozshtejnDA@volgatech.net
Сидоркина И.Г.
ПГТУ, зав. кафедрой ИБ
доктор технических наук, профессор
SidorkinaIG@volgatech.net

ОРГАНИЗАЦИЯ ЗАЩИЩЕННОЙ ВИДЕОКОНФЕРЕНЦСВЯЗИ С ИСПОЛЬЗОВАНИЕМ КВАНТОВОГО КАНАЛА СВЯЗИ

Во время видеоконференций некоторые сеансы требуют передачи внутренней конфиденциальной информации коммерческих предприятий и государственных структур. Поэтому видеоконференцсвязь (ВКС), основанная на высокоскоростных мультимедийных коммуникационных технологиях, должна быть надежно защищена от деструктивных воздействий любого рода. Зачастую, безопасность этой информации имеет ключевое значение, и атаки на видеоданные серьезно сказываются на деятельности крупных организаций и даже государств, что является сдерживающим фактором для дальнейшего развития видеотехнологий.

В последние годы был предложен ряд методов, обеспечивающих защиту ВКС, такие как решение для избирательного шифрования видеоданных в реальном времени [1], скрытие данных с помощью замены кодового слова в зашифрованных видеороликах MPEG-4 (Moving Picture Experts Group-4) [2], архитектура безопасности ВКС в пиринговых сетях [3] и многое другое.

Одним из возможных способов обеспечения безопасности ВКС является использование дополнительной квантовой связи для генерации ключей шифрования.

Квантовая коммуникация - технология кодирования и передачи данных в квантовых состояниях фотонов. Наиболее применимый вариант использования квантовых коммуникаций для обеспечения безопасности связи реализован в виде протоколов квантового распределения ключей (КРК) [3,4,5,6].

Технология КРК, основанная на фундаментальных принципах квантовой механики, может установить безусловно надежный ключ шифрования между двумя сторонами, обменивающимися данными. Поэтому её практическая применимость в современных сетевых технологиях привлекает все большее внимание. За последние 5 лет были реализованы различные схемы генерации квантовых ключей [1,5,6,7,8] для классических сетей, разработан план интеграции существующей сети беспроводной связи и квантовой сети [10], предложена структура безопасности квантовой сети для облака [11], и др.

В данной статье для организации защищенной ВКС предлагается использовать технологию КРК, так как она обеспечивает гарантированную безопасность передачи данных, причем как для однофотонного квантового источника [9], так и для многофотонного [12]. Предложен алгоритм формирования ключей для данного протокола, который состоит в следующем:

1. Центральная платформа и терминал ВКС договариваются, о порядке интерпретации состояний фотонов (например, 0 – для вертикальной поляризации, 1 – для горизонтальной в вертикально-горизонтальном базисе, аналогично для диагонального базиса);

2. Центральная платформа отправляет отдельные фотоны на терминал в произвольном базисе, используя генератор случайных чисел;

3. Терминал измеряет принимаемые фотоны в выбранном произвольно базисе. В итоге у него будет “сырая” строка битов с 25% ошибок;

4. По каждому состоянию терминал по открытому каналу сообщает,

базис, в котором проводилось измерение, не указывая его результаты;

5. Центральная платформа сообщает, в каких случаях её базис совпал с базисом терминала. Если базисы совпали, то бит оставляют, а если нет, то игнорируют его.

Половина данных, соответствующая событиям несовпадения базисов, выбрасывается, оставляя “просеянную” битовую последовательность. Если в канале связи нет значительных помех или подслушивания, обе стороны получат коррелированную строку случайных битов. Ошибки, вызванные помехами и несанкционированным прослушиванием канала, могут быть идентифицированы и устранены, если их количество в полученной битовой последовательности не превышает 11% [5,7]. Если количество ошибок попадает в указанные пределы, создается ключ шифрования, что гарантирует безопасность, так как злоумышленник о нем не знает. В противном случае секретный ключ не будет создан, и квантовый канал считается блокированным. Таким образом, исключается возможность доступа злоумышленника к данным, передаваемым по квантовому каналу, что и определяет безопасность алгоритма.

Схема ВКС с использованием КРК

В данной статье предложена стратегия применения квантового ключа в системе ВКС. В ходе работы была не только сформирована сетевая схема для беспрепятственного подключения квантового шлюза к системе ВКС, но и предложен алгоритм расширения квантового ключа, основанный на том факте, что скорость генерации квантового ключа ниже, чем скорость шифрования. Поэтому за счет увеличения скорости генерации ключа можно обеспечить абсолютно безопасную передачу видеоданных с использованием системы одноразового блокнота для шифрования. Система одноразового блокнота является одной из наиболее распространенных в системах КРК, так как канал связи, который невозможно подслушивать без высокой вероятности обнаружения, позволяет многократно использовать одноразовый

блокнот. При обнаружении прослушивания его легко заменить новыми случайными битами. [13]

На рисунке 1 представлена система ВКС с квантовым ключом.

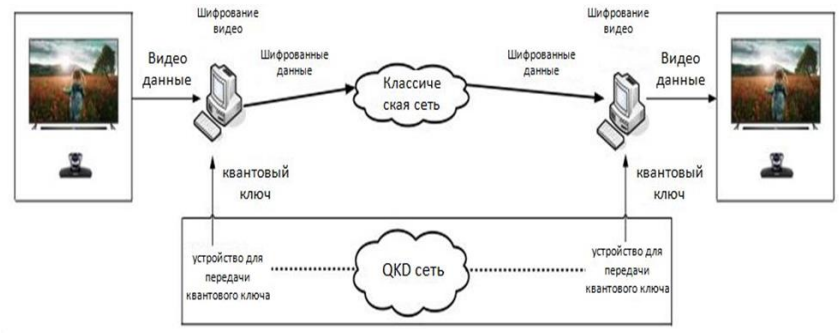


Рисунок 1. Общая схема ВКС с использованием квантового ключа

В этой системе технология КРК используется для реализации совместного использования квантового ключа получателем и отправителем. Видеотерминалы могут получать квантовый ключ от устройства передачи квантового ключа, а видеоданные шифруются на основе одноразового блокнота. Зашифрованные данные могут передаваться через классическую сеть на другие видеотерминалы, которые могут осуществлять дешифрование с помощью общего квантового ключа.

Для создания простейшей топологии видеоконференцсвязи были объединены трехузловая квантовая коммуникационная сеть и классическая сеть. Топология предложенного решения ВКС на основе КРК показана на рисунке 2.

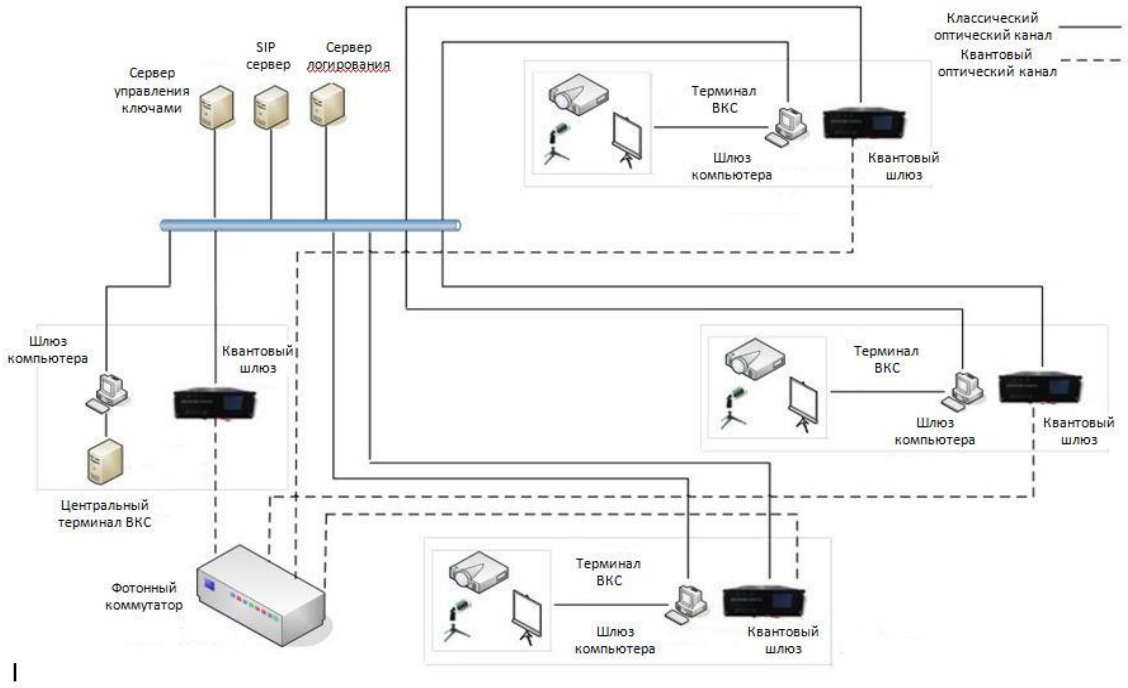


Рисунок 2. Топология системы ВКС с использованием квантового ключа

В этой топологии выделены следующие элементы:

1. Квантовая оптоволоконная линия, которая использовалась для распределения квантового ключа, показана пунктирной линией. Сплошная линия изображает классическую оптоволоконную линию, которая необходимадля обмена информацией для системы ВКС.

2. Каждому из узлов квантовой оптоволоконной линии требуются собственные квантовый и программный шлюз.

3. Матричный фотонный коммутатор в квантовой волоконно-оптической линии осуществляет соединение внутренних и внешних оптических портов.

4. Сервер управления генерацией ключей используется для управления процессом КРК для всей квантовой оптоволоконной линии связи. Сервер SIP (протокол установления сеанса) используется для установления сеанса пользователя. Сервер логирования используется для мониторинга рабочего состояния всей квантовой волоконно-оптической линии.

5. Каждый узел может $K(i)$ быть напрямую подключен к офисным приложениям или к подсети офисных данных, а квантовый шлюз может служить выходом брандмауэра подсети.

Таким образом, система ВКС, основанная на квантовом ключе, представляет собой телекоммуникационную сеть, для которой принят системный стандарт для передачи мультимедиа-данных H.323, включающий одну центральную платформу и три удаленных терминала конференц-системы. Система видеоконференцсвязи была построена с использованием квантовой защищенной сети связи для обеспечения повышенной безопасности видеоконференции. Центральная платформа включает специализированный сервер, используемый для передачи информации о видеоконференции из различных удаленных конференц-залов. Терминалы конференц-системы подключаются к центральной платформе через классическую сеть связи. Также они оснащаются квантовым шлюзом и интерфейсом видеоконференции высокой четкости, отвечающими за прием видеоизображений, отправляемых центральной платформой, и отправку этих изображений, собранных локальными камерами высокой четкости, на центральную платформу. Кроме того, каждый терминал должен быть оснащен набором всенаправленных цифровых микрофонов, которые могли осуществлять сбор звука в каждом зале видеоконференций, и ЖК-телевизором высокой четкости для вывода изображения. Акустические и видеоустройства каждого конференц-зала должны быть подключены к квантовым устройствам в канале передачи данных, что обеспечит безопасную передачу данных в сети.

Заключение.

В статье была предложена схема применения КРК в системе ВКС, объединяющая классическую сеть и сеть квантовой связи, а также разработан специальный алгоритм расширения квантового ключа, который позволяет увеличить его генерацию до скоростей, необходимых для обеспечения

нормального качества видеоизображения. Возможность применения квантового ключа в системах ВКС создает теоретическую базу для организации более сложных систем ВКС в реальных сетях связи, использующих шифрование с квантовым ключом.

СПИСОК ЛИТЕРАТУРЫ

1. Габдулхаков, И.М. Построение многоканальной системы квантового распределения ключей с частотным кодированием / И.М.Габдулхаков, О.Г. Морозов //ИВД. — 2020 — №5 — (с.60-65).
2. Hamidouche, W.. Real-time selective video encryption based on the chaos system in scalable HEVC extension. / W.Hamidouche, M. Farajallah, N. Sidaty, S. E. Assad, O. Deforges // Signal Processing Image Communication. — 2017. — №58. — pp. 73–86.
3. Rohara, J. Using Codeword Substitution to Hide Data in Encrypted MPEG-4 Videos. / J. Rohara, V. B. Gaikwad // IRJET. — 2017. — №04(04). — pp. 3276–3280
4. Wu W. P2P-based video conferencing security management strategy /W. Wu, B. Ej // International Conference on Multimedia Technology. - 2018 -
5. Bennett, C. H. Quantum Cryptography: Public Key Distribution and Coin Tossing. in Proc. / C. H. Bennett, G. Brassard // IEEE International Conference on Computers, Systems and Signal Processing.—1984. — pp. 175–179
6. Ekert, A. K. Quantum cryptography based on bell’s theorem. / A.K. Ekert// Phys. Rev. Lett. — 1991. — pp.67-76
7. Bennett C. H. Quantum cryptography using any two nonorthogonal states. / C. H. Bennett // Phys. Rev. Lett.— 1992 — № 68. — pp. 3121–3124.
8. Xu, F. Secure quantum key distribution with realistic devices. / F. Xu, X. Ma, , Q. Zhang, H.-K. Lo, J.-W.Pan, // Rev. Mod. Phys. — 2020. — №92. — pp.61-69
9. Shor P.W. Simple proof of security of the BB84 quantum key distribution protocol. / P.W. Shor, J. Preskill// Phys Rev Lett. — 2000. — №85. —pp. 441–447

10. Liu, X. H. Quantum wireless communication network model and performance analysis. / X. H. Liu, C. X. Pei, M. Nie // Journal of Jilin University — 2014. — №44(4) — pp. 177–181.

11. Kelley, B. Securing Cloud Containers Using Quantum Networking Channels. / B. Kelley, J. J. Prevost, P. Rad, A. Fatima // IEEE International Conference on Smart Cloud. — 2016. — pp.103-111

12. Gottesman, D. Security of quantum key distribution with imperfect devices. / D.Gottesman, H. K. Lo, J. Preskill // Quantum Information & Computation — 2004. — pp. 70-75

13. Bennett, C.H.; Brassard, G.; Breidbart, S. Quantum Cryptography II: How to re-use a one-time pad safely even if P=NP. / C.H. Bennett,; G. Brassard,; S. Breidbart // Nature Communications. — 2014. — №13 — pp. 453–458

Дебеева Е.Е.
ЮРГПУ(НПИ) им. М. И. Платова, студент
katyusha.debeeva@mail.ru
Алексеев В.П.
ЮРГПУ(НПИ) им. М. И. Платова, преподаватель
Старший преподаватель кафедры ИБ
aleksvictor@bk.ru

ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ ТЕСТИРОВАНИЯ WEB-ПРИЛОЖЕНИЙ НА УЯЗВИМОСТИ

Современный этап развития информационного общества характеризуется массовым использованием интернет ресурсов, и предоставлением широкого спектра онлайн-услуг. Всё больше пользователей обращаются к сайтам, web-приложениям для обмена и хранения информации, которая требует защиты от всевозможных злоумышленников. Поэтому на сегодняшний день анализ защищенности web-приложений от уязвимостей является одной из актуальных задач в области информационной безопасности.[1]

На основании статистических данных и по итогам 2021 года 60% web-приложений содержали критические уязвимости, которые поставили под угрозу конфиденциальность, целостность и доступность хранящихся данных на сайтах и могли стать причиной нелегитимных действий.[4] Чтобы правильно выбрать способы защиты, необходимо теоретически знать и иметь технические возможности, анализировать защищенность web-приложений, проводить обзор возможных уязвимостей, используя актуальную базу данных уязвимостей и практически грамотно устранять полученную информацию об обнаруженных уязвимостях.

Большинство современных организаций используют web-приложения для обеспечения бизнес-процессов. Тем не менее, многие сайты и web-сервисы недостаточно защищены от уязвимостей и представляют собой легкую добычу для злоумышленников любого уровня подготовки.

Для анализа защищенности web-приложений, как правило используют методологию инструментального анализа защищенности (сканирования) и тестирование на возможность проникновения уязвимостей.[2]

На кафедре «Информационная безопасность» ЮРГПУ НПИ разработан программный комплекс, позволяющий анализировать web-приложения на широко распространённые виды уязвимостей, используемый также для обучения способам и методам ручного и автоматизированного сбора информации об уязвимостях. Разработанный программный комплекс может быть использован в качестве как самостоятельного программного обеспечения на этапе сбора информации, так и в качестве средства решения специфичных задач при использовании дополнительных скриптов, созданных пользователями. Все инструменты поиска и анализа уязвимостей работают в рамках одного программного комплекса, обеспечивая при этом простоту в настройках, легкость в эксплуатации и быстрое освоение программы пользователем.

В рейтинг наиболее широко распространенных уязвимостей включены: инъекции SQL, позволяющие с помощью внедрения кода в запросы получать доступ к данным, манипулировать ими; недочеты системы аутентификации, например, отсутствие при обработке запросов дополнительных проверок; незащищенность критичных данных или отсутствие шифрования критичных данных, таких как аутентификационные данные или номера кредитных карт; внедрение внешних XML (XXE); нарушение контроля доступа (проверку контроля доступа, как на стороне клиента, так и на стороне сервера, так как запросы могут приходить еще и асинхронно, например с помощью технологии AJAX); небезопасная конфигурация web-приложения;

межсайтовый скриптинг(XSS), при которой злоумышленник может передать код Java Script на исполнение в браузер пользователя; использование дополнительных компонентов, например CMS и фреймворки, могут использовать дополнительные компоненты, такие как плагины и модули. Многочисленные компоненты имеют открытый исходный код, что означает, что любой пользователь может провести анализ кода и выявить в нем уязвимости, например, очень часто находят уязвимости в плагинах для CMS WordPress.

На официальном сайте Федеральной службы по техническому и экспортному контролю (ФСТЭК) России размещен банк данных угроз безопасности информации, содержащий сведения об основных угрозах и уязвимостях безопасности информации. Эта информация выборочно использована в разработанном программном комплексе при автоматизированном средстве контроля защищенности информации (сканере безопасности) в части web-приложений.

База данных уязвимостей, имеющаяся в системе, требует постоянного развития, поэтому предусмотрено периодическое обновление базы данных уязвимостей из Банка данных угроз безопасности информации ФСТЭК России.

Порядок тестирования web-приложений на уязвимости выполняется по классической схеме. В настоящее время программный комплекс состоит из следующих блоков: анализ состояния защищенности web-приложения; поиск наличия уязвимостей в web-приложениях; формирование отчетности по результатам проводимых сканирований; оперативное оповещение о найденных уязвимостях; оценка соответствия безопасности web-приложения стандартам ФСТЭК РФ; вывод и отображение результатов сканирования.

Результат поиска отображается на главной панели программного комплекса. В случае обнаружения SQL инъекции, на экране будет показана найденная SQL инъекция и инструкция по её устранению.

Чтобы обеспечить полноту ответных действий со стороны персонала в результате тестирования web-приложения на уязвимости формируется отчет, расширенная версия которого состоит из следующих разделов: цель анализа; объект тестирования; оценки степени риска уязвимостей собственно отчет по уязвимостям с указанием имени, краткого описания, степени риска, количество обнаруженных уязвимостей и указания идентификации уязвимости.

Разработанный программный комплекс имеет широкий спектр применения и позволяет проводить поиск уязвимостей не только непосредственно web-приложений, но и web-серверов.

Работа программного комплекса позволяет определить структуру сайта. используя специальные скрипты, позволяет находить все страницы авторизации на web-сайте. Для работы модуля необходимо указать адрес сайта для получения его структуры. Обнаруженные ссылки на внешние источники перенаправляются в другие скрипты для проверки на предполагаемые угрозы-уязвимости.

Таким образом, пользователь получает полный документированный анализ web-приложения, основанный на известных и внесенных в базу данных программного комплекса уязвимостях на момент проведения тестирования. Программный комплекс внедрен в учебный процесс и применяется при изучении курсов «Защищенные информационные системы», «Комплексная система защиты информации на предприятии», «Основы информационной безопасности», «Основы управления рисками и инцидентами информационной безопасности». «Теоретические основы защиты объектов информатизации».

СПИСОК ЛИТЕРАТУРЫ

1 Пермякова, О.В. Анализ уязвимостей АСУТП как объекта критической информационной инфраструктуры / Пермякова О.В., Пермякова М.А., Пермякова М.А. // Безопасность информационного

пространства : сб. трудов XVIII Всерос. науч.-практ. конф. студ., аспирантов и молодых ученых, 28-29 нояб. 2019 г., г. Магнитогорск / Магнитогорский гос. технический ун-т им. Г.И. Носова. – Магнитогорск, 2019. – С. 222-225.

2 OWASP TOP-10: практический взгляд на безопасность веб-приложений [Электронный ресурс] / Блог компании SimplePay Сайт Хабр (habr.com). – URL: https://habr.com/ru/company/simplepay/blog/258499/(дата обращения: 16.04.2021).

3 Банк данных угроз безопасности информации [Электронный ресурс] – URL: https://bdu.fstec.ru

4 Новостная статья Известия IZ [Электронный ресурс] - URL : https://iz.ru/1196257/anna-ustinova/servernoe-siianie-57-prilozhenii-bankov-i-onlain-magazinov-uiazvimy-dlia-khakerov

5 Хонин А. Сканеры защищенности веб-приложений (WASS) – обзор рынка в России и в мире [Электронный ресурс] / Сайт Anti-Malware.ru. – URL https://www.antimalware.ru/reviews/web_application_security_scanners_market_russia_worldwide

6 Кляус, Т.К. Подход к оценке эффективности системы защиты информации с использованием экономических метрик безопасности / Кляус Т.К., Гатчин Ю.А. // Вестник УрФО. Безопасность в информационной сфере. – 2019. – № 2 (32). – С. 39-44.

7 Менщиков, А.А. Комбинированный метод обнаружения и противодействия автоматизированному сбору информации с веб-ресурсов / Менщиков А.А., Гатчин Ю.А., Коробейников А.Г. // Вестник УрФО. Безопасность в информационной сфере. – 2019. – № 2 (32). – С.25-29.

8 Сердечный А.Л. Технология выявления сведений об уязвимостях сторонних компонентов программного обеспечения с открытым исходным кодом / Сердечный А.Л., Герасимов И.В., Макаров О.Ю., Пастернак Ю.Г.,

Тихомиров Н.М. // Информация и безопасность. – 2020. – Т. 23, № 3. – С. 347-364.

9 Сайт ФСТЭК {Электронный ресурс] URL: https://fstec.ru/

10 Бегаев А.Н., Тестирование на проникновение. Бегаев С.Н., Федотов В.А. – : Университет ИТМО, 2018. –1 - 45 с.

Дорохов С.В.
МИРЭА – Российский технологический университет,
доцент БК «Цифровые устройства и системы защиты информации» №235,
к.т.н., с.н.с.
Михайлов В.Э.
МИРЭА – Российский технологический университет,
ассистент БК «Цифровые устройства и системы защиты информации» №235,
mihajlov_v@mirea.ru

ПРОБЛЕМА НЕКОРРЕКТНОЙ ВАЛИДАЦИИ СЕРТИФИКАТОВ (IMPROPER CERTIFICATE VALIDATION) ПРИ УСТАНОВЛЕНИИ ДОВЕРЕННЫХ СОЕДИНЕНИЙ

Сертификат — это токен, который связывает объект с криптографическим ключом. Сертификаты могут использоваться для проверки принадлежности открытого ключа предполагаемому владельцу [1]. С помощью использования цифровых сертификатов можно определить, что зашифрованная информация исходит от доверенной стороны, а не от злоумышленника. При обработке информации, передаваемой по протоколу безопасности транспортного уровня (TLS), например, данных, возвращаемых веб-службой, ключевым моментом является то, что валидация (проверка) сертификата происходит при закреплении криптографического ключа за доменом [2]. Сертификаты должны быть подписаны доверенным центром сертификации, использоваться только до истечения срока их действия и проверяться по спискам отозванных сертификатов перед использованием.

Протокол TLS – это криптографический протокол, обеспечивающий сквозную защиту данных, пересылаемых между приложениями через Интернет [3]. Работу протокола TLS можно увидеть при использовании веб-браузера на страницах, отмеченных специальным символом «замок». Кроме этого, протокол используется в других приложениях: почтовых программах, программах для

обмена файлами, проведения аудио- и видеоконференций, мессенджерах и др. Протокол TLS произошел от протокола Secure Socket Layers (SSL), разработанного в 1994 г. компанией Netscape Communications Corporation для защиты веб-сеансов. SSL версии 1.0 никогда не выпускался публично, в то время как SSL 2.0 был быстро заменен на SSL 3.0, на котором основан TLS.

В независимом рейтинге OWASP Top 10 за 2021 год уязвимость *Improper Certificate Validation* (CWE-295 [4], [5]) относится к категории *Identification and Authentication Failures* и занимает 7 место [6]. Данная уязвимость была обнаружена в некоторых программных продуктах и веб-сайтах ([7], [8], [9], [10]).

Когда сертификат является недействительным или вредоносным, это может позволить злоумышленнику подделать доверенный объект, вмешавшись в канал связи между хостом и клиентом. Программное обеспечение может подключиться к вредоносному хосту, полагая, что этот хост является доверенным, либо может начать принимать поддельные данные, которые, как представляется, исходят от доверенного хоста.

Соединения TLS по интернет-протоколу используют сертификаты X.509 в качестве основы алгоритмов шифрования с открытым ключом. Если веб-сервер инициирует исходящие TLS-соединения, например, если он выполняет вызовы веб-службы посредством протокола HTTPS, то валидация сертификата должна проводиться перед установкой соединения.

Представленные ниже примеры помогают проиллюстрировать причины возникновения уязвимости, связанной с некорректной валидацией сертификатов (*Improper Certificate Validation*), и описать методы и приемы, которые можно использовать для снижения риска.

Пример №1.

В блоке исходного кода происходит проверка сертификата подключенного узла.

```
if ((cert = SSL_get_peer_certificate(ssl)) && host)
  var = SSL_get_verify_result(ssl);
if ((X509_V_OK == var || X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN == var))
  // сертификат прошел проверку, хост является доверенным
```

В данном случае, поскольку сертификат является самоподписанным, отсутствует внешний удостоверяющий центр, который мог бы подтвердить личность хоста. Программа может обмениваться данными с другой системой, которая подменяет хост, например. путем «отравления» DNS-кэша или использования атаки «человек посередине» (MITM) [11] для изменения трафика от сервера к клиенту.

Пример №2.

В приведенном коде OpenSSL [12] программа получает сертификат и проверяет его.

```
cert = SSL_get_peer_certificate(ssl);
if (cert && (SSL_get_verify_result(ssl) == X509_V_OK)) {
  // код программы
}
```

Несмотря на то, что на шаге проверки возвращается значение *X509_V_OK*, этот шаг не включает в себя проверку параметра *Common Name* на соответствие имени хоста. Следовательно, гарантия того, что сертификат принадлежит

нужному хосту, отсутствует. В результате SSL-соединение может быть установлено с вредоносным хостом, предоставившим действительный сертификат.

Пример №3.

В приведенном OpenSSL-коде программа гарантирует проверку наличия сертификата и позволяет использовать сертификаты с истекшим сроком действия.

```
if (cert = SSL_get_peer_certificate(ssl)) {
  var = SSL_get_verify_result(ssl);
  if ((X509_V_OK == var || (X509_V_ERR_CERT_HAS_EXPIRED == var))
    // код программы
}
```

В случае, если при вызове функции *SSL_get_verify_result()* возвращается значение *X509_V_ERR_CERT_HAS_EXPIRED*, это будет означать, что срок действия сертификата истек. Со временем у злоумышленников возрастает вероятность компрометации сертификата.

Пример №4.

В приведенном коде OpenSSL программа гарантирует проверку наличия сертификата перед тем, как продолжить свое исполнение.

```
if (cert = SSL_get_peer_certificate(ssl)) {
  // получение сертификата, затем исполнение кода программы
}
```

Из-за того, что в коде не используется функция *SSL_get_verify_result()* для проверки сертификатов, программа может принимать сертификаты, которые были

ранее отозваны. В таком случае ПО может обмениваться данными с вредоносным хостом.

Пример №5.

В приведенном OpenSSL-коде гарантируется, что хост имеет сертификат.

```
if (cert = SSL_get_perr_certificate(ssl)) {
  // сертификат получен, хост является доверенным
  // var = SSL_get_verify_result(ssl);
  // if (X509_V_OK == var) ...
}
```

В данном блоке кода не происходит вызова функции *SSL_get_verify_result(ssl)*, поэтому этап проверки сертификата отсутствует.

ВЫВОДЫ

При разработке программного обеспечения с целью корректной валидации сертификата в исходном коде программы должна быть реализована проверка того, что:

1) сертификат выдается доверенным центром сертификации;
2) ни один из сертификатов в цепочке не имеет истекший срок действия.

Только после выполнения приведенных условий валидация сертификата при установлении доверенных соединений может считаться успешной.

СПИСОК ЛИТЕРАТУРЫ

1. Improper Certificate Validation | Martello Security [www.martellosecurity.com] – URL: https://martellosecurity.com/kb/mitre/cwe/295/ (дата обращения 19.09.2022). – Текст: электронный.

2. Improper Certificate Validation | Vulnerability Fix Database | ShiftLeft [www.shiftleft.io] – URL: https://www.shiftleft.io/community-and-training/vulnerability-fix-database/java/improper-certificate-validation-java/ (дата обращения 19.09.2022). – Текст: электронный.

3. What is TLS & How Does it Work? | ISOC Internet Society [www.internetsociety.org] – URL: https://www.internetsociety.org/deploy360/tls/basics/ (дата обращения 19.09.2022). – Текст: электронный.

4. CWE-295: Improper Certificate Validation | Vulnerability History Project [www.vulnerabilityhistory.org] – URL: https://vulnerabilityhistory.org/tags/cwe-295/ (дата обращения 19.09.2022). – Текст: электронный.

5. CWE-295 – Improper Certificate Validation [www.cybersecurity-help.cz] – URL: https://www.cybersecurity-help.cz/vdb/cwe/295/ (дата обращения 19.09.2022). – Текст: электронный.

6. OWASP Top 10:2021 [www.owasp.org] – URL: https://owasp.org/Top10/ (дата обращения 19.09.2022). – Текст: электронный.

7. #903424 SSL certificate not validated when registering with a provider [www.hackerone.com] – URL: https://hackerone.com/reports/903424/ (дата обращения 19.09.2022). – Текст: электронный.

8. CVE-2022-22306 : An improper certificate validation vulnerability [CWE-295] in FortiOS 6.0.0 [www.cvedetails.com] – URL: https://www.cvedetails.com/cve/CVE-2022-22306/ (дата обращения 19.09.2022). – Текст: электронный.

9. Improper Certificate Validation in libcurl | CVE-2022-27782 | Snyk [security.snyk.io] – URL: https://security.snyk.io/vuln/SNYK-AMZN2-LIBCURL-2950345/ (дата обращения 19.09.2022). – Текст: электронный.

10. Improper Certificate Validation in OkHttp – software database | Vulners [www.vulners.com] – URL: https://vulners.com/osv/OSV:GHSA-4HC2-JH7R-WRC3 (дата обращения 19.09.2022). – Текст: электронный.

11. The Bad Side Of Improper Certificate Validation [www.appknox.com] – URL: https://www.appknox.com/blog/the-bad-side-of-improper-certificate-validation/ (дата обращения 19.09.2022). – Текст: электронный.

12. CWE – CWE-297: Improper Validation of Certificate with Host Mismatch (4.8) [cwe.mitre.org] – URL: https://cwe.mitre.org/data/definitions/297.html (дата обращения 19.09.2022). – Текст: электронный.

Кадацкова В. В.
Юргпу(НПИ) им. М.И. Платова
100502-ЗИСа-017, 5 курс
Vlada_and_vlad@mail.ru
Научный руководитель:
Лысенко Н. В.
ЮРГПУ(НПИ) им. М. И. Платова,
Доцент, к.п.н.
Nikstar_2010@mail.ru

ПОДГОТОВКА СОТРУДНИКОВ ДЛЯ МОНИТОРИНГА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОТИ

Киберполигон — многофункциональный программно-аппаратный комплекс, повторяющий типовые инфраструктуры предприятий различных отраслей. Позволяет отработать практические навыки специалистов без рисков, что что-то пойдет не по плану, и киберучения нанесут ущерб деятельности реального предприятия.

Подготовка сотрудников для мониторинга событий информационной безопасности должна происходить на реальных угрозах, которые существуют в базе данных ФСТЭК (БДУ - Угрозы (fstec.ru)).

В качестве исходных данных для определения угроз безопасности информации используется банк данных угроз безопасности информации (bdu.fstec.ru), ведение которого осуществляется ФСТЭК России в соответствии с подпунктом 21 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085, а также иные источники, содержащие сведения об уязвимостях и угрозах безопасности информации.

По результатам определения угроз безопасности информации необходимо найти наиболее популярные уязвимости для подготовки специалистов на платформе киберполигона.

Модель угроз безопасности информации должна содержать описание информационной системы и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

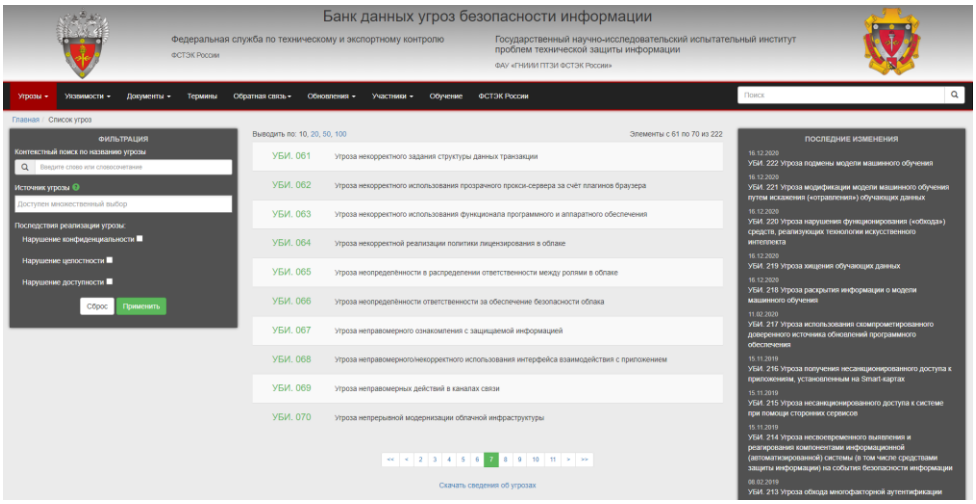


Рис.1 – Сайт ФСТЭК. Банк данных угроз.

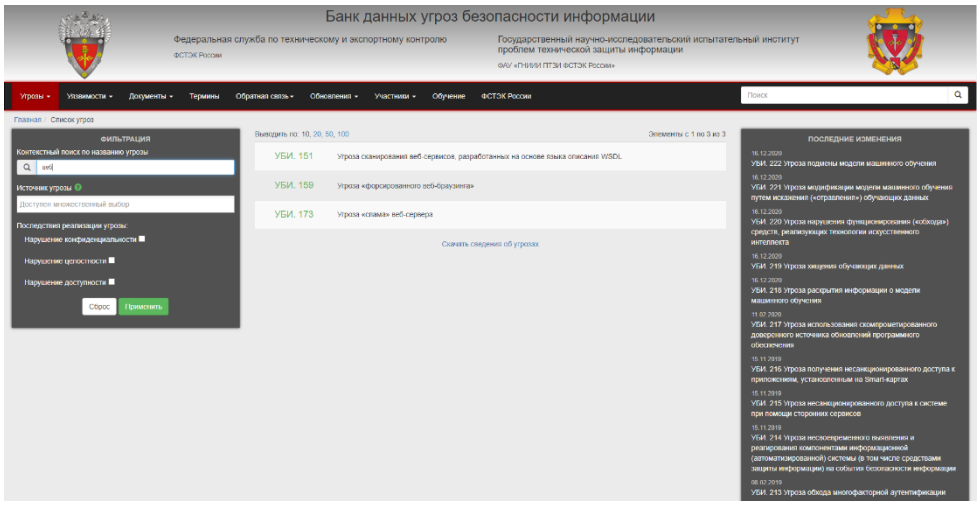


Рис.2 – Банк данных угроз. Поиск по фильтрам.

Модель сети предприятия представляет: коммутаторы, маршрутизатор, терминальный сервер, файловый сервер, сервер базы данных, почтовый сервер, web-сервер и VPN-шлюз. Сеть представлена на Рис.3.

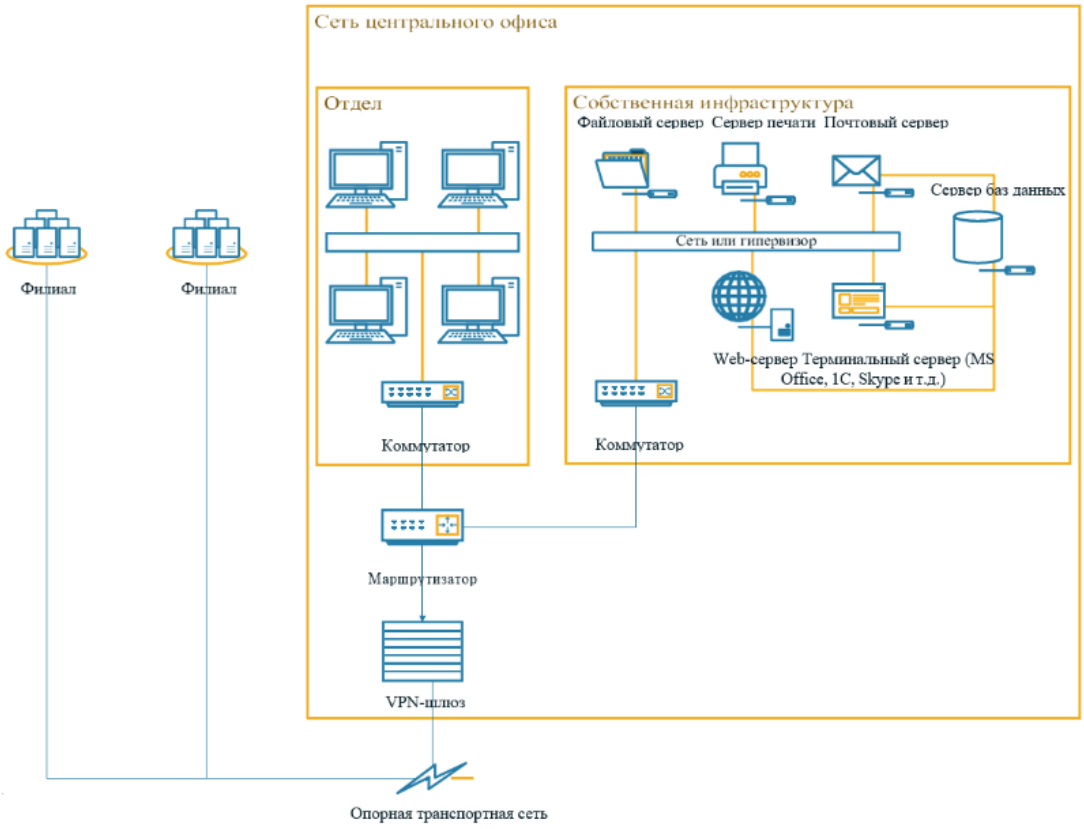


Рис.3 – Сеть предприятия.

По статистике можно выявить наиболее распространенные уязвимости.

На сайте касперского (https://securelist.ru/it-threat-evolution-q1-2021-non-mobile-statistics/101518/) приведена статистика информационных угроз в первом квартале 2021 года. В конце прошлого года, равно как и в первые месяцы года нынешнего, постепенно снижалось количество пользователей, которые были атакованы зловредами, предназначенными для кражи денежных средств с банковских счетов.

Таблица 1. Финансовые угрозы.

	Название	Вердикты	%*
1	Zbot	Trojan.Win32.Zbot	30,8
2	CliptoShuffler	Trojan-Banker.Win32.CliptoShuffler	15,9
3	Trickster	Trojan.Win32.Trickster	7,5

Trojan.Win32.Zbot:

Была признана в качестве опасной вредоносной инфекции, которая попадает под троянской категории. Угроза вторгается ваш компьютер, она проводит серию злонамеренных актов в фоновом режиме. Момент этот неприятный троян входит в вашу систему, он начинает мониторинг вашего веб-деятельности, такие как поисковые запросы, наиболее посещаемых страниц, наиболее открытые ссылки и т.д. Он крадет все ваши личные и конфиденциальные данные и разделяет их с хакерами для злых целей. Мошенники могут забрать все деньги, которые хранятся на вашем банковском счету и причинить вам страдать большие финансовые потери.

Win32/Zbot помогает удаленным преступникам легко контролировать систему и управлять своими злонамеренными действиями внутри. Мошенники могут злоупотреблять вашей социальной средой для массового распространения информации. Просят деньги от ваших друзей или членов семьи на ваше имя. Он отключает работу установленных мер безопасности, включая антивирусные средства и брандмауэры Windows, и делает устройство уязвимым для других вредоносных инфекций. Эта вирусная программа способна принести смертельный крипто-вирус машине, которая имеет тенденцию шифровать ваши важные файлы. Так, для того чтобы

предотвратить ваши устройство может быть атакованным такими угрозами, вы должны исключить Win32/Zbot от работы-станции быстро.

Trojan-Banker.Win32.CliptoShuffler:

В отличие от какого-нибудь шифровальщика-вымогателя этот вирус обходится без спецэффектов — он вообще изо всех сил старается не привлекать внимания. Вирус сидит в памяти и наблюдает за всем, что попадает в буфер обмена.

Как только CryptoShuffler замечает, что в буфер обмена попал адрес криптовалютного кошелька — а по характерным признакам вроде длины строки или символов в начале их довольно легко отличить от других данных — он аккуратно заменяет его на другой. В итоге криптовалютный перевод действительно уходит, и именно на ту сумму, которую вводил пользователь, — просто приходит он не владельцам пиццерии, а злоумышленникам, создавшим CryptoShuffler.

Trojan.Win32.Trickster:

Способен заражать 32- и 64-разрядные версии операционной системы Windows. Вирус имеет небольшой размер (до 500 КБ) и не имеет дополнительной упаковки и шифрования основного тела. Судя по протоколу взаимодействия с командным сервером, он переписан из исходного кода Dyre (Dyreza), но, в отличие от Dyre, способен осуществлять веб-инжекты.

Основное тело Trojan.Win32.Trickster содержит следующие характерные строки в формате Unicode:

• TrickLoader;

• Global\TrickBot;

• BotLoader.

Характерной и легко узнаваемой чертой является также наличие строки TrickLoader в поле User-Agent сетевых пакетов.

Файл со списком командных серверов Trojan.Win32.Trickster хранится в секции ресурсов в зашифрованном виде. Для расшифровки списка, а также модулей, получаемых от командных серверов, используется алгоритм шифрования AES. В качестве ключа используется хеш в формате RSA-256.

На данный момент известно о следующих модулях, используемых зловредом:

• systeminfo – первый модуль для Trojan.Win32.Trickster;

• injectDll – модуль, который встраивается в браузер и используется для веб-инжект.

В первом квартале были обнаружены атаки с использованием программ-майнеров на компьютерах 432 171 уникального пользователя.

Таблица 2. Угрозы майнеров.

	Название	Вердикты	%*
1	WannaCry	Trojan-Ransom.Win32.Wanna	19,37
2	(generic verdict)	Trojan-Ransom.Win32.Gen	12,01
3	(generic verdict)	Trojan-Ransom.Win32.Phny	9,31

Trojan-Ransom.Win32.Wanna:

Вредоносное ПО WannaCry, шифрующее файлы пользователя и распространяющееся по сети путем эксплуатации уязвимости в SMB.

Он изменяет системные файлы, добавляет новые папки, создает Windows задачи и добавляет файлы для заражения и взлома компьютерной системы. Большинство пользователей понятия не имеют, как эту угроза

Trojan-Ransom.Win32.Wanna установлена на их компьютере, пока их антивирусные программы определяют ее как вредоносную угрозу, вредоносную программу или вирус.

Trojan-Ransom.Win32.Gen:

Trojan-Ransom.Win32.Gen изменяет системные файлы, добавляет новые папки, создает Windows задачи и добавляет файлы для заражения и взлома компьютерной системы. Trojan-Ransom.Win32.Gen-это вирус, который загружается на вашем компьютере во время серфинга в интернете.

Trojan-Ransom.Win32.Phny:

Такие программы-вымогатели представляют собой разновидность вредоносного ПО, которое используется интернет-мошенниками для того, чтобы потребовать от цели выплаты выкупа. В большинстве ситуаций заражение Trojan.Win32.Phny.ry, безусловно, даст указание своим жертвам начать перевод средств с целью уменьшения последствий изменений, внесенных троянской инфекцией в гаджет жертвы.

В первом квартале 2021 года было отмечено снижение доли эксплойтов для уязвимостей пакета Microsoft Office, однако они все еще занимают лидирующую позицию с показателем 59%.

Первый квартал оказался богат не только на давно известные уязвимости, но и на уязвимости нулевого дня. В частности, большой интерес как со стороны специалистов по ИБ, так и со стороны злоумышленников вызвали уязвимости в популярном Microsoft Exchange Server:

- CVE-2021-26855:

ProxyLogon — это название уязвимости CVE-2021-26855 (SSRF), позволяющей внешнему атакующему обойти механизм аутентификации в

MS Exchange и выдать себя за любого пользователя. Подделав запрос на стороне сервера, атакующий может отправить произвольный HTTP-запрос, который будет перенаправлен к другому внутреннему сервису от имени машинного аккаунта почтового сервера;

- CVE-2021-26857:

Позволяет злоумышленникам выполнить произвольный код от имени системы (для ее использования требуются либо права администратора, либо эксплуатация предыдущей уязвимости);

- CVE-2021-26858:

Эта аутентификация в ECP с последующей эксплуатацией уязвимостей CVE-2021-26858 для загрузки веб-шелла на сервер. Для того чтобы атакующий мог выдать себя за администратора при установлении сессии, ему необходимо узнать SID учетной записи администратора почтового сервера.

Например, мы можем рассмотреть для WannaCry BDU:2022-02174: Уязвимость реализации сетевого протокола Windows SMB операционной системы Windows, позволяющая нарушителю выполнить произвольный код.

Находится в таких операционных системах и аппаратных платформах, как:

- Microsoft Corp. Windows Server 2008 R2 SP1 64-bit;

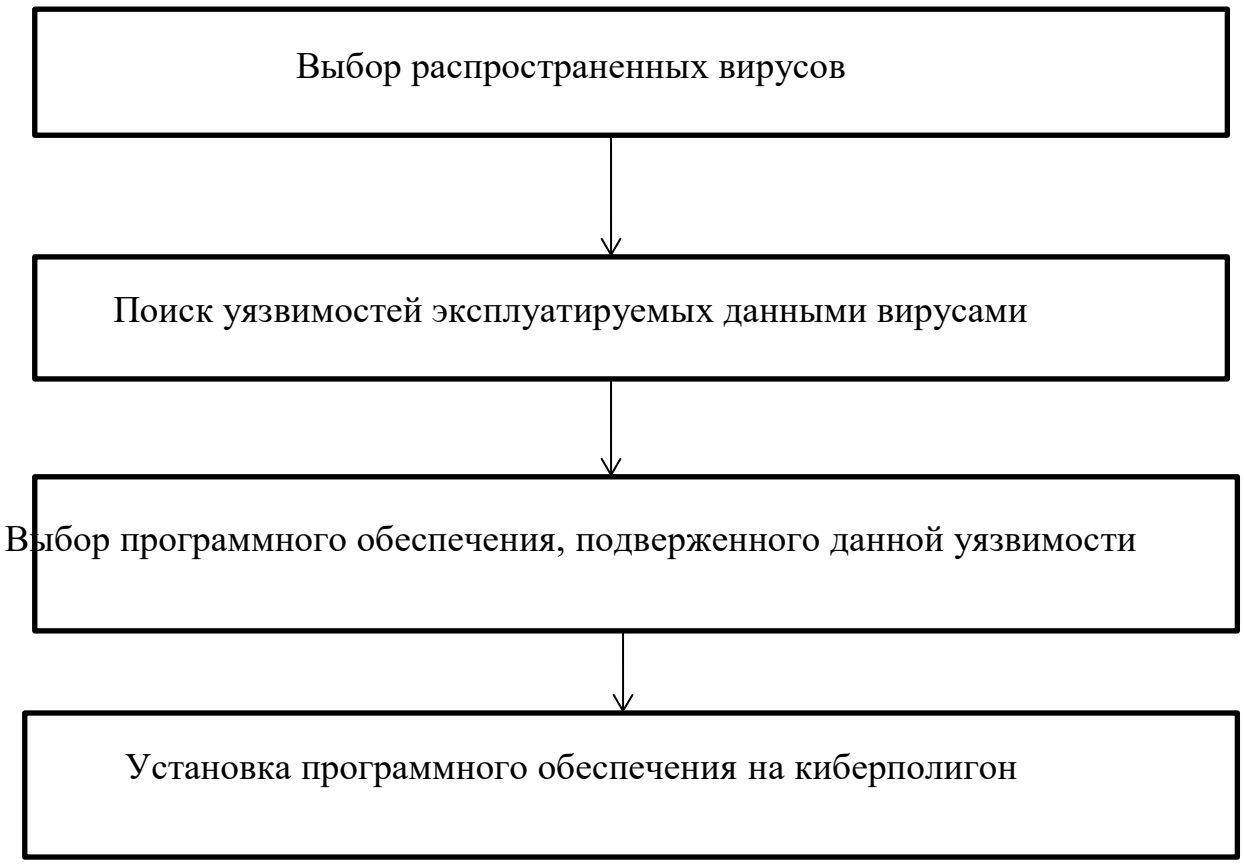
- Microsoft Corp. Windows 7 SP1 64-bit;

- Microsoft Corp. Windows Server 2008 SP2 32-bit;

- Microsoft Corp. Windows 7 SP1 32-bit;

- Microsoft Corp. Windows 8.1 64-bit.

Таким образом, мы понимаем, что сотрудникам различных предприятий для мониторинга событий информационной безопасности необходимо для тренировок использовать киберполигон. Тренировки должны производится с угрозами, которые по статистике являются наиболее актуальными для эффективности действий с реальными угрозами.



СПИСОК ЛИТЕРАТУРЫ

1. https://fstec.ru/
2. https://bdu.fstec.ru/threat
3. https://securelist.ru/it-threat-evolution-q1-2021-non-mobile-statistics/101518/
4. https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A2%D1%8F%D0%B6%D0%B5%D0%BB%D0%BE_%D0%B2_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D1%83%D1%87%D0%B5%D0%BD%D0%B8%D1%8F%D1%85,_%D0%BB%D0%B5%D0%B3%D0%BA%D0%BE_%D0%B2_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8
5. https://stakhanovets.ru/blog/issledovanie-ugrozy-informacionnoj-bezopasnosti-chast-1-statistika/
6. Ю. Родичев "Нормативная база и стандарты в области информационной безопасности" (2017)
7. Е. Баранова, А. Бабаш "Информационная безопасность и защита информации" 3-е изд. (2016)
8. С. Нестеров "Основы информационной безопасности" (2016)
9. А. Бирюков "Информационная безопасность: защита и нападение" 2-е изд. (2017)
10. «Кибербезопасность: стратегии атак и обороны» — Юрий Диогенес, Эрдаль Озкайя

Лисютин П.А.
АО «НИИ «Кулон», инженер-конструктор
МТУСИ, аспирант
pavelis@yandex.ru

ПОМЕХОЗАЩИЩЕННОСТЬ И УЯЗВИМОСТЬ ПРОВОДА ВИТОЙ ПАРЫ КАК СРЕДЫ РАСПРОСТРАНЕНИЯ СИГНАЛА НА ФИЗИЧЕСКОМ УРОВНЕ МОДЕЛИ OSI

Введение. Информация в цифровом виде, скомпонованная в пакет данных по протоколу, TCP/IP стандарта IEEE 802.3, передаваемая по витым медных парам проводов технологии Ethernet 10(100(1000))-(G)Base-T(4,X), состоящая из последовательности битов (байтов), и преобразованная после избыточного (помехоустойчивого) логического кодирования и скремблирования (перемежения нулей и единиц) в последовательность электромагнитных импульсов поступит в приемо-передающие (Rx Tx) линии связи сетевого устройства.

Сформированный на схемотехническом (аналоговом) уровне импульс требуемой по напряжению (и заданной длительности) формы за счет мгновенной (равной скорости света) скорости распространения электро-магнитной волны мгновенно одновременно появится на сетевых устройствах приема передачи: входах(выходах) маршрутизатора и(или) сетевой карте вычислительных устройств**.**

Для некоторых радиотехнических нужд был изготовлен работоспособный кабель с разъемами 8P8C (патчкорд) (рис.1), в котором применен иной тип провода, отличный от проводов сетевых кабелей (UTP, FTP, STP).

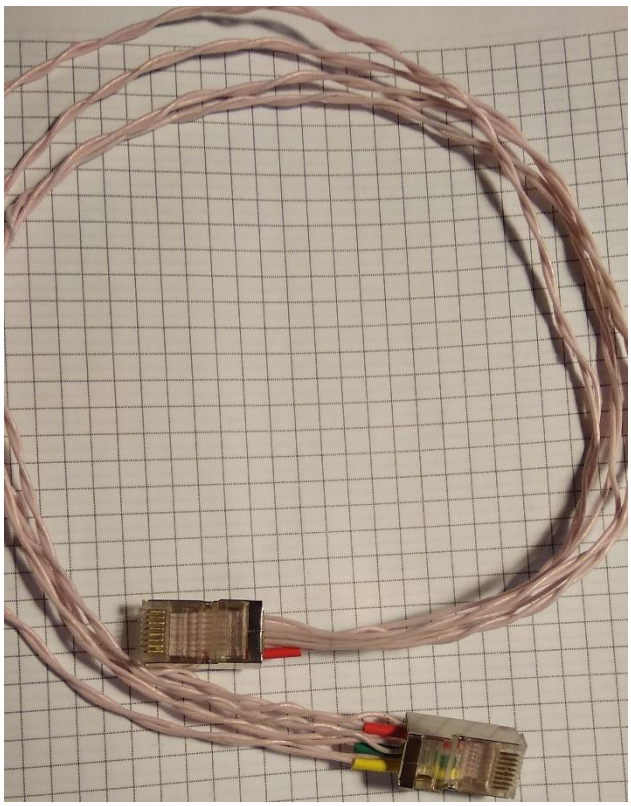


Рис. 1. Экспериментальный кабель

Как видно из Рисунка 1 без общей внешней изоляции конфигурация геометрического расположения витых пар может меняться.

Допустим для осуществления атаки «Man-in-the-Middle» мы включили кабель в локальную сеть с помощью соединителя для интернет-кабеля RJ45-RJ45(мама-мама).

На сколько сложна реализация атаки?

Методом «мозгового штурма», при котором ни одна из гипотез на этапе первоначальной генерации не отбрасывается, составлена структурная схема (рис.2).

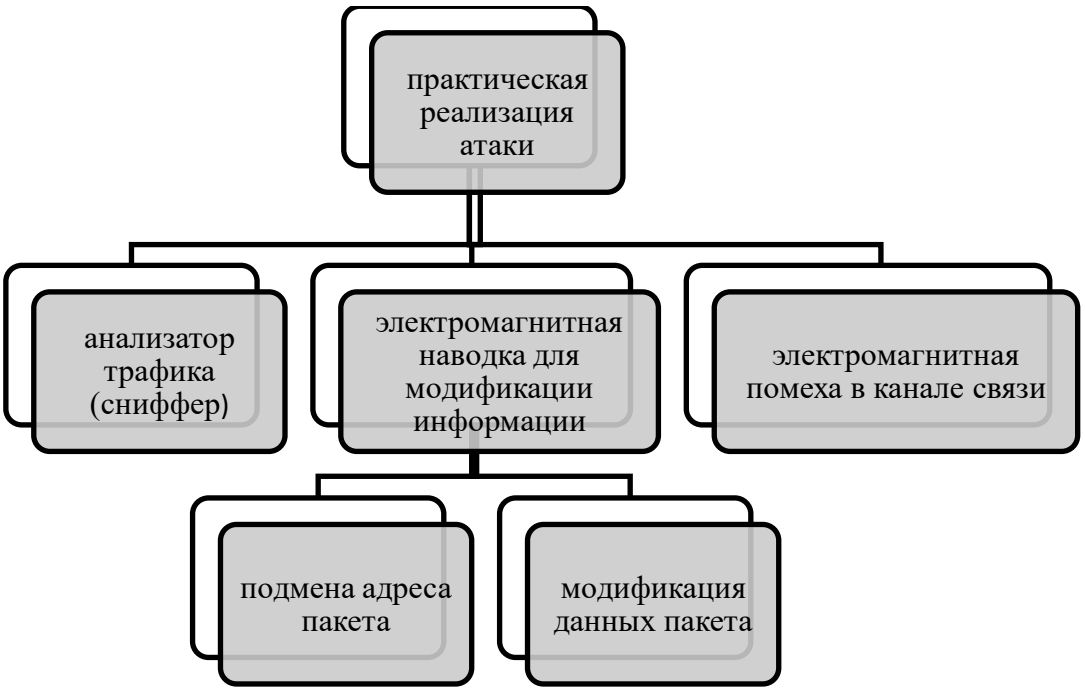


Рис. 2. Задачи модификации кабеля

Для отсева нереализуемых на практике задач, обратимся к теории.

Физический уровень сетевой модели OSI

Физический уровень определяет электротехнические, механические, процедурные и функциональные характеристики активации, поддержания и дезактивации физического канала между конечными системами. Спецификации физического уровня определяют уровни напряжений, синхронизацию изменения напряжений, скорость передачи физической информации, максимальные расстояния передачи информации, требования к среде передачи, физические соединители и другие аналогичные характеристики.

Пожалуй, простым способом исследования было бы найти и перевести стандарт, но на 700 страницах IEEE 802.3 [1] обнаружилось такое обилие технических терминов, что уловить их взаимосвязь сходу не удалось, пришлось подступаться с аппаратной части (hardware) начиная с проводов.

Изначально витая пара придумана как способ укладки проводов для снижения электромагнитных наводок при совместной прокладке телефонных проводов (рис.3).

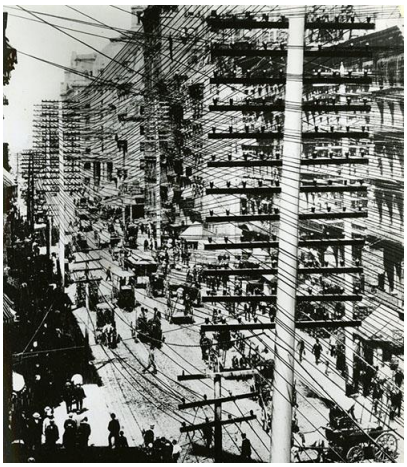


Рис. 3. Предпосылка исторического изобретения витой пары

Технические характеристики проводов витых пар, применяемых в кабелях UTP, FTP, STP категории 5e-7e, AWG 24 - AWG26 (сечением жилы 0,2 и 0,14 мм^2) диаметр которых по изоляции (как правило полиэтиленовой или поливинилхлоридной PVC) примерно равен 0,9 мм были заложены в стандарте Ethernet 10Base-T. Производители магнитных трансмиттеров (Pulse Electronics) и процессоров AMD в кооперации в 1993 году разработали американский стандарт ANSI «XT3T9.5 for Unshielded Twisted Pair operation» [2].

Были изучены технические условия (datasheet) - микроконтроллеров сетевых плат 10Base-T, 100-Base-T производителей Intel 82558 [3], Via VT6105 [4] и Realtek RTL 8139D[5], кристалл микроконтроллера был извлечен корпуса и увеличен под микроскопом (рис. 4).

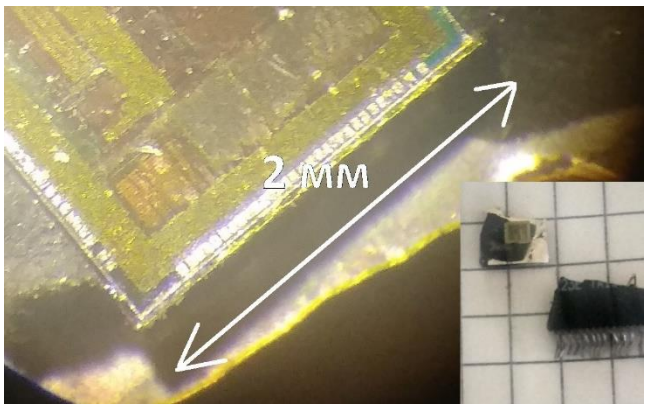


Рис. 4. Кристалл микроконтроллера сетевой платы под микроскопом

Линия из двадцати пяти контактов на каждой из сторон – 1,8 мм, итого площадь контакта по которому приходит каждый сигнал приема-передачи - 0,1 мм х0,1 мм=0,01 мм^2.

Пятнадцатикратный (0,14/0,01) запас по сечению проводов витой пары используется для технологического удобства изготовления проводов в кабеле, уменьшения их затухания с расстоянием.

Сравнив технические условия производителей микроконтроллеров устаревших сетевых плат 1996-2002 г.в. удалось разобраться со следующим: аналоговый («физический») сигнал зависит от ***скорости*** применяемого в сетевой карте (рис. 5) стандарта ***Ethernet*** (Таблица 1), разделение цифрового сигнала в ***дифференциальный***, передаваемый на расстояние в витой паре, выполняется в магнитном трансмиттере (рис. 6), аналоговый сигнал не просто ***чередование импульсов и пауз*** в повторении единиц и нулей из сформированного, состоящего из адресной и информационной частей пакета данных TCP/IP – сигнал ***многоуровневый*** по амплитуде, подготовленный для передачи: ***кодированный*** и ***скремблированный*** (рис. 7), ***с синхронизацией*** скорости (рис.8)**.**

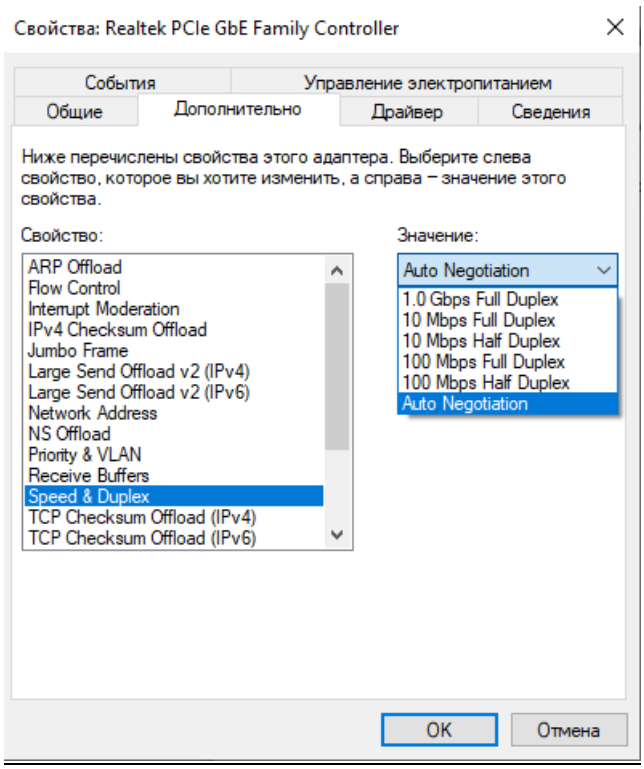


Рис. 5. Выбор скорости приема-передачи в свойствах сетевого адаптера

Таблица 1. Сравнение стандартов Ethernet витой пары.

№ п/п	Название протокола	Краткое описание
1.	10BASE-T, IEEE 802.3i	Как и стандарт 10Base2, локальные сети класса 10BaseT обеспечивают передачу данных со скоростью 10Мбит/с, Для обмена информации используется две пары: одна для приема сигнала, вторая - для передачи.
2.	100BaseTX	Использование стандартной витой пары пятой категории, в которой задействовано только четыре проводника из восьми имеющихся: два - для приема данных, и два - для передачи.
3.	100BaseT4	В сетях также используется витая пара, однако в ней задействованы все восемь жил проводника: одна пара работает только на прием данных, одна - только на передачу, а оставшиеся две

		обеспечивают двунаправленный обмен информацией.
4.	1000BASE-T, IEEE 802.3ab	Стандарт, в котором используется витая пара категории 5e. В передаче данных задействовано 4 пары. Скорость передачи данных составляет 250 Мбит/с по одной паре. В стандарте применен пятиуровневый метод кодирования PAM5.
5.	1000BASE-TX	Используется раздельная приемо-передача конструкция Существенным отличием 1000BASE-TX является отсутствие схемы цифровой компенсации наводок и возвратных помех, однако, для стабильной работы по такой технологии необходимо использовать лишь кабель 6 категории.
6.	10GBASE-T,	IEEE 802.3an-2006 — стандарт принят в июне 2006 года, спустя 4 года разработки. В нем используется экранированная витая пара. Расстояние работы — до 100 метров. В стандарте применен метод кодирования PAM16.
7.	10BASE-T1L 802.3cg-2019	Новый стандарт передачи Ethernet 10BaseT по двух проводам (одной витой пары). См. источник [6].

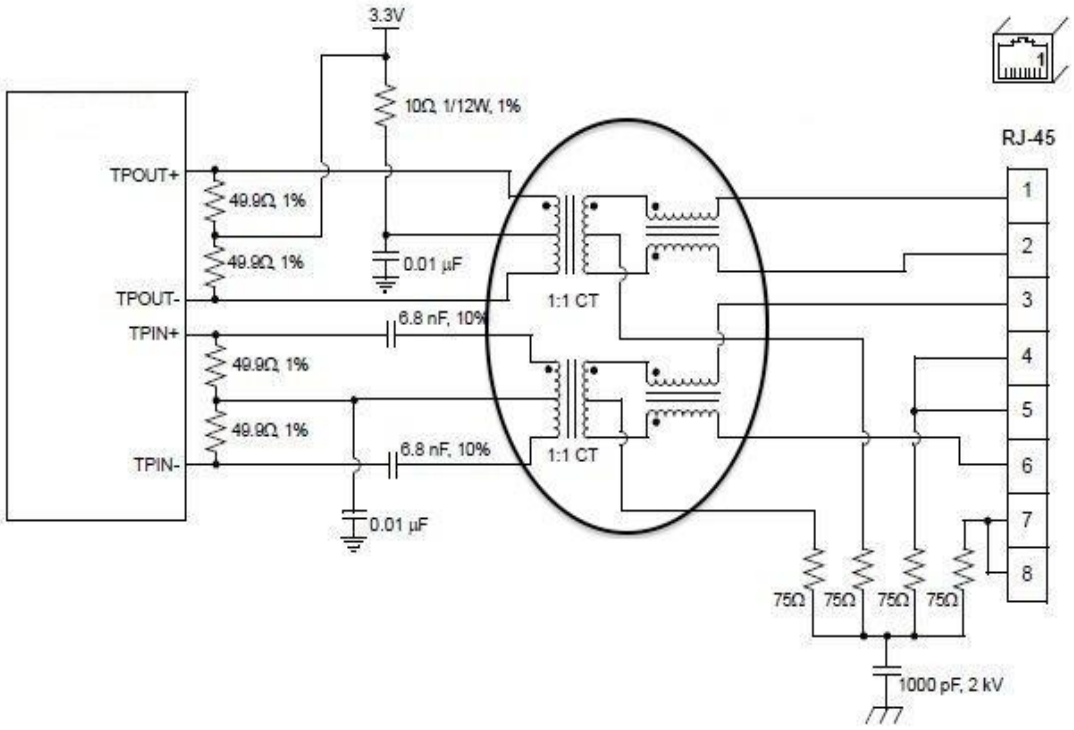


Рис. 6. Электрическая принципиальная схема и внешний вид магнитного трансивера стандарта Ethernet 10Base-T

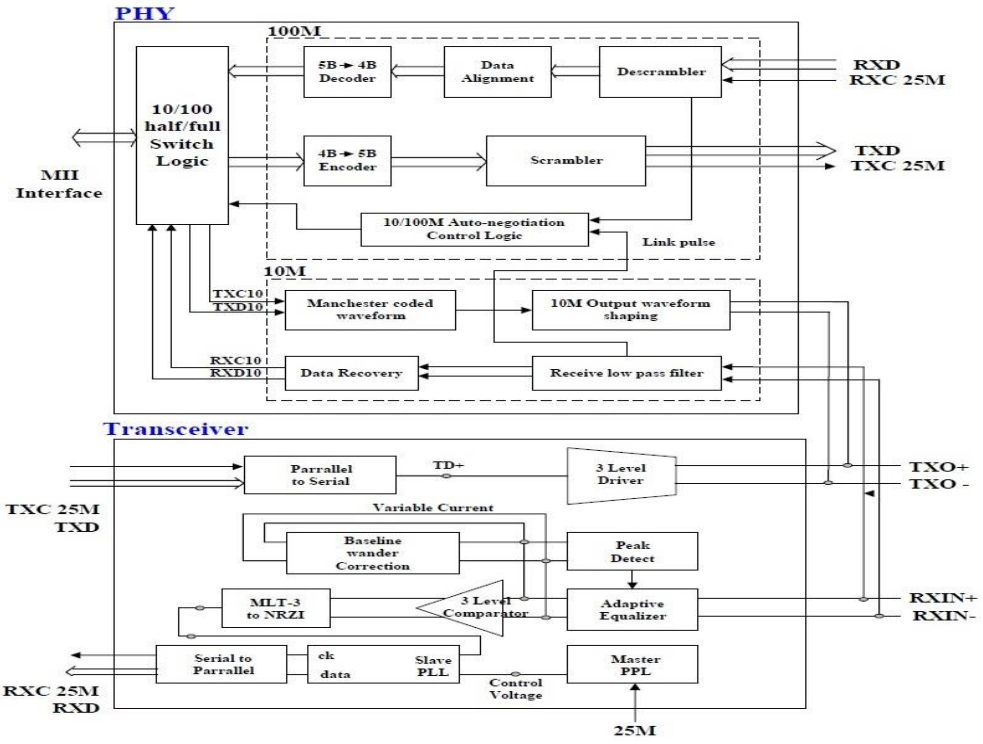


Рис. 7. Блок схема кодировки сигнала на физическом уровне Ethernet

TP Interface

10BaseT Normal Link Pulse Timing (0 < Tpd < 300)

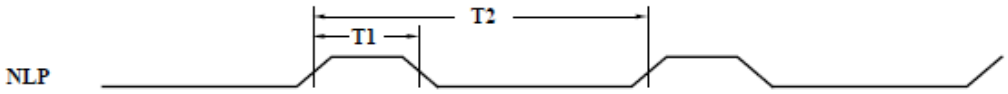


Figure 18. 10Base-T Normal Link Pulse Timing (0 < Tpd < 300)

Symbol	Parameter	Min	Typ	Max	Unit
T_1	NLP Pulse Width		100		ns
T_2	NLP TO NLP Period		12		ns

Auto Negotiation Fast Link Pulse Timing (0 < Tpd < 300)

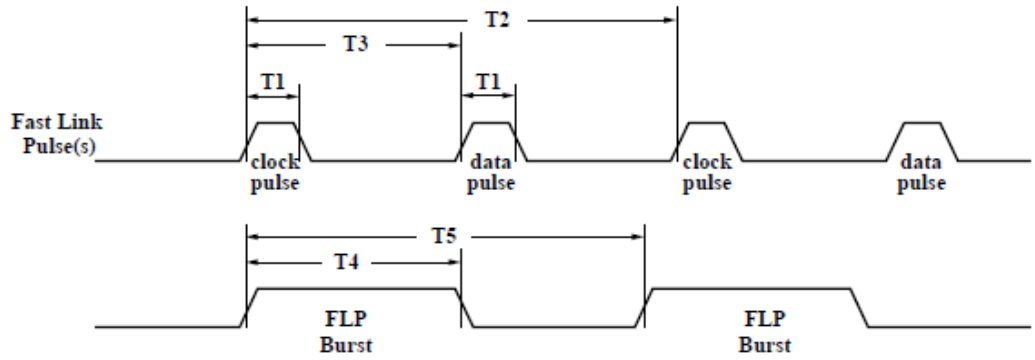


Figure 19. Auto Negotiation Fast Link Pulse Timing (0 < Tpd < 300)

Symbol	Parameter	Min	Typ	Max	Unit
T_1	Clock, Data Pulse Width		100		ns
T_2	Clock Pulse to Clock Pulse Period		125		µs
T_3	Clock Pulse to Data Pulse Period		62.5		µs
T_4	Burst Width		4.2		ns
T_5	FLP Burst to FLP Burst Period		8.5		ns

Рис.8. Временные диаграммы для фиксированной скорости 10Мбит/с и в режимае Автосогласования до 100Мбит/с

Выводы: для обнаружения сигнала в дифференциальной паре теоретически может быть достаточно лишь одного сигнала из пары, в этом случае для распознавания дуплекса потребуется двухканальный

осциллограф с полосой пропускания не менее 50МГц для 100BaseT и четырехканальный для 100BaseT4 (с полосой 50МГц) и 1000BaseT (500МГц).

Оценка возможностей нетривиальной модификации кабеля

Конкурентная предпосылка модификации кабеля: крайне маловероятная возможность его обнаружения сетевыми программно-аппаратными устройствами.

Объективные условия применения кабеля:

- сегмент проводных линий связи по витой паре вытесняется оптическими линиями связи (в т.ч. технологии PON - Passive Optic Network), беспроводными способами передачи (мобильный интернет, Wi-fi);

- для установки кабеля требуется физический доступ к ЛВС;

- в отличие от адресной части - данные в передаваемых пакетах часто защищены различными способами передачи с шифрованием, соответственно, вероятность распознавания пусть даже достоверно полученной зашифрованной «последовательности битов» невысока.

Информация о программных снифферах представлена в источнике [7].

Необходима оценка окупаемости ресурсов на создание «аппаратного» сниффера в условиях конкурентного существования программных.

Для оценки использования приспособления не сниффером а для применения электромагнитной наводки (помехи) в источнике [8] найдена информация о современных устройствах тестирования ЛВС.

Для витых пар доступен анализ «разбиение пар кабелей, наличие кабельных вставок, отводов, пупиновских (в начале 20 века М. Пупин предложил встраивать в линию катушки с индуктивностью, которая превышает собственную индуктивность телефонной линии почти на два порядка, и тем самым значительно снижать затухание в диапазоне частот до 3 кГц) катушек и других неоднородностей (вставки отрезков кабеля другого типа)».

Это приборы ПКМ-4МЦ (измерение параметров и обнаружение неисправностей кабелей), Fluke 1507/1503 (измерение сопротивления изоляции), генератор – селективный измеритель уровня PSM-137/139 (измерения в полосе частот спектра сигнала), рефлектометр HST-3000 (измерение характеристик медных кабелей), 3M Dynatel 1965AMS.

Можно ли использовать приспособление в стеганографии?

В общем виде сетевая стеганография является семейством методов по модификации данных в заголовках сетевых пакетов и в передаваемой полезной нагрузке с использованием протоколов прикладного уровня, по изменению структуры передачи пакетов и гибридных методов в том или ином сетевом протокол (в подавляющем большинстве случаев TCP/IP но и не исключая протокол UDP – без подтверждения доставки) [9].

Рис. 9 Методы TCP/IP стеганографии

К сожалению, для радиоканала нельзя таким же образом отличить искусственные помехи от естественных. Однако можно отсечь ошибки, возникающие в результате DoS-атак, поставив необходимые фильтры. Но всё это делается на более высоком уровне, чем физический.

Как быть с вносимой средством измерения (осциллографом) помехой при «считывании» и записи последовательности сигналов с проводов?

Не нарушится ли синхронизация (появление джиттера)?

Вести запись последовательности импульсов как архив данных или использовать для записи программные продукты систем реального времени?

Кроме того остались невыясненными вопросы измерения джиттера на осциллографе способом «глазковых диаграмм».

Не полностью изучены характеристики импульса цифровой связи согласно стандарту ГОСТ 27763-88 [10].

Заключение

Пробный стенд измерения электрических параметров стандарта Ethernet 100Base-T из цифрового осциллографа Owon SDS7102E (с полосой 100 МГЦ) (рис. 10) ,экспериментального кабеля (пачткорда) №2, ноутбука для генерации трафика через PON маршрутизатор Huawei Echolife HG8245 (не показан) представлен далее (рис.10).

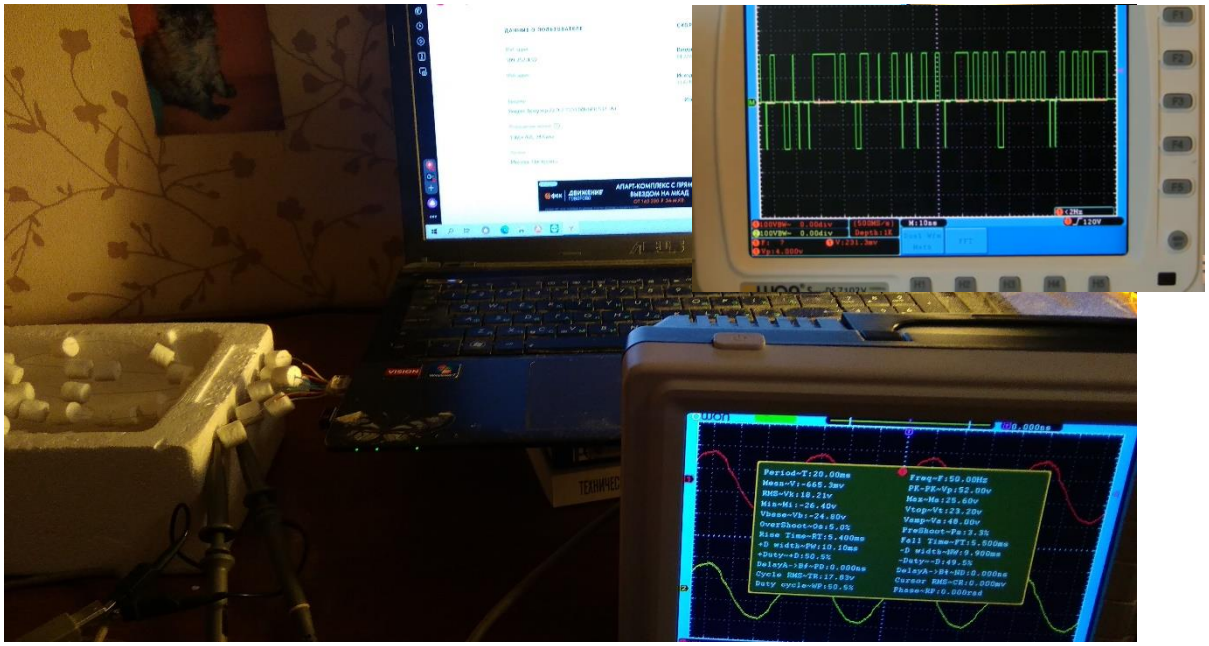


Рис. 10. Пробный стенд измерения электрических характеристик

На работоспособном экспериментальном кабеле №2 вместо витых пар использованы прямые участки стальных (магнитных) проводов (проволок из полевого кабеля П274М), разведенных пенопластовыми изоляторами. Тестовый трафик генерировался онлайн сервисом «проверка скорости Интернет».

Результате не совсем ясен: не является ли попытка модификации кабеля «изобретением» аналога магнитного трансмиттера вышеупомянутой Pulse Electonics? Можно ли изменив электрические параметры среды физического уровня модели OSI: навести «сигнал-трафик» для «не Ethernet» канала связи?

Практическая ценность работы: предпосылка для создания оригинального обучающего лабораторного макета для изучения электромагнитных характеристик среды передачи данных физического уровня OSI.

Список источников информации

1. IEEE 802.3-2008 «Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method and Physical Layer specifications» https://opencores.org/websvn/filedetails?repname=1000base-x&path=%2F1000base-x%2Ftrunk%2Fdoc%2F802.3-2008_section2.pdf&bcsi_scan_91c2e97ef32f18a3=V1Ygi7liGXdis80J3CYk1MUlxZsSAAAACY4+BA%3D%3D+
2. ANSI XT3T9.5 https://www.amd.com/system/files/TechDocs/18258.pdf
3. Техническое описание микроконтроллера Realtek RTL8139D , 2001 г
4. Техническое описание микроконтроллера Intel 82558, 1996г.
5. Техническое описание микроконтроллера Via VT6105, 2002г.
6. Четвертушка Ethernet-а: старая скорость, новые возможности 802.3cg-2019 https://habr.com/ru/post/489314/

7. Скорых М., Израилов К., Башмаков А., Задачаориентированное сравнение средств анализа сетевого трафика, Сборник трудов всероссийской гаучно-технической конференции Теория и практика обеспечения информационной безопасности, М, МТУСИ, 2021 ,стр.104-108.
8. И.Власов, Э.Новиков, Техническая диагностика современных цифровых сетей связи, Горячая линия-Телеком, 2019. -480 с. ISBN 978-5-9912-0195-7
9. Е. Крапухин, Методы срытой передачи информации, М.: Горячая линия-Телеком, 2020. -80 с. ISBN978-5-9912-0851-2
10. ГОСТ 27763-88 Структуры циклов цифровых групповых сигналов. Первичной сети единой автоматизированной сети связи Требования и нормы». https://docs.cntd.ru/document/1200016555

Потапова К.А.,
Аспирант, Морской, государственный университет им. адм. Г.И. Невельского, г.Владивосток, Россия
smirnovaksenia2018@inbox.ru

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ С МОРСКОГО СУДНА НА БЕРЕГ В УСЛОВИЯХ ОГРАНИЧЕННОГО КАНАЛА СВЯЗИ

Актуальность темы исследования заключается в том, что основная специфика мореплавания заключается в постоянной передаче информации с морского судна на берег. С помощью осуществления контактов удается осуществлять взаимодействие с удаленными от стационарных береговых баз на сотни миль. Хорошая и отлаженная связь способствует обеспечению информационной безопасности и позволяет осуществлять руководство с крупными морскими соединениями и их подразделениями. Однако существуют проблемы передачи информации через системы связи, такие как затухание сигнала, шум, теневые зоны, многолучевое распространение сигналов, замирание сигнала, его ограниченность и т.д. Данные проблемы создают огромные препятствия и снижают безопасность движения морского судна в открытом пространстве.

Вопросами изучения проблем передачи информации с морского судна на берег в условиях ограниченного канала связи занимались многие ученые. Среди работ, которых можно отметить труды С.В. Петрова, В.Н. Платонова, С.И. Гуськова и других. Необходимо продолжить исследование в данном направлении и более углубленно изучить отдельные вопросы темы.

В данной статье предпринята попытка изучения проблем передачи информации с морского судна на берег в условиях ограниченного канала связи.

Следует отметить, что самым лучшим и надежным каналом связи является радиосвязь. Использование данного вида связи позволяет с высокой

точностью определить местонахождение судна, обозначить его координаты, установить связь с портом назначения, узнать погодные условия, подать сигнал об аварийности судна. Кроме того, в условиях цифровизации и глобализации общества широкое распространение получила глобальная морская система связи, включающая в себя навигационные спутниковые системы связи, цифровые инструменты управления движения судна, автоматизированную идентификационную систему и контроль безопасности.

В основе передачи информации с морского судна на берег лежит принцип передачи физического сигнала на расстоянии (дистанционно). Под сигналом в данном случае понимается специальный условный код (знак), переданный по каналу связи одной системой (в данном случае с борта морского судна) на другую систему (находящуюся на берегу). Сигналы могут быть постоянные и периодические. Периодический сигнал – это сигнал, повторяющийся через определенные промежутки времени. Постоянный сигнал – это непрерывный сигнал, подающийся морским судном на берег.

Рассмотрим более подробно основные проблемы передачи информации с морского судна на берег в условиях ограниченного канала связи. Одной из важных проблем является проблема затухания сигнала. То есть когда сигнал проходит по каналу связи его собственная амплитуда уменьшается и сигнал падает. Затухание сигнала происходит с увеличением роста частоты. В свою очередь из-за большого затухания происходит искажение информации, появляются шумы или сигнал может вообще пропасть [3].

Еще одной важной проблемой является проблема шума при передаче сигнала. Атомы и молекулы при передаче сигнала вибрируют и излучают электромагнитные волны в виде исходящего шума. Шум создает фоновый уровень и вызывает ошибки в передаче информации. Высокий уровень шума приводит к потере сигнала, передаваемого с морского судна на берег.

Теневые зоны представляют собой ухудшение передачи информации вследствие влияния различных помех и препятствий. Так как металлические

предметы непроницаемы для радиоволн сантиметрового диапазона, то пространство, находящееся непосредственно позади препятствия, окажется в тени. Величина теневой зоны зависит от размеров препятствия и расстояния от него до антенны. В отдельных теневых зонах передача информации может вовсе отсутствовать.

Следующей проблемой является проблема многолучевого распространения сигналов. Основной причиной возникновения многолучевого распространения сигналов является их отражение от различных объектов на пути передачи сигнала. Так как в пространстве существует всегда несколько путей распространения сигналов, то различные варианты и копии одного и того же сигнала интерферируют друг с другом, которые в свою очередь вызывают эффект замирания [1].

Замирания оказывают прямое влияние на качество передаваемой связи от морского судна на берег. Длительное замирание ведение к остановке или длительной передаче данных, а иногда к их потере в информационном пространстве. Если происходит замирание с искажением передачи информации в течение определенного периода времени, то такие замирания называются селективными [6]. Считается, что лучшим способом борьбы с замираниями является разнесение сигнала.

Условия ограниченности канала связи при передаче информации с морского судна на берег может быть вызвано различными причинами. Так, например, погодные условия могут нарушить прием и передачу информации, вызвать ее искажение или потерю. Нарушить данные условия также может фактор профессиональной некомпетентности членов экипажа судна, которые должны обладать рядом коммуникативных умений и навыков: умением принимать и отправлять сообщения, знать и понимать значения передаваемых сигналов с морского судна на берег, вести постоянный контроль и наблюдение при передаче информации, устанавливать связь с

другими объектами, в случае аварийности или бедствия подать необходимый сигнал связи и т.д. [2].

Считаем, что данные проблемы передачи информации должны быть устранены на основе применения комплексного подхода, а именно со стороны руководства морского судна, а также поддержки государства в реализации программы обеспечения информационной безопасности.

В данной статье разработан алгоритм повышения эффективности передачи информации с морского судна на берег в условиях ограниченного сигнала связи, наглядно представленный на рисунке 1.

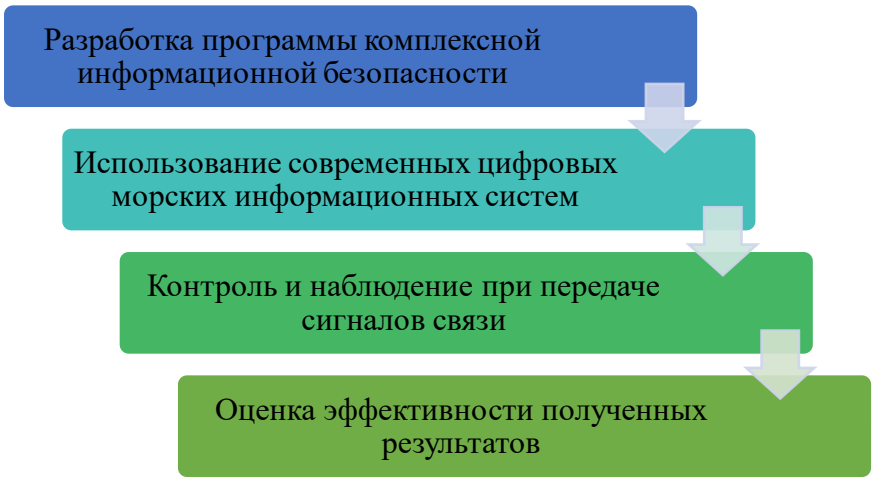


Рис.1. Алгоритм повышения эффективности передачи информации с морского судна на берег в условиях ограниченного сигнала связи

Представленный алгоритм позволит решить основные проблемы передачи информации по каналам связи, а также повысить уровень информационной безопасности в условиях ограниченного канала связи.

В целом можно сделать вывод, что существующие проблемы передачи информации с морского судна на берег в условиях ограниченного канала связи требуют комплексного подхода к их решению. Совокупный положительный эффект достигается в случае снижения возможных рисков и потерь, а также сохранения надежности передачи данных по каналам связи.

СПИСОК ЛИТЕРАТУРЫ

1. Казанцев, А. М. Научная организация труда на речном транспорте / А.М. Казанцев, С.С. Слуцкий. - М.: Транспорт, 2019. - 224 с.

2. Мочалова, Я.В. Влияние образования на формирование личности / Я.В. Мочалова // Актуальные проблемы развития науки и современного образования. - Белгород: ИД «Белгород» НИУ «БелГУ». - 2017. - С. 246-247.

3. Радиосвязь на внутренних водных путях [Электронный ресурс] общий доступ: https://mys.ru/Article_87.html

4. Передача данных [Электронный ресурс] общий доступ: https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D0%B5%D0%B4%D0%B0%D1%87%D0%B0_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85

5. Передача сигналов по линиям связи [Электронный ресурс] общий доступ: http://book.itep.ru/2/21/trans_21.htm

6. Проблемы передачи информации по системам связи [Электронный ресурс] общий доступ: https://cyberleninka.ru/article/n/problemy-peredachi-informatsii-po-sistemam-svyazi

7. Исследование передач сигналов по частично ограниченному каналу [Электронный ресурс] общий доступ: .https://stud.wiki/radio/3c0b65635a3ad79b5c43a88421206d26_0.html

8. Прохождение дискретного сигнала по частотно-ограниченному каналу [Электронный ресурс] общий доступ: https://otherreferats.allbest.ru/radio/00708040_0.html

9. Разработка и применение алгоритма цифровой обработки сигналов при передаче данных [Электронный ресурс] общий доступ: http://vunivere.ru/work97751

10. Способы получения и передачи информации. [Электронный ресурс] общий доступ: https://leally.ru/internet/sposoby-polucheniya-i-peredachi-informacii-v-informatike-kakimi-sposobami/

Шукенбаев А.Б.
РТУ МИРЭА, доцент
к.т.н., доцент
shukenbaev@mail.ru
Мирзоева Л.В.
специалист банка ВТБ
lyaman1031@mail.ru

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДИК ТЕСТИРОВАНИЯ БЕЗОПАСНОСТИ ПРОЕКТОВ

Тестирование безопасности проектов является необходимым первым шагом для организаций, целью которых является определение уровня информационной безопасности и ее повышения для укрепления защиты.

В связи с этим становится актуальным проведение анализа известных методик и стандартов тестирования безопасности проектов.

Каждая отдельная методология описывает процесс, который организация может выполнить для обнаружения уязвимостей. Компании могут как создать свою внутреннюю методологию, так и использовать уже существующую, но чаще всего специалисты проводят тестирование безопасности согласно известным методикам.

По нашему мнению, к наиболее авторитетным методикам и стандартам относятся:

– Руководство по методологии тестирования безопасности с открытым исходным кодом OSSTMM [1];

– Руководство по тестированию безопасности веб-приложений OWASP WSTG [2];

– Техническое руководство по тестированию и оценке информационной безопасности NIST SP800-115 [3];

– Стандарт выполнения тестирования на проникновение PTES [4];

– Методика оценки безопасности информационных систем ISSAF [5];

– Методология изучения модели тестирования на проникновение BSI SPTM [6],

– Методика Positive Technologies [7].

В ходе анализа различий методик и стандартов тестирования безопасности можно сделать вывод о совпадении ряда аспектов данных документов. Несмотря на то, что количество схожих аспектов превалирует, документам присущи отличительные особенности. Ярко выраженные различия затрагивают следующие области:

– содержание методики,

– степень углубленности в технические вопросы,

– приведение примеров тестирования безопасности,

– приведение технических деталей проведения тестирования безопасности.

Так, методики OSSTMM, BSI SPTM и стандарт NIST SP800-115 характеризуются в большей степени теоретическим подходом к тестированию безопасности. Наиболее проработанной и узко-ориентированной на тестирование безопасности веб-приложений является методика OWASP WSTG. Методика ISSAF отличается тем, что содержит в себе как теоретический, так и практический подход к тестированию на проникновение. Отметим также, что стандарт PTES является практико-ориентированным и содержит совокупность технических рекомендаций и определенных уязвимостей, которые необходимо проверять при проведении тестирования на проникновение, подробно изложенные вопросы тестирования безопасности беспроводных и телекоммуникационных сетей.

На основе проведенного сравнительного анализа была выбрана методика OWASP WSTG для тестирования безопасности веб-приложения банка ВТБ.

Для проведения тестирования безопасности проектов существуют различные бесплатные и платные инструментальные средства: Kali Linux [8], Acunetix WVS [9], Netsparker [10], Burp Suite Professional [11], OWASP ZAP [12] и другие.

Инструментальные средства тестирования безопасности проектов являются ключевыми в бизнес-стратегии компании. Тестировщику необходимо составить перечень необходимых инструментов для проведения тестирования в зависимости от функциональности системы и приложения, эффективности и скорости поиска, а также цены, которая должна быть сравнима с ценностью защищаемой информации, поскольку универсальных инструментов не существует.

Рассмотрим практическую реализацию на примере тестирования безопасности выше названного веб-приложения.

Перед проведением тестирования безопасности веб-приложения сотрудники отдела тестирования безопасности банка составляют техническое задание. Далее сотрудники блока «Управление и обеспечение» знакомятся с данным документом и вносят правки при необходимости.

Модель тестирования безопасности веб-приложения состоит из:

– группы специалистов по тестированию безопасности;

– инструментов, необходимых для проведения тестирования безопасности;

– методов тестирования безопасности.

С учетом проведенного анализа комплексное тестирование безопасности веб-приложения проводилось на основе методики OWASP и внутренней методики для оценки рисков. Для сканирования уязвимостей веб-приложения были использованы: OWASP ZAP, Acunetix WVS, Netsparker, Burp Suite Professional. Тестировщики рассматривают объект тестирования с позиции «черного ящика», то есть все действия должны выполняться

специалистами, находящимися в тех же условиях, что и потенциальный нарушитель.

В первой области выбираем режим сканирования:

– безопасный режим (отключает все вредоносные функции в процессе тестирования),

– защищенный режим (предотвращает сканирование нежелательных сайтов),

– стандартный режим (доступны любые действия с веб-приложением),

– режим атаки.

Во второй области отображаются все посещенные URL-адреса в древовидной структуре.

Третья область является рабочей и включает в себя 3 вкладки:

– быстрый старт (способ начать активное сканирование),

– запрос (показывает данные, которые браузер отправляет в веб-приложение, содержит заголовок и тело запроса),

– ответ (показывает данные, которые веб-приложение отправляет обратно в браузер, содержит заголовок и тело ответа).

Четвертая область является информационной и включает в себя следующие вкладки:

– история запросов (показывает запросы в том порядке, в котором они были сделаны),

– поиск (позволяет искать регулярные выражения во всех URL-адресах, запросах, ответах, заголовках и других функциях, предоставляемых надстройками),

– оповещения (отображаются предупреждения (уязвимости), которые были вызваны в этом сеансе),

– вывод (показывает различные информационные сообщения).

В результате сканирования веб-приложения в стандартном режиме получена его древовидная структура (вторая область) и список найденных

уязвимостей (четвертая область) (рисунок 1). При нажатии на существующую уязвимость можно получить ее описание с уровнем риска.

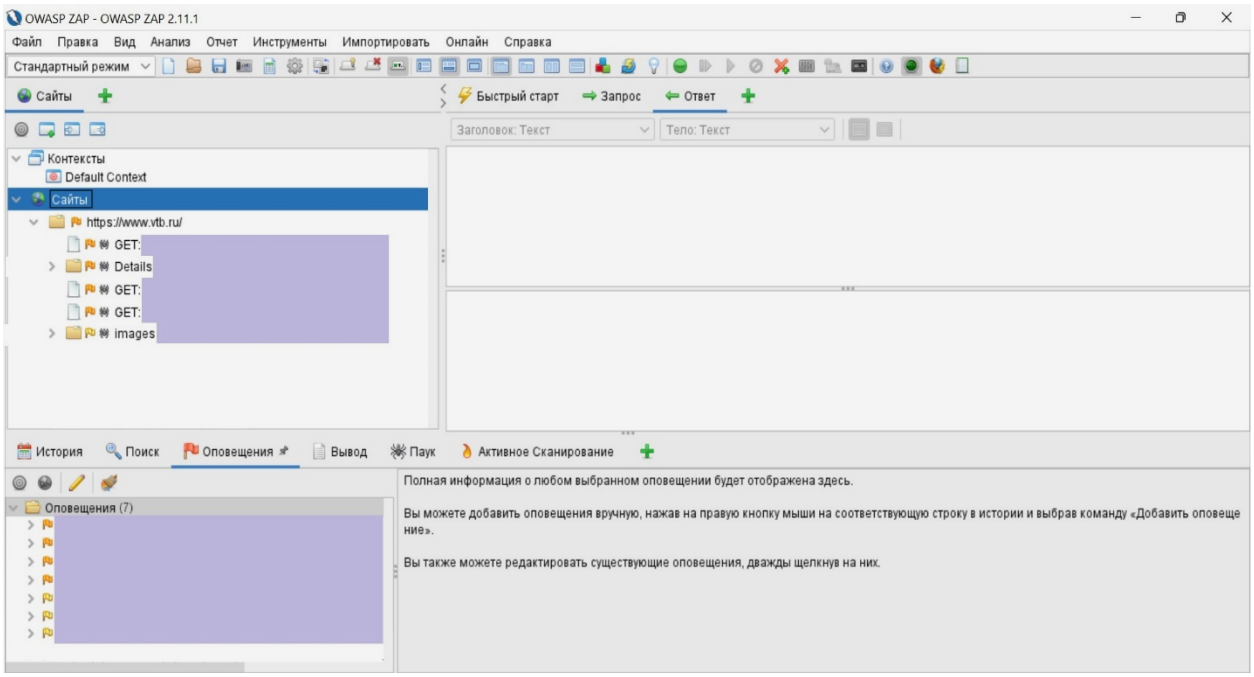


Рис. 1 – Результат сканирования веб-приложения

В тестируемом веб-приложении было обнаружено 7 уязвимостей: 3 с низким уровнем риска и 4 со средним. С критическим уровнем опасности обнаружено не было.

Также у инструмента OWASP ZAP есть возможность получения отчета по результатам сканирования веб-приложения, где присутствуют рекомендации по устранению уязвимостей.

Сканирование уязвимостей веб-приложения с помощью Acunetix Web Vulnerability Scanner, Netsparker, Burp Suite Professional не приводится.

Таким образом, с помощью инструмента OWASP ZAP мы увидели, что веб-приложение Банка ВТБ является безопасным и выявленные уязвимости некритичны.

На основе проведенного тестирования безопасности методика OWASP WSTG, на наш взгляд, представляет собой совершенный документ для анализа защищенности веб-приложения финансовой организации.

Несмотря на то, что инструмент OWASP ZAP автоматически присваивает каждой найденной уязвимости уровень риска, в организации выработали свою внутреннюю методику оценки рисков, по которой можно получить их точное описание и определить, какие из них необходимо устранить в первую очередь.

Использовали 2 шкалы:

1) шкала вероятности возникновения риска (рисунок 2),

2) шкала тяжести последствий при возникновении риска (рисунок 3).

При оценке применялся матричный метод (рисунок 4). Значение уровня риска определяется как пересечение шкалы вероятности возникновения и тяжести последствий при его возникновения.

В соответствии с методикой компании выделяются 3 уровня рисков:

1) Первый уровень (зеленый) – приемлемый уровень риска, не требующий разработки корректирующих мероприятий.

2) Второй уровень (желтый) – средний уровень риска, требующий разработку и внедрение корректирующих мероприятий.

3) Третий уровень (красный) – высокий уровень риска, требующий разработку и внедрение корректирующих мероприятий с высоким приоритетом.

Рис. 2 – Шкала вероятности возникновения риска

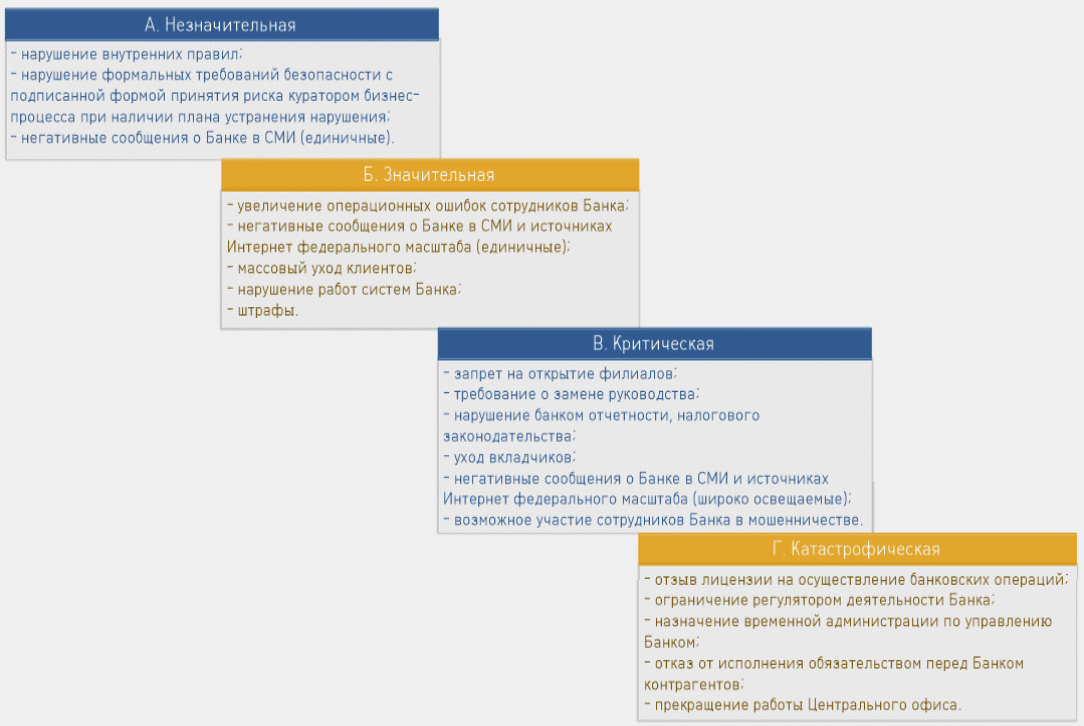


Рис. 3 – Шкала тяжести последствий при возникновении риска

	I	II	III	IV	V	VI
А	1	1	1	1	2	2
Б	1	1	1	2	2	2
В	1	1	2	2	3	3
Г	1	2	2	3	3	3

Рис. 4 – Матричный метод оценки рисков

После определения уровня риска необходимо разработать комплекс мероприятий для его исключения или снижения. Особое внимание должно быть уделено контролю рисков третьего уровня. Анализ по предотвращению таких ситуаций должен быть более глубоким и детальным, чем при обычной оценке. Также потребуется более тщательное планирование и внедрение мероприятий.

Корректирующие мероприятия подразделяются на:

– технические мероприятия (установка защитных систем, модернизация системы, отказ от системы);

– регуляторные мероприятия (процедуры, инструкции, памятки).

После разработки и внедрения мероприятий необходимо провести контроль их эффективности. Для этого нужно выполнить переоценку тех

рисков, которые ранее были идентифицированы с помощью инструментов.

Все действия специалиста должны быть занесены в специальную форму во внутренней системе банка.

Таким образом, оценка рисков является одним из основных элементов комплексного тестирования безопасности, поскольку позволяет выявить опасности, определить их величины и тяжести потенциальных последствий.

Согласно внутренней методике были определены риски только первого уровня. Следовательно, разработка и внедрение мероприятий по их устранению не требуется. Процесс оценки рисков повторно доказывает безопасность веб-приложения банка.

По окончании тестирования безопасности веб-приложения разрабатывается документ «Отчет о результатах тестирования безопасности веб-приложения», который содержит:

– общие сведения о проведенном анализе защищенности веб-приложения;

– результаты проведенных проверок;

– выводы (как развернутые технические, так и более краткие);

– оценку состояния защищенности веб-приложения;

– описание выявленных уязвимостей, ранжирование их по степени потенциальной опасности, вероятности их использования, описание последствий реализации выявленных уязвимостей;

– описание сценариев проведенных атак;

– рекомендации по устранению выявленных уязвимостей и повышению уровня защищенности веб-приложения.

Проведение тестирования безопасности проектов не является обязательным требованием для компаний. Однако при отказе от данного процесса велика вероятность атаки злоумышленника на информационные системы и сети организации, обнаружения и использования им найденных уязвимых мест, что приведет к нарушению информационной безопасности.

Следовательно, тестирование безопасности необходимо для защиты

информации, находящейся в автоматизированных системах финансовой организации, а также для своевременного выявления угроз и уязвимостей.

СПИСОК ЛИТЕРАТУРЫ

1. OSSTMM [Электронный ресурс]. – URL: https://www.isecom.org/OSSTMM.3.pdf (дата обращения 03.10.2022).
2. OWASP WSTG [Электронный ресурс]. – URL: https://owasp.org/www-project-web-security-testing-guide/stable.
3. NIST SP800-115 [Электронный ресурс]. – URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf.
4. PTES [Электронный ресурс]. – URL: http://www.pentest-standard.org/index.php/Main_Page.
5. ISSAF. – URL: https://untrustednetwork.net/files/issaf0.2.1.pdf (дата обращения 03.10.2022).
6. BSI SPTM [Электронный ресурс]. – URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.pdf?__blob=publicationFile&v=1.
7. Positive Technologies [Электронный ресурс]. – URL: https://www.ptsecurity.com/ru-ru/services/pentest.
8. Инструменты Kali Linux [Электронный ресурс]. – URL: https://www.kali.org/tools.
9. Acunetix WVS [Электронный ресурс]. – URL: https //www.acunetix.com.
10. Burp Suite Professional [Электронный ресурс]. – URL: - https://portswigger.net/burp.
11. Netsparker [Электронный ресурс]. – URL: - https://www.netsparker.com
12. OWASP ZAP [Электронный ресурс]. – URL: https://www.zaproxy.org.
13. Шукенбаева Н.Ш., Шукенбаев А.Б., Александрова С.И. Пример тестирования WEB- приложения // Сборник трудов 1-го международного форума «Корпорации – парадигма формирования национальной экономики». Москва. НОУ ВО МИГКУ, 2013, с.145-152

НАУЧНАЯ СЕКЦИЯ

«КИБЕРБЕЗОПАСНОСТЬ»

Руководитель: **Симонян Айрапет Генрикович**,
Московский технический университет связи и информатики,
доцент кафедры «Информационная безопасность»,
кандидат технических наук, доцент

Козьминых Сергей Игоревич
профессор департамента Информационной безопасности,Финансового университета при Правительстве Российской Федерации,доктор технических наук, доцент,
SIKozminykh@fa.ru

ПРОБЛЕМЫ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА

Введение.

С тех пор, как в нашей стране стала массово внедряться мобильной связь, появились телефонные мошенники. Сначала звонили «операторы связи» и грозили отключить телефон, если абонент не направит СМС-сообщение, которое прислал мошенник. При этом все деньги с телефона переводились на телефон мошенника. Но, как правило, на счете телефона не хранили большие суммы, поэтому мошенники стали придумывать новые схемы отъема денег. Профессор Департамента информационной безопасности Финансового университета при Правительстве Российской Федерации, доктор технических наук, доцент Сергей Козьминых рассматривает варианты телефонного мошенничества и способы защиты от него.

1. Тренды кибермошенничества и методы телефонного мошенничества.

Тренды кибермошенничества с каждым годом меняются. Ранее преобладало вирусное заражение через установку вирусного программного обеспечения и СМС-банкинг. Скимминг – мошенничество посредством банкоматов – ушел в историю. Фишинг остается рабочей схемой мошенников. Социальная инженерия сейчас является основной в кибермошенничестве, так как на человека воздействовать проще, чем

технически разрабатывать вирусы и приложения.

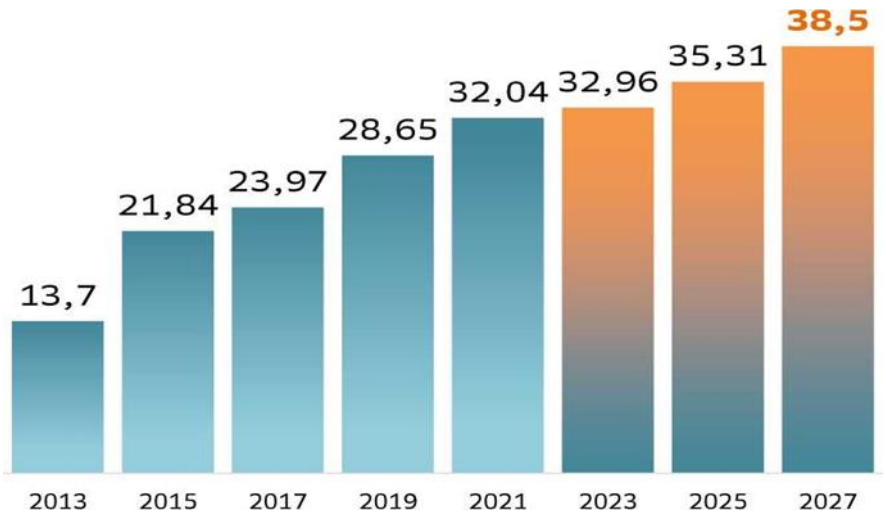


Рис. 1. Прогноз мировых потерь от кибермошенничества в млрд долларов

В контексте информационной безопасности социальная инженерия определена как психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации. Метод основан на использовании слабостей человеческого фактора и является очень эффективным.

Социальная инженерия – метод, который используют мошенники, чтобы заставить сообщить данные, необходимые для хищения. Для этого организованы специальные контактные центры и офисы с IP-телефонией. Как правило, звонят «сотрудник» службы безопасности банка, представитель государственных органов, предупреждают об оформлении кредита, изменении номера телефона, попытке кражи средств со счета, сообщают о расследовании дела в отношении клиентского менеджера банка. По данным СБЕРа социальная инженерия применяется в 94% случаев кибермошенничества. Ежемесячно в России совершается несколько сот тысяч мошеннических телефонных звонков.

Два основных результата действий мошенников при контакте с жертвой социальной инженерии:

- «самоперевод»: клиент самостоятельно переводит деньги под давлением мошенника;

- кража личности: мошенник получает необходимые данные для перевода на своем устройстве из аккаунта жертвы.

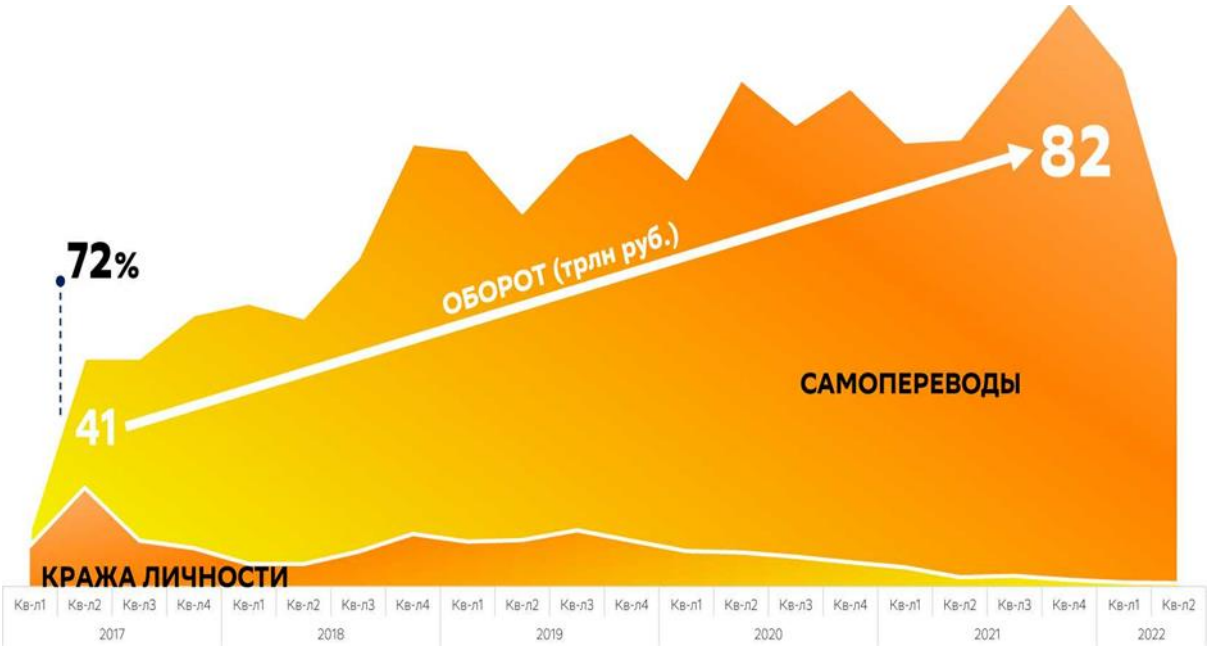


Рис. 2. Кража личности и само переводы за 2017-2022

В 99% случае происходит подмена номера телефона, с которого звонят мошенники и поэтому определить, откуда они звонят достаточно сложно. Подобные преступления раскрываются очень редко это стимулирует увеличение данного рода мошенничества.

Приведем несколько примеров телефонного мошенничества:

На телефон приходит фишинговая рассылка – письмо, в котором написано, что вам полагается приз, если вы правильно выберете коробочку на интерактивной картинке и вам дается три попытки. Первые две попытки как правило неудачные, а третья открывает приз со значительной суммой денег. Вы счастливы и уже думаете куда потратить деньги. Но для того, чтобы получить приз вы должны ввести номер вашей карты, на которую переведут деньги. Приз, конечно, не получите, а вот данные вашей карты

позволят мошеннику снять с нее деньги. Как говориться: «Бесплатный сыр бывает только в мышеловке». Надо всегда об этом помнить.

Звонит «оператор банка» или сотрудник службы безопасности. С вашего счета пытаются снять деньги, их надо срочно перевести на другой счет. Клиент начинает нервничать, на него давит мошенник и он переводит деньги на неизвестный ему счет и теряет их окончательно. Известен случай, когда мошенники таким путем завладели 300 млн рублей. Женщина целую неделю под руководством мошенника снимала деньги со счета и через платежный терминал переводила их на неизвестный ей счет, а муж помогал ей это делать. Мошенников так и не поймали.

Что делать? Надо знать, что из банка звонят клиентам только чтобы предложить новые услуги банка. Кстати, об услугах банка можно ознакомиться на его сайте. В остальных случаях никто звонить не будет. Если есть сомнения по поводу несанкционированного доступа к счету, надо срочно позвонить в банк и заблокировать карту или счет. Телефон на оборотной стороне карты. В целях защиты ваших денег можно скрыть данные вашей карты и счета. СБЕР предоставляет такую услугу и это можно сделать из вашего личного кабинета, тогда мошенники не смогут получить доступ к вашим деньгам.

Еще пример. Звонит «оператор банка» или сотрудник службы безопасности и сообщает, что на ваше имя пришел запрос на оформление кредита. В ходе выяснения ситуации мошенник умело выясняет ваши персональные данные, данные вашей карты, номер счета и потом использует эти данные для кражи денег. Конечно, ни один банк по телефону не решает вопросы выдачи кредитов, если вам звонят по этому вопросу, это мошенник.

Звонит «сотрудник» службы безопасности и просит вас помочь поймать нечестного сотрудника банка, и когда он позвонит сыграть с ним в игру «переведи деньги». Если вы пойдете навстречу этому сотруднику, то тоже попрощаетесь со своими деньгами. Иногда мошенники наглеют

настолько, что после того, как вы потеряли деньги, опять звонят вам от имени правоохранительных органов и предлагают еще перевести деньги на указанный счет, чтобы поймать преступников и вернуть вам все, что вы перевели. Результат уже понятен;

Раньше присылали СМС «мама положи деньги на этот телефон». Теперь вам звонит ваш сын, дочь, внук или близкий друг, говорит, что у него сел телефон, поэтому он звонит с чужого и просит срочно на этот телефон или по номеру телефона на счет перевести деньги, так как он якобы попал в какую-нибудь сложную ситуацию: попал в автоаварию, сбил человека, сломал ногу, кончился бензин или что-то подобное. Современные технологии позволяют подделать любой голос. Вспомните наших знаменитых пранкеров Лексуса и Вована. Эти технологии стали широко доступны, и жулики их уже используют их для отъема денег у населения. В этом случае не торопитесь переводить деньги. В ходе разговора задайте пару вопросов, ответы на которые знает только тот, от чего имени звонят. Кличку собаки, любимое место встреч, девичью фамилию матери или еще что-то личное. Попробуйте дозвониться, тому кто звонил. Главное не принимайте скоропалительных решений, и вы выведете жулика на чистую воду;

Еще один способ завладеть вашими деньгами. После того как мошенники получили доступ к вашим данным, они через знакомого оператора связи оформляют сим-карту на ваш номер телефона и таким образом получают доступ к вашему мобильному банку, дальше не требуется много времени, чтобы перевести деньги с вашего счета. Как только активируется другая сим-карта ваш телефон перестает работать, и вы не узнаете о том, что у вас крадут деньги. Как защититься в такой ситуации, прежде всего не разглашайте свои персональные данные, сразу как у вас отключился телефон, необходимо заблокировать карту, это можно сделать с любого телефона. Можно скрыть данные карты и счета. Можно ограничить переводы с вашей карты, посчитайте сколько вы тратите в день, обратитесь в

банк, и он ограничит сумму ежедневных переводов.

Можно было бы привести еще несколько примеров, но все они сводятся к одному – желанию мошенника залезть в ваш кошелек, получить доступ к карте или счету, заставить вас перевести ваши деньги на чужой счет. Ежемесячно в России совершается несколько сот тысяч мошеннических телефонных звонков.

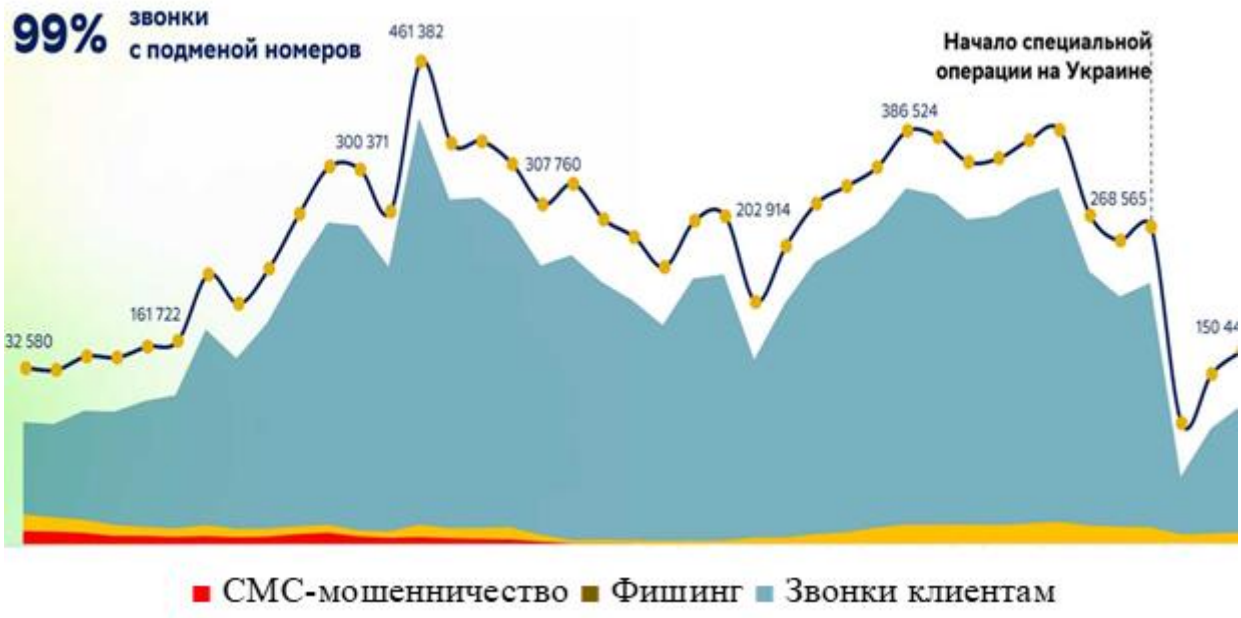


Рис.3. Телефонное мошенничество в РФ в период с 2019 по 2022 год

Если вас просят перевести деньги на незнакомый счет, представьте, что, вы вынули из кармана кошелек с деньгами и отдаете его незнакомцу. У людей часто деньги на карте не ассоциируются с «живыми» купюрами, они легче тратятся. Если хотите сэкономить, снимите деньги, положите в конверт и записывайте расходы. Тратить живые деньги жалко, а с карты не очень.

Не отвечайте на незнакомые звонки и СМС сообщения. У вас есть список ваших абонентов и если звонит кто-то незнакомый, то лучше всего с ним вообще не разговаривать. Установите на телефоне программу WhoCalls (кто звонит) ее бесплатно можно скачать на Google Play. Эта программа

подскажет вам что идет массовый обзвон или звонят из Свердловской области, где у вас нет знакомых. Назойливые звонки и СМС-сообщения заносите в черный список, обозначайте как спам, блокируйте на своем телефоне. Помните враг не дремлет и с ним надо уметь бороться!

Заключение

Чего ожидать в будущем? Дальше будет еще круче. Недавно по телевидению был показан ролик Мегафона с участием Азамата Мусагалиева и помолодевшего Брюса Уиллиса, вот только один из самых высокооплачиваемых актёров мира на съёмочную площадку так и не приехал - вместо этого разработчики проекта использовали его образ, который был «нарисован» нейросетями для наложения на кадр. Искусственный интеллект с использованием нейросетевых технологий уже используется для производства рекламы.

Мошенники уже освоили подмену телефонных номеров, осваивают подмену голоса и скоро освоят подмену изображения. И тогда вам с телефона вашего сына на смартфон поступает видеозвонок, мошенник с лицом сына и его голосом слезно просит срочно перевести деньги на его телефон, вряд ли вы откажите. Но деньги, которые вы пошлете сыну скорее всего попадут к мошеннику, подумайте, как этому можно будет помешать.

Литература:

1. OWASP, «OWASP Top 10 Application Security Risks – 2019», https://www.owasp.org/index.php/Top_10-2017_Top_10, 27 марта 2019 года.

2. Positive Research, «Статистика атак на веб-приложения: II квартал 2019 года», 14 сентября 2019 года.

3. Косинов А.А., учебный курс «Системы обнаружения атак», Москва, 2017;

4. Бил Джей, «Snort 2.1 обнаружение вторжений», 2018 г.

5. А.В. Лукацкий, «Система обнаружения атак», 2017 г.

6. Синица И.Н., «Вопросы безопасности и пути их решения в современных компьютерных сетях», 2021 г

7. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия. Интернет-университет информационных технологий − ИНТУИТ.ру, 2020.

8. Robert Auger, Ryan Barnett, Yuval Ben-Itzhak, Erik Caso и др. - Web Application Security Consortium (перевод: Классификация ВЕБ угроз). Издательство webappsec, США, 2020.

9. Корпорация МАЙКРОСОФТ – Fundamentals of Network Security (перевод: основы сетевой безопасности). Издательство МАЙКРОСОФТ, США, 2019.

10. Michael Sutton, Adam Greene, and Pedram Amini. Fuzzing : brute force vulnerabilty discovery. Upper Saddle River, NJ: Addison-Wesley, 2018.

11. Takanen, Ari, Jared D. Demott, and Charles Miller. Fuzzing for software security testing and quality assurance. Boston: Artech House, 2020.

12. Mark Dowd, John McDonald, and Justin Schuh. The art of software security assessment: identifying and preventing software vulnerabilities. Indianapolis, Ind: Addison-Wesley, 2019.

13. Зима В.М., Котухов М.М., Ломако А.Г., Марков А.С., Молдовян А. А. Учебное пособие. Разработка систем информационно-компьютерной безопасности. - СПб, 2017. - 304 с.

14. Мельников В.В. Безопасность информации в автоматизированных системах. - М.: 2018. - 367 с.

15. Доценко С.П. Подход к построению модели систем менеджмента информационной безопасности: Научный журнал КубГАУ, 2017, №53. - с. 1-4.

Гнидин Дмитрий Александрович
ЮРГПУ(НПИ)
mityagnidin8@gmail.com

РАЗРАБОТКА МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ПОПЫТОК КИБЕРАТАК НА СЕРВЕРЫ БАЗ ДАННЫХ

Аннотация: в статье рассмотрена разработка методов защиты информации от попыток кибератак на серверы баз данных

Ключевые слова: информация, базы данных, кибератака, защита.

Целью исследования является вопрос повышения уровня защиты баз данных.

Задачами исследования является: анализ существующих способов кибератак и защиту от них, методов защиты баз данных, анализ эффективности методов защиты баз данных.

Актуальность данной научной работы заключается в изучении и анализе кибератак, разработке методов защиты, повышение безопасности баз данных, защиты информации хранящейся в базах данных.

Выводы: в результате проделанной работы, были изучены кибератаки, как способ дестабилизации системы, способы защиты от них, а также некоторые рекомендации направленные о предупреждении кибератак.

Практическое значение: полученные в научной статье мысли и умозаключения, возможно использовать при проведении дальнейших испытаний по обозначенной теме. Все полученные знания являются практически полезными, что позволяет использовать их в ходе предупреждения кибератак на базы данных, а также для уменьшения их вредоносного воздействия.

Оригинальность: данная работа будет полезна как простым рабочим в компаниях, таким как сотрудникам отдела по предотвращению

киберпреступлений, так и простым пользователям обычной компьютерной техникой.

Что же такое кибератаки и как с ними бороться?

Кибератака в узком смысле-это нападение на информационную систему, с целью ее захвата. В широком же смысле, кибератака это поиск методов и средств для полного захвата информационной системы, для получения полного контроля над ней, с целью выведения из строя. Специалисты выделяют 12 основных видов кибератак: утечка данных, фишинг, мошенничество от лица CEO, мошенничество через отдел кадров, сексуальное вымогательство, атаки на корпоративную сеть, программа-вымогатель, мошенничество через техническую поддержку, электронные письма с вредоносным ПО, DoS-атаки, атаки рекламным ПО, мошенничество через поставщика.

Что такое базы данных и почему их следует защищать?

База данных (БД) – совокупность организованной информации, относящейся к определённой предметной области, предназначенная для длительного хранения и использования в электронном виде из компьютерной системы.

Простыми словами, база данных-это такая система, в которой содержится вся информация об организации, от сотрудников до клиентов. Все что хранится в базе данных доступно для изменения и извлечения при необходимости.

Именно поэтому базы данных становятся желанной добычей для хакеров, следовательно нашу систему нужно как следует защитить.

Так, например, в 2020 году, были атакованы спецслужбы США, хакеры через базы данных получили доступ к 270 Гб секретных данных правоохранительных органов в виде более 1 млн файлов. Такая утечка была названа BlueLeaks.

Стабильное состояние и функционирование баз данных обусловлено ее возможностью противостоять кибератакам любого характера. Кибератаки, как и любая другая сфера, постоянно развиваются и улучшаются, как

повышением сложности, так и ростом масштабов. Что требует постоянного улучшения баз данных, для их корректной работоспособности.

Ущерб от компьютерных атак за последние несколько лет составил от 350 млрд до 1.5 трлн долларов. На Россию пришлось 10% всех мировых атак за 2019 год

Компьютерная атака, в отличие от обычного вируса, носит целенаправленный характер и ее цель- конкретная информационная система (в нашем случае базы данных), в которых содержатся как данные и пароли работников, так и информация о компании в целом, поэтому защититься от нее достаточно сложно.

Если как следует не защитить базу данных, то это будет легкой добычей для хакеров, которым атаковать базу данных предприятия не составит никакого труда. Ущерб может быть разным: от контролирования хакерами системы, до полного уничтожения всех данных, без возможности восстановления. От всех видов кибератак, требуется разный уровень защищенности и разный уровень нанесенного ущерба. Однако от всех таких компьютерных преступлений защита имеет несколько основных правил, соблюдение которых минимизирует риск проникновения в базу данных.

Но даже если нам как-то удастся защитить наши базы данных от хакеров, то вероятность проникновения в систему не исключена полностью, так как есть пользователи компьютерных систем, ведь многие инциденты происходят по их вине. Поэтому для того чтобы свести к минимуму риск кибератаки, пользователям системы стоит соблюдать несколько правил, которые направлены на защиту не только их самих, но и на защиту базы данных.

Если база данных была атакована, не стоит спешить перечислять денежные средства хакерам, так как нет гарантии того, что вредоносное программное обеспечение будет удалено и у вас будет восстановлен полный доступ к компьютеру, а также не скрывать произошедший инцидент компьютерной безопасности, как от руководства, так и от правоохранительных органов, не

пытаться самостоятельно переустановить систему. Необходимо незамедлительно сообщить в правоохранительные органы и принять все меры к сохранению и фиксации следов осуществленной кибератаки. Соблюдение всех рекомендаций и правил защитит базу данных от кибератаки, а также поможет в фиксации киберпреступлений и их дальнейшее расследование.

СПИСОК ЛИТЕРАТУРЫ

1. Кибератака - URL: http://www.securitylab.ru/news/tags/%EA%E8%E1%E5%F0%E0%F2%E0%EA%E0/ (Дата обращения 5 мая 2017 г.).

2. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента РФ от 5 дек. 2016 г. №646. - Доступ из справ. правовой системы «Консультант Плюс».

3. ФСБ оценила ущерб от кибератак в мире... - URL: http://www.rbc.ru/technology_and_media/02/02/2017/5892f53b9a7947133199f41 (Дата обращения 1 июня 2017 г).

4. Россия заняла второе место по количеству кибератак. - URL: http://www.itsec.ru/newstext.php?news_id=117006

5. Ли Ирина. Кого бьют хакеры // РБК. - №100 (2597). – 13 июня 2017 г. – URL: http://www.rbc.ru/newspaper/2017/06/13/593a9a749a794766d6b11c54.

6. Вирус атаковал компьютерные сети по всему миру. - URL: https://www.1tv.ru/news/2017/0513/325215virus_atakoval_kompyuternye_seti_po_vsemu_miru (Дата обращения 3 июня 2017 г.).

7. Дремлюга Р.И. Интернет-преступность: моногр. - Владивосток: Изд-во Дальневост. ун-та, 2008. – 240 с.

8. Введенская О.Ю. Проведение предварительной проверки сообщений об интернет-преступлениях и организация первоначального этапа расследования. - Краснодар: КрУ МВД России, 2016. – 51 с.

9. Указ Президента РФ от 15 января 2015 года № 31с «О создании

государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» - Доступ из справ. правовой системы «Консультант Плюс».
10. Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (Концепция утверждена Президентом Российской Федерации 12 декабря 2014 г. № К 1274) // официальный сайт Совета Безопасности Российской Федерации. – URL: http://www.scrf.gov.ru/documents/6/131.html.
11. Бехметьев А.Е. Кибератаки //Административное право. - №1. - 2017. - С.

Красов А.В.
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, заведующий кафедрой ЗСС
кандидат технических наук, доцент,
krasov@inbox.ru
Паскидов Н.В.
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, студент,
paskidov.nv@spbgut.ru
Салита А.С.
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, студент,
salita@internet.ru

ИСПОЛЬЗОВАНИЕ СЕТЕВОЙ СТЕГАНОГРАФИИ В СЕТЯХ NGN

С развитием информационных технологий возрастает потребность в новых услугах связи и улучшении качества существующих сервисов, в связи с чем требуется развитие и модернизация транспортной системы. Одна из ветвей такого развития – сети NGN. Данные сети позволяют объединить существующие сети старого поколения с сетями, построенными на базе стека протоколов TCP/IP. Однако как и все существующие технологии в сетях NGN остро стоит вопрос безопасности.

Мультисервисные сети связи или Next Generation Networks – концепция построения сетевой инфраструктуры, в которой качество предоставления услуг не зависит от используемых технологий. В общем случае сети NGN предлагают конвергенцию существующих телефонных сетей общего пользования и сетей, построенных на базе стека TCP/IP [1]. В

настоящее время данная концепция активно используется в крупном корпоративном сегменте и в государственном секторе, соответственно сети, построенные в рамках данной концепции должны иметь высокий уровень информационной безопасности. Общая структура сети представлена на рисунке 1.

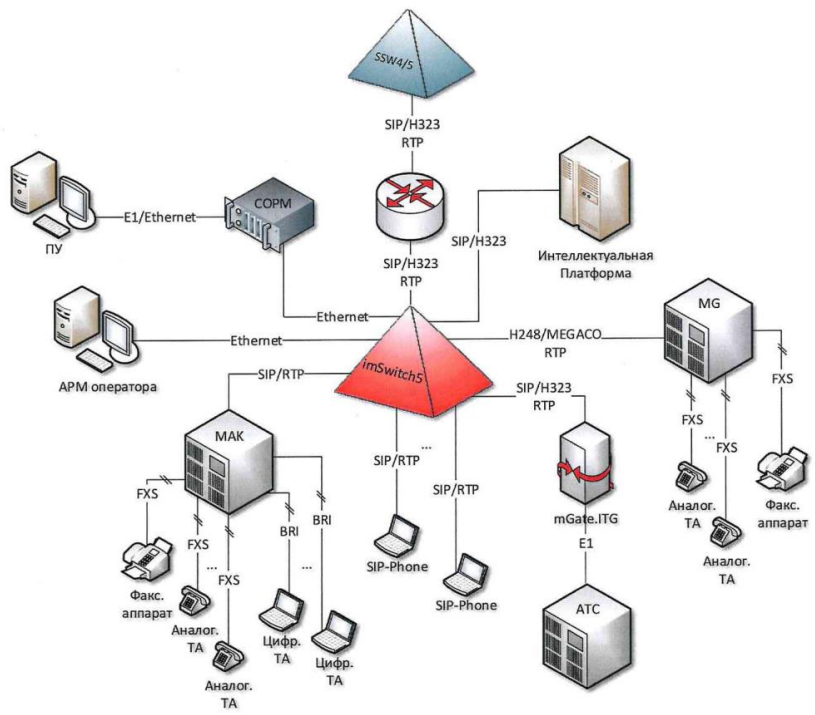


Рисунок 1 – Схема типовой сети NGN

Затрагивая вопрос информационной безопасности типовой сети, стоит понимать неизбежность его разделения на IP составляющую и ТФоП. Телефонные сети в данном контексте можно считать более защищёнными, поскольку сами по себе данные сети являются изолированными и закрытыми структурами, однако с другой стороны стыка чаще всего обычная сеть “Интернет”, имеющая все присущие ей проблемы. Несмотря на это чаще всего такие сети, разворачиваемые в крупных компаниях или сети в рамках операторов связи чаще всего достаточно хорошо защищены от несанкционированных вторжений. В данной ситуации особенно интересно рассмотреть вопрос существования стегоинсайдеров и вопрос возможности использования стеганографических методов в целом.

Согласно списку угроз ФСТЭК, сетевая стеганография обозначена под кодом УБИ.111: Угроза передачи данных по скрытым каналам. Данная угроза заключается в существовании возможности вывода защищаемой информации из системы и передаче управляющих команд методом их нестандартного размещения в передаваемых по сети данных с помощью маскирования под служебные данные каналов связи.

Сетевая стеганография — технология позволяющая скрытно осуществлять передачу информации по общедоступным каналам связи, причём данные скрыты не только от человека, но и от промежуточных устройств.

Как было сказано ранее, сети NGN, используемые в крупных организациях и у операторов связи достаточно хорошо защищены. Обычно на стыках таких сетей установлены аппаратные межсетевые экраны, а также используется технология фильтрации DPI. Однако как показали опыты [2,3], данные установки в большинстве случаев пропускают пакеты, являющиеся стегоконтейнерами. Кажется, что в таком случае бессмысленно рассматривать вопрос использования сетевой стеганографии, поскольку сети NGN не являются частным случаем, однако это не так. Изучая структуру типовой сети можно заметить такую её составляющую как SBC. Session border controller или Пограничный контроллер сессий – составная часть сети NGN, выполняющая ряд функций необходимых для безопасного функционирования всей сети. Несмотря на название и предназначение, данный элемент не является заменой обычному межсетевому экрану, а скорее дополнением к нему. Основная роль SBC – защита сети IP – телефонии и серверов обработки медиапотоков. На базе собственных ресурсов SBC организовывает списки контроля доступа, защиту от DDOS атак и проводит анализ пакетов на предмет нарушений.

В работах [4,5] были рассмотрены методы вложений в VoIP потоки, а также вложения в протокол SIP, однако в схемах, подобных представленной выше данные методы не были протестированы.

С теоретической точки зрения, при правильном выборе полей SBC должен пропустить трафик с вложениями в сигнальный протокол, поскольку если информация об установке вызова не искажена, то вопросов к пакетам не должно возникнуть. С медиапотоками RTP и RTSP ситуация сложнее. SBC обеспечивает шифрование потоков, а также выполняет функции транскодирования в случаях если стороны не могут договориться о параметрах передачи в сообщениях SDP. В данном случае метод TranSteg невозможен в реализации. Метод LACK также невозможно применить, поскольку при попытке реализации пакеты будут отбрасываться на контроллере сессий и работу с вложениями возможно произвести только в случае доступа злоумышленника непосредственно к контроллеру.

Для подтверждения данных утверждения был проведён небольшой эксперимент. На сети одной из компаний, пожелавшей остаться неизвестной была развёрнута сеть, состоящая из пограничного контроллера сессий, мультисервисного коммутатора доступа (АТС) и сопутствующей инфраструктуры (Рис. 2). В ходе эксперимента было принято решение переслать пакеты с вложениями в поле “User-Agent” протокола SIP, а также в поля “Length” и “Packet id” пакетов протокола RTP сначала изнутри сети, а затем извне.

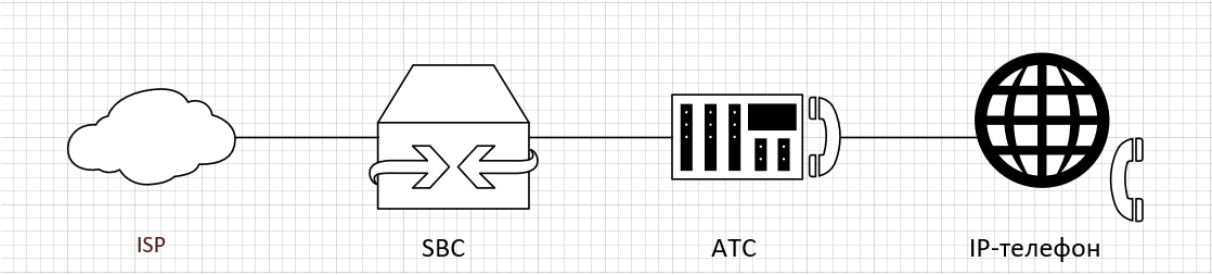


Рисунок 2 – Схема сети

Было выявлено, что при вложении в RTP после сразу после установления вызова SBC разрушал вызов из-за ошибок при передаче медиапотока (Рис. 3).

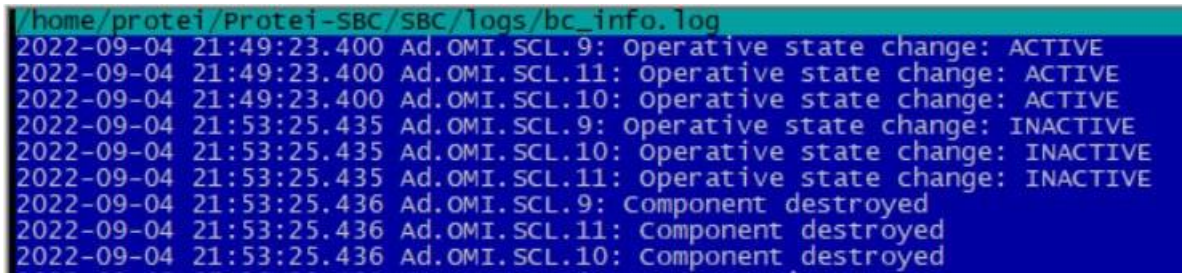


Рисунок 3 – Разрушение вызова

Однако при вложении в протокол SIP сессия вызова устанавливалась корректно, хотя контроллер выдавал предупреждение о некорректном формате протокола сигнализации (Рис. 4).

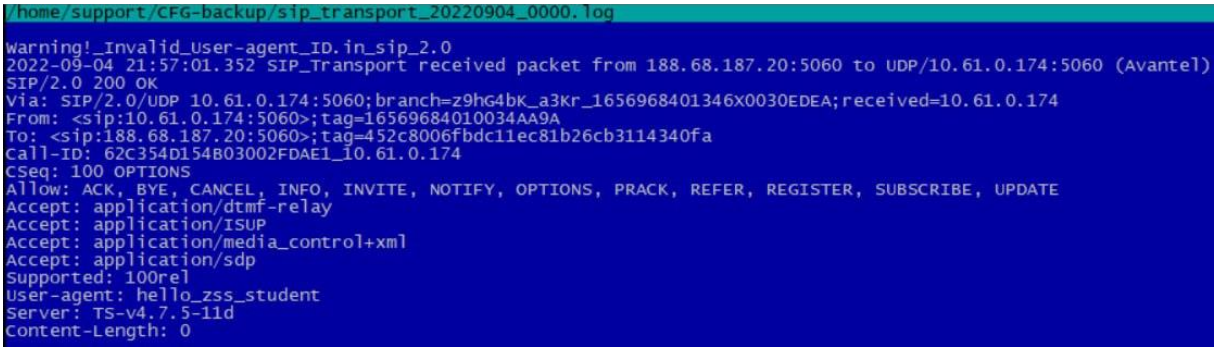


Рисунок 4 – предупреждение о некорректном поле user-agent

На основании полученных результатов можно сделать вывод о том, что стеганографические каналы имеют потенциал в использовании в сетях NGN, однако имеют ньюансы при выборе стегоконтейнера, а также достаточно низкую пропускную способность.

СПИСОК ЛИТЕРАТУРЫ

1. Гольдштейн, А.Б. SOFTSWITCH / А.Б. Гольдштейн, Б.С. Гольдштейн // СПб.: БХВ Санкт-Петербург — 2006 — С. 13-15, 41-50.

2. Салита, А.С. Практическое применение сетевой стеганографии на примере протокола IPV4 / А. С. Салита, А. В. Красов // Региональная

информатика и информационная безопасность : Сборник трудов конференций: Санкт-Петербургской международной конференции и Санкт-Петербургской межрегиональной конференции, Санкт-Петербург, 28–30 ноября 2020 года. – Санкт-Петербург: Региональная общественная организация "Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления", 2020. – С. 288-291. – EDN ZHRXSP.

3. Салита, А. С. Создание стеганографического канала при помощи полей / А. С. Салита, А. В. Красов // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2021. – № 2. – С. 36-40. – DOI 10.46418/2079-8199_2021_2_6. – EDN TLRNVO.

4. Волкогонов, В.Н. Методы и способы создания стеганографических вложений в сетевых пакетах / В.Н. Волкогонов, Е.М. Гетьман, А.С. Салита // Актуальные проблемы инфотелекоммуникаций в науке и образовании. — 2021. — С. 178 – 183.

5. Mazurczyk, W. Steganography of VoIP streams / W. Mazurczyk, K. Szczypiorski // Proceedings of the OTM 2008 Confederated International Conferences, CoopIS, DOA, GADA, IS, and ODBASE 2008. Part II on On the Move to Meaningful Internet Systems — 2008 — С. 1001–1018

6. Алейников, А.А. Контроль, измерение и интеллектуальное управление трафиком : монография / А.А. Алейников, К.З. Билятдинов, А.В. Красов, М.В. Левин // Санкт-Петербург : Центр научно-информационных технологий "Астерион", 2016. – 92 с. – ISBN 978-5-00045-385-8. – EDN WLROTL.

7. Ушаков, И.А. Организация, принципы построения и функционирования компьютерных сетей / И.А. Ушаков, А.В. Красов, Н.В. Савинов // Academia — 2019. — С. 240

8. Mazurczyk, W. Retransmission steganography and its detection / W. Mazurczyk, M. Smolarczyk, K. Szczypiorski // Soft Computing — 2009 — 15(3) — С. 505–515.

9. Коржик, В.И. Цифровая стеганография и цифровые водяные знаки. / В.И. Коржик, К.А. Небаева, Е.Ю. Герлинг, П.С. Догиль, Федянин И.А // под общей ред. проф. В.И. Коржика. Санкт-Петербург, 2016. Том Часть 1 Цифровая стеганография.
10. Диордица, В. Н. Исследование современных методов сетевой стеганографии / В. Н. Диордица, А. В. Красов, А. И. Таргонская // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020) : IX Международная научно-техническая и научно-методическая конференция : сборник научных статей, Санкт-Петербург, 26–27 февраля 2020 года. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2020. – С. 404-409.

Лошкарев Алексей Валерьевич,
Аспират**,** Морской государственный университет им. адм. Г.И. Невельского, г.Владивосток, Россия;
e-mail: kroslesha12@mail.ru
Балацкий И. А.,
Школьник, МОБУ СОШ №3, г.Арсеньев, Россия

ВИДЫ КИБЕРУГРОЗ В СУДОВОЖДЕНИИ

Аннотация: В настоящий момент пользование электронных систем набирает все больше популярности во всех сферах жизни человека. Каждая электронная система может быть подвержена угрозе взлома с помощью внедрения различных вирусов и вредоносных программ. Знание всех видов информационного вмешательства ведет к предотвращению взломов систем или скорейшему восстановлению элетронно-информационных баз.

Наряду с прогрессом электронных систем каждая судоходная компания должна разработать план по кибербезопасности и меры по предотвращению кибервзломов и проводить с членами экипажа всех судов ежеконтрактный или полугодовой тренинг согласна разработанному плану и методам по киберзащите всех информационных баз данных.

В связи с вышеизложенным, в статье приведены виды киберугроз в сфере кибербезопасности и меры по предотвращению их действия и распространения в судовождении.

Ключевые слова: кибербезопасность, вредоносное программное обеспечение, вирус, меры по кибербезопасности

Вредоносное программное обеспечение и его виды, используемые в судовождении

Вредоносное программное обеспечение (ПО) - это любое программное обеспечение, которое было написано с целью повредить устройство, украсть данные и, как правило, вызвать беспорядок.

Вредоносное ПО является сложной технологической системой, вследствие чего, зачастую создается командой хакеров. Киберпиратство осуществляется по ряду причин, самая часто применимая – получение денежных средств. В основном распространение вредоносного ПО осуществляется самими разработчиками, но также может быть продана тому, кто предложит самую высокую цену на платформе Dark Web в интернете.

Однако могут быть и другие причины для создания вредоносного ПО - его можно использовать как инструмент протеста, способ проверки безопасности или даже как оружие войны между правительствами.

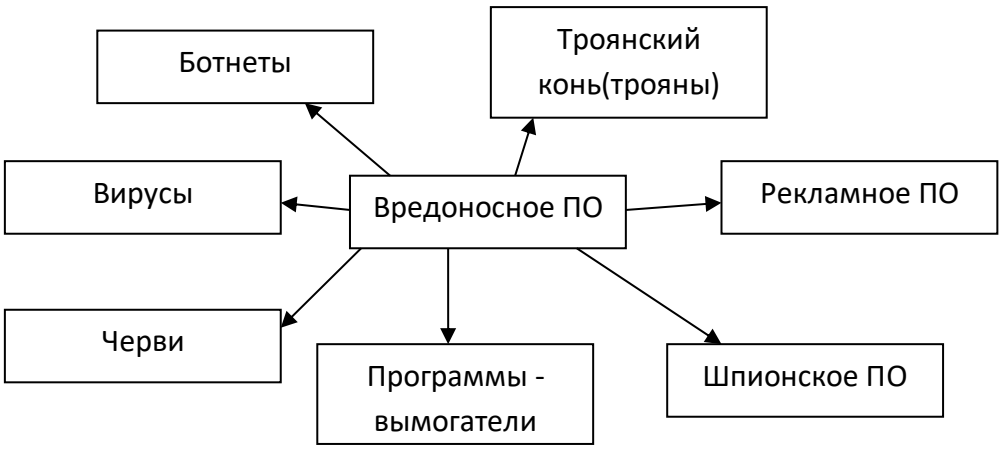


Рис. 1 Вид вредоносного программного обеспечения

Вирусы. Как и их биологические тезки, вирусы прикрепляются к чистым файлам и заражают их. Они могут бесконтрольно распространяться, нарушая основные функции системы, удалять или повреждать файлы. Обычно они отображаются в виде исполняемого файла (.exe).

Трояны. Такое вредоносное ПО маскируется под законным программным обеспечением или скрывается в легитимном программном обеспечении, в которое были внесены изменения. Он имеет тенденцию действовать незаметно и создавать бэкдоры (бэкдор – это дефект алгоритма

системы, который позволяет получить несанкционированный доступ к сети, системам, файлом) в вашей безопасности, чтобы проникнуть внутрь других вредоносных программ.

Шпионское ПО - вредоносное ПО, предназначенное для слежки. Он скрывается в фоновом режиме и записывает, действия, производимые в Интернете, включая запись ввода паролей, номеров кредитных карт, основных просматриваемых сайтов, файлов и многое другое.

Черви заражают целые сети устройств, как локально, так и через Интернет, используя сетевые интерфейсы. Он использует каждую последовательно зараженную сеть для заражения всей системы.

Программы-вымогатели. Этот вид вредоносного ПО, который обычно блокирует ваш компьютер и ваши файлы, благодаря чему существует вероятность потери всей системы и всех данных, если не будет получен выкуп киберпреступниками.

Рекламное ПО. Агрессивное рекламное программное обеспечение, которое подрывает IT-безопасность только при показе рекламы.

Ботнеты - это сети зараженных компьютеров, которые работают под контролем злоумышленника.

Рассмотрев каждый вид вредоносного программного обеспечения кратко, можно сделать вывод: зная все виды вредоносного программного обеспечения, возрастает вероятность вовремя обнаружить кибератаку, что способствует своевременному применению всех мер по предотвращению кибервзлома.

Социальная инженерия

Социальная инженерия - это психологическое манипулирование людьми с целью выполнения действий или раскрытия конфиденциальной информации.

• Злоумышленники могут обманом заставить вас предоставить конфиденциальную информацию, доступ к системам, перевод денег и многое другое.

• Злоумышленники исследуют факты о членах экипажа, судне или компании с помощью интернета или социальных сетях. Затем они используют эти знания, чтобы завоевать доверие.

• Тот, кто уже так много знает, может легко притвориться коллегой или другом друга.

К социальной инженерии можно отнести подозрительные телефонные звонки.

Телефонные звонки могут быть от мошенника, утверждающего, что он из службы поддержки IT, информируя вас, что:

• вам необходимо установить обновление или

• вы должны щелкнуть ссылку на веб-странице / электронном письме и

• ввести свои учетные данные или

• с просьбой разрешить им удаленно управлять вашим компьютером

Такие телефонные звонки относятся к кибератаке. В таких случаях рекомендуется:

• Получить контакты IT-поддержки из проверенного источника, а не от подозрительных лиц, страниц, систем

• Обратиться за советом в свою настоящую IT-службу поддержки по официально одобренным контактным данным.

К социальной инженерии также относится фишинг, взлом электронной почты.

Фишинг - попытка мошенников получить конфиденциальную информацию, такую как логин, пароль и данные кредитной карты, замаскировавшись под надежную организацию в электронном сообщении. Фишинг может иметь вид ссылки, вложения, фальшивые логины, подозрительные письма, подозрительные сайты.

Безопасность электронной почты

Зачастую кибермошенники используют электронную почту для собственных незаконных действий. В этом случае:

• Если вы подозреваете, что сообщение не является подлинным, обратитесь к отправителю для проверки, желательно по телефону или электронной почте (но необходимо повторно вводить адрес электронной почты отправителя).

В случае нажатии на кнопку «ответ», в большинстве случаев, ваше сообщение будет отправлено обратно фальсификатору.

• Необходимо помнить, что при получении электронной почты нельзя доверять имени и адресу отправителя. Подделать личность в Интернете очень легко.

• Важную для судоходства информацию никогда не следует отправлять по электронной почте. Любые важные данные можно передать через агента. Если все же используется электронная почта, то следует удостоверится в подлинности адреса получателя. Также необходимо убедиться, что сообщение было получено, особенно если время имеет важное значение.

• Также если необходимо отправить конфиденциальную информацию, ее можно включить в файл с защищенным паролем, и отправить в виде вложения вместо обычного текста в электронном письме. Пароль может быть отправлен в виде SMS-сообщения на мобильный телефон получателя.

Используя все факты о социальной инженерии, можно предотвратить кибервзломы и усилить кибербезопасность всей системы судна, компании.

Меры по кибербезопасности со стороны работников судоходных компаний.

Следующая политика должна применяться в судоходных компаний работниками:

1. Приобретение знаний

Каждая судоходная компания должна проводить инструктаж по кибербезопасности перед каждым рейсом и в течении рейса, если его продолжительность более 6 месяцев.

2. Личная осведомленность

Каждый моряк, работая в море, должен самостоятельно интересоваться кибербезопасностью для защиты собственных и судоходных баз информации.

3. Защита устройств от посторонних лиц.

Компания должна на каждую электронную технику ставить защитные программ, пароли и многое другое для защиты всей информации судна и судоходства.

4. Соблюдение всех правил и рекомендаций.

5. Сообщение о подозрительном поведении.

6. Обеспечение безопасности электронной почты и других способов связи.

7. Сохранение конфиденциальности всей информации компании - судна.

8. Избегайте высказываний в социальных сетях.

9. Сообщение о подозрительных запросах от внешних лиц.

Соблюдая все эти пункты, риск поражения систем и кражи информации злоумышленниками уменьшается в несколько раз.

Итак, не зная видов киберугроз в судовождении, не возможно понять, как бороться с киберпреступлениями и предотвращать их. Соблюдая все правила безопасности, возникновение кибервзлома сводиться к незначительному проценту, а значит, информационным базам и их системам ничего не угрожает.

СПИСОК ЛИТЕРАТУРЫ

1. Вагущенко Л.Л. Интегрированные системы ходового мостика. – Одесса: «Латстар», 2003.-170с.

2. Семененко, В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. — М.: МГИУ, 2017. — 277 с.

3. Мещеряков Р.В., ШелупановА.А., Белов Е.Б., Лось В.П. Основы информационной безопасности.- М.: Горячая линия-Телеком, 2006. - 350 с.

4. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; Под ред. акад. Б.П. Смагоринского. - М.: Право и закон, 2014.- 182 с.

5. Авчаров И.В. Борьба с киберпреступностью / И.В. Авчаров. // Информатизация и информационная безопасность правоохранительных органов. XI межд. конф. - М., 2012. - С. 191-194.

6. Raunek Kantharia. A Pocket Guide to Cybersecurity for Seafarers / Raunek Kantharia // Marine Insight, 2018. – 38 с.

7. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2018. - 400 с.

8. Малюк, А.А. Защита информации в информационном обществе: Учебное пособие для вузов / А.А. Малюк. - М.: ГЛТ, 2015. - 230 с.

9. Мельников, В.П. Информационная безопасность и защита информации / В.П. Мельников. - М.: Академия (Academia), 2012. - 276 с.

10. Старовойтов А.В. Кибербезопасность как актуальная проблема современности // Информатизация и связь. 2011. № 6. С. 4-7.

11. Марков А.С., Цирлов В.Л. Управление рисками - нормативный вакуум информационной безопасности // Открытые системы. СУБД. 2007. № 8. С. 63-67

Красов А.В.
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, заведующий кафедрой ЗСС, кандидат технических наук, доцент,
krasov@inbox.ru

СРАВНЕНИЕ ВОЗМОЖНОСТЕЙ НЕЙРОННОЙ СЕТИ И СИСТЕМЫ ПРЕДТВРАЩЕНИЯ ВТОРЖЕНИЙ ПРИ ОБНАРУЖЕНИИ СЕТЕВОЙ СТЕГАНОГРАФИИ В ПРОТОКОЛЕ TCP

На сегодняшний день набирают популярность технологии обеспечения конфиденциальности при использовании сети «Интернет». Наиболее популярный способ обеспечения конфиденциальности – криптография. Данная технология позволяет ограничить доступ к информации сторонними лицами путём шифрования данных. Криптографические протоколы надёжно защищают конфиденциальные данные, однако использование методов шифрования сопряжено с некоторыми недостатками. Основные минусы при использовании криптографии – необходимость соблюдения законодательства в сфере информационной безопасности, в частности подзаконных актов, регламентирующих использование криптографии. Второй недостаток заключается в том, что при передаче зашифрованной информации посторонние лица не смогут получить доступ, однако смогут увидеть факт самой передачи информации, что не всегда приемлемо. Ввиду существованию данных изъянов набирают популярность методы стеганографии. Стеганография – набор методов и технологий, позволяющий решить определенный набор задач по защите информации. Помимо сокрытия фактов передачи информации стеганография обеспечивает помехоустойчивую аутентификацию, защиту от цифрового пиратства, трассировку передаваемой по каналам связи информации и другие

возможности [1]. Стеганография разделяется на две подкатегории: собственно сама стеганография и цифровые водяные знаки. Цифровые водяные знаки позволяют защитить авторские права правообладателей на цифровой контент. Стеганография же в узком смысле — это семейство методов, которые позволяют при сохранении высокого качества контейнера обеспечить невозможность обнаружения вложения нелегитимными пользователями.

Существует большое количество стеганографических методов, однако в данной работе будет рассмотрен лишь один из них, как наиболее новый и наименее исследованный.

Данный метод есть использование сетевой инфраструктуры для организации скрытых каналов связи или сетевая стеганография.

Применение данного метода привлекает не только законопослушных граждан, желающих добиться конфиденциальности в интернете, но также злоумышленников, пытающихся скрыть свои намерения от правоохранительных органов, в связи с чем растёт потребность в обнаружении фактов использования сетевой стеганографии.

Сокрытие информации может достигаться за счёт инъекции полезной нагрузки в поля заголовков пакетов, модификации основных данных, передающихся по каналу связи или изменения структуры очерёдности пересылки пакетов. Также могут использоваться различные комбинации данных методов, например намеренная потеря аудио пакетов с целью последующего изменения и ретрансляции.

В данной работе будут рассмотрены возможности системы предотвращения вторжений IPS и метода, использующего нейронные сети в обнаружении сетевой стеганографии.

Intrusion Prevention System или система предотвращения вторжений — программное обеспечение или программно-аппаратный комплекс сетевой безопасности, предназначенная для обнаружения несанкционированных атак

и вторжений, а также автоматизированного противодействия им. Фактически IPS выступает второй линией защиты, располагающейся за межсетевым экраном или входящим в его состав. Для обнаружения угроз IPS анализирует сигнатуры, аномалии сетевого трафика и политики безопасности. При обнаружении подозрительного трафика система блокирует пакеты, сбрасывает сетевое соединение и оповещает администраторов.

Нейронная сеть — математическая модель, описывающая структуру организации нервных клеток живых организмов. Данная модель появилась вследствие изучения процессов и активностей, протекающих в мозге. Концепция нейронных сетей позволяет использовать их практически в любой области, в том числе и в обеспечении информационной безопасности. В данном контексте выявление фактов сокрытия данных с применением нейронных сетей — это использование существующих метрик и данных совокупно с алгоритмами классификации.

Для оценки возможностей обнаружения вложений были произведены вложения в заголовки пакетов протокола транспортного уровня TCP с помощью программной библиотеки Scapy версии 2.4.5. Данная интерактивная оболочка и программная библиотека, предназначенная для манипулирования сетевыми пакетами на языке программирования Python, позволяет генерировать большинство известных кадров, пакетов и блоков данных.

Заголовок протокола TCP содержит 11 полей, однако не все из них пригодны для вложений. Рассмотрим поля подробнее.

Source Port содержится в обоих протоколах и определяет порт отправителя. При изменении данного поля ответ не будет доставлен нужному приложению и как следствие будет утеряно. Но если при организации скрытого канала не требуется подтверждать доставку пакета или порт источника будет изменяться при помощи вмешательства после прочтения вложения, то поле пригодно для вложения в него сокрытых данных.

Destination Port – обязательное поле двух протоколов, содержащее порт получателя. Может также использоваться для передачи сокрытых данных, если будет считано получателем перед обработкой пакета. Его использование в качестве стегоконтейнера крайне затруднительно без потери приходящих данных, но возможно.

Sequence Number — поле, содержащееся в протоколе TCP и указывающее номер последовательности. Значение данного поля генерируется случайно и увеличивается на единицу при передаче байта полезной нагрузки. Не представляется возможным для вложения данных.

Acknowledgment Number есть только в протоколе TCP и необходимо для определения порядкового номера октета получение которого ожидает принимающая сторона. Использование данного поля зависит от того установлен ли флаг ACK. Если флаг не установлен, то поле возможно использовать в качестве стегоконтейнера.

Data offset в протоколе TCP необходимо для определения длины заголовка пакета и определения начала данных. Здесь содержится длина заголовка в тридцатидвух-битовых словах, из-за чего не пригодно для использования.

Поле Reserved зарезервировано и заполнено нулями. Может использоваться для передачи информации, однако легко может быть выявлено.

Flags — используется в протоколе TCP и не подходит для вложений, так как в данном поле устанавливаются флаги фрагментации и их изменение может повлечь за собой ошибку передачи данных, а также разрыв сессии.

Window Size — поле содержащееся в протоколе TCP, содержащее в себе количество октетов, которое принимающая сторона готова принять в настоящий момент без подтверждения. Данное поле пригодно для построения стеганографического канала.

Checksum – поле, в котором содержится контрольная сумма, подсчитанная для заголовка и данных пакета. Это поле не пригодно для вложения данных, так как его модификация ведет к потере данных.

Options — поле протокола TCP содержащее произвольную последовательность полей, описывающую необязательные данные заголовка и влияющую на принятие пакета противоположной стороной. Не пригодно для организации стеганографического канала.

Поле Length есть только в протоколе UDP и содержит значение длины всей датаграммы. Несовпадение значения данного поля с реальной длиной вызывает ошибку, следовательно поле не пригодно для вложений.

Поле Urgent pointer содержит значение счетчика пакетов, начиная с которого следуют пакеты повышенной срочности. Пригодно, если не стоит флаг URG, в другом случае влияет на передачу данных.

Исходя из анализа полей заголовка, к вложению пригодны следующие поля: source port, destination port, acknowledgement number, window size, urgent pointer.

В качестве системы предотвращения вторжений была выбрана IPS-система Snort со стандартными правилами (Рис. 1).

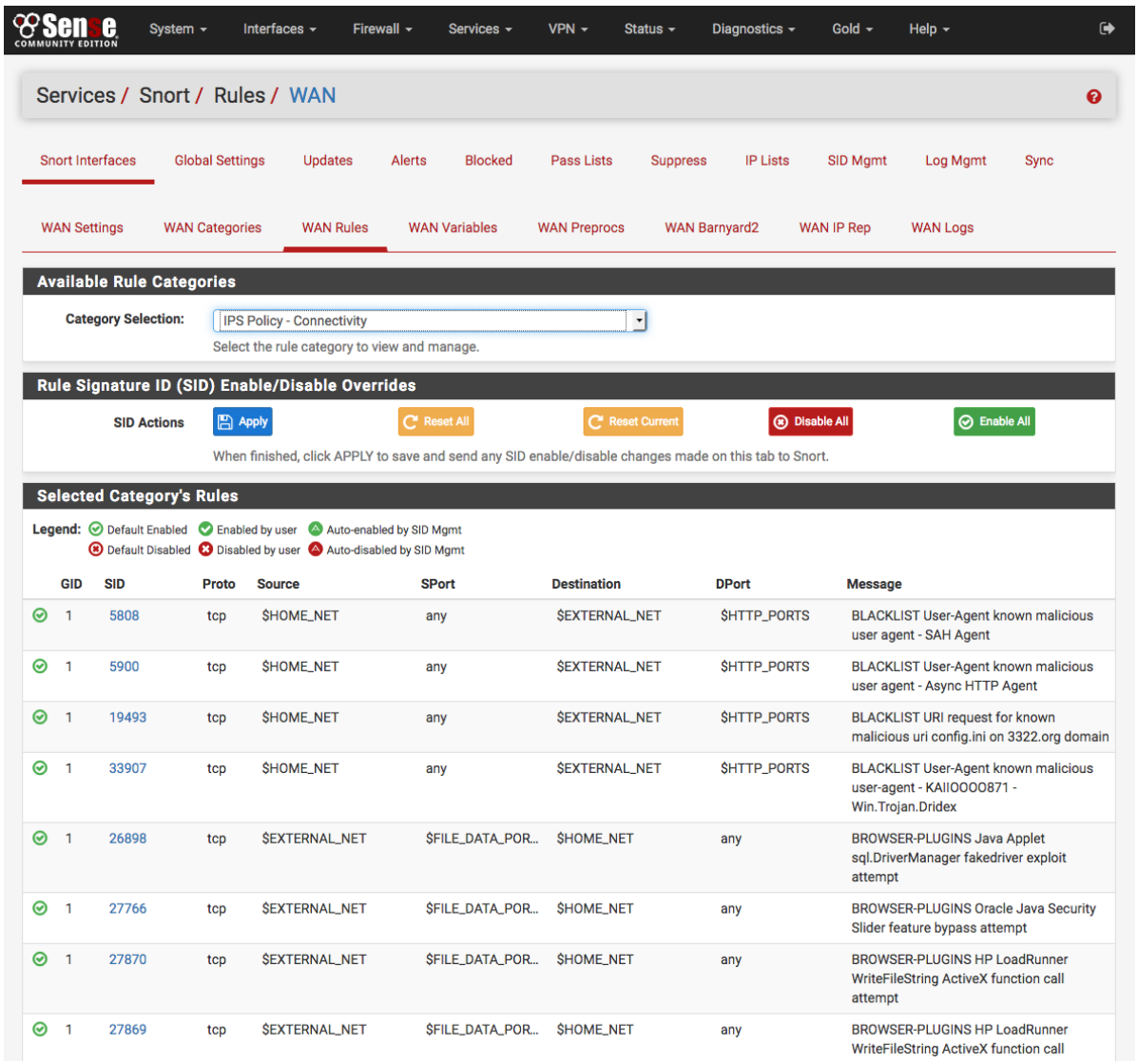


Рис. 1. Экран управления IPS Snort

Также с помощью конструктора Neural Designer была построена и обучена пятислойная нейронная сеть (Рис. 2).

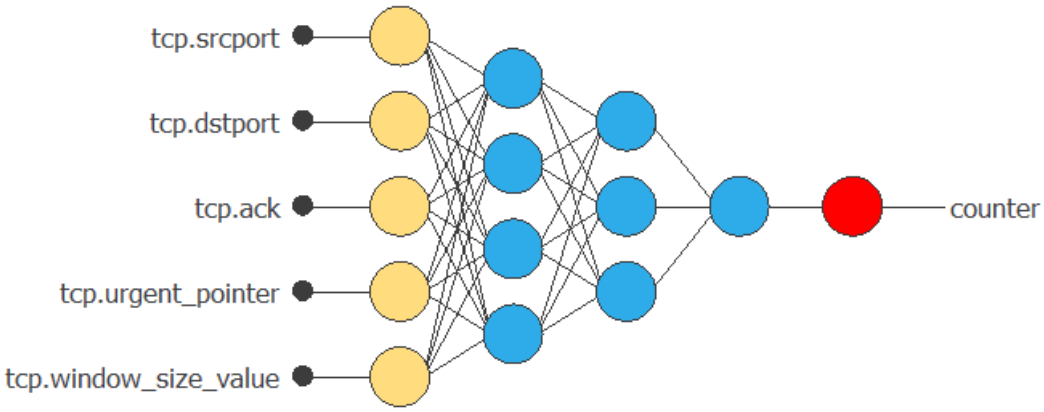


Рис. 2. Нейронная сеть для анализа протокола TCP

Дампы пакетов протокола TCP созданы следующим образом: для полей Source Port, Destination Port, Acknowledgement Number, Urgent pointer и Window Size по одному дампу, содержащему вложения и два дампа, один из которых не содержит вложений, и один, содержащий вложения во все поля.

Нейронная сеть продемонстрировала следующие результаты (Табл. 1).

Табл. 1. Результат работы нейронной сети

Исследуемое поле	**Всего пакетов в дампе**	**Обнаружено пакетов**	**Пакетов с вложениями**
Source port	3615	666	666
Destination port	9681	591	586
Acknowledgement number	12096	586	586
Urgent number	1805	774	774
Window size	8084	475	704
Контрольный дамп	8756	0	0
Вложение во все поля	13561	886	1082

Исходя из приведённых выше результатов можно утверждать о том, что программное средство выявляет вложения в различные поля пакетов всеми методами с достаточно высокой точностью. Также программа прошла проверку на ложные срабатывания, правильно определив отсутствие пакетов в контрольном дампе.

В результате пересылки пакетов с вложениями через систему IPS, был заблокирован трафик с вложениями в поля Destination port и Urgent pointer. Данный трафик был помечен как «Misc activity» в случае с Destination port и «Unknown traffic» в ситуации с Urgent pointer. Также «Misc activity» был помечен трафик, содержащий вложения во все поля заголовков. При проверке на контрольном дампе блокировки отсутствовали.

Исходя из полученных результатов можно утверждать, что нейронная сеть детектирует вложения в поля заголовков пакетов протокола TCP более эффективно, в сравнении с IPS-системой Snort со стандартным набором правил.

СПИСОК ЛИТЕРАТУРЫ

1. Ушаков, И.А. Организация, принципы построения и функционирования компьютерных сетей / И.А. Ушаков, А.В. Красов, Н.В. Савинов // Academia — 2019. — С. 240

2. Костырин, А.С. Обзор возможностей реализации канальной стеганографии на основе протоколов сетевого и транспортного уровней модели OSI / А.С. Костырин, А.В. Красов // Актуальные проблемы инфотелекоммуникаций в науке и образовании. — 2017. — С. 437 – 443.

3. Салита, А.С. Создание стеганографического канала при помощи полей / А.С. Салита, А.В. Красов // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2021. – № 2. – С. 36-40. – DOI 10.46418/2079-8199_2021_2_6. – EDN TLRNVO.

4. Волкогонов, В.Н. Методы и способы создания стеганографических вложений в сетевых пакетах / В.Н. Волкогонов, Е.М. Гетьман, А.С. Салита // Актуальные проблемы инфотелекоммуникаций в науке и образовании. — 2021. — С. 178 – 183.

5. Mazurczyk, W. Steganography of VoIP streams / W. Mazurczyk, K. Szczypiorski // Proceedings of the OTM 2008 Confederated International

Conferences, CoopIS, DOA, GADA, IS, and ODBASE 2008. Part II on On the Move to Meaningful Internet Systems — 2008 — С. 1001–1018

6. Chourib, M. Detecting selected network covert using machine learning / M. Chorib // The 2019 international conference on high performance computing & simulation – 2019 – Dublin, Ireland. Hal-02460864

7. Mazurczyk, W. Retransmission steganography and its detection / W. Mazurczyk, M. Smolarczyk, K. Szczypiorski // Soft Computing — 2009 — 15(3) — С. 505–515.

8. Алейников, А.А. Контроль, измерение и интеллектуальное управление трафиком : монография / А.А. Алейников, К.З. Билятдинов, А.В. Красов, М.В. Левин // Санкт-Петербург : Центр научно-информационных технологий "Астерион", 2016. – 92 с. – ISBN 978-5-00045-385-8. – EDN WLROTL.

9. Диордица, В. Н. Исследование современных методов сетевой стеганографии / В. Н. Диордица, А. В. Красов, А. И. Таргонская // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020) : IX Международная научно-техническая и научно-методическая конференция : сборник научных статей, Санкт-Петербург, 26–27 февраля 2020 года. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2020. – С. 404-409.

10. Коржик, В.И. Цифровая стеганография и цифровые водяные знаки. / В.И. Коржик, К.А. Небаева, Е.Ю. Герлинг, П.С. Догиль, Федянин И.А // под общей ред. проф. В.И. Коржика. Санкт-Петербург, 2016. Том Часть 1 Цифровая стеганография.

Раковский Дмитрий Игоревич,
ассистент кафедры "Информационная безопасность"
(Московский технический университет связи и информатики), Москва, Россия.
E-mail: Prophet_alpha@mail.ru

ПРОГНОЗИРОВАНИЕ ПРОФИЛЯ ФУНКЦИОНИРОВАНИЯ КОМПЬЮТЕРНОЙ СИСТЕМЫ С ПРИМЕНЕНИЕМ АППАРАТА ТОЧЕЧНО-МНОЖЕСТВЕННЫХ ОТОБРАЖЕНИЙ

Системы обнаружения атак, основанные на методах обнаружения аномалий, демонстрируют высокие показатели эффективности обнаружения атак как известного, так и не известного типов [1, 2]. Принцип работы методов обнаружения аномалий основан на автоматическом построении модели нормального поведения компьютерной системы (КС) на основании данных о ее функционировании «в прошлом». Актуальной является задача прогнозирования профиля функционирования КС с целью своевременного обнаружения отклонения от нормального поведения. Решение данной задачи сводится к прогнозированию временных рядов на основании «исторических данных» [3, 4], учитывающих поведение системы «в прошлом» [5, 6].

Целью работы является обоснование модели обнаружения и предупреждения нарушений в КС посредством прогнозирования профиля поведения КС при помощи математического аппарата точечно-множественных отображений и многозначных зависимостей [7].

Обзор работ по теме исследования

Задачу прогнозирования можно рассмотреть с точки зрения задачи классификации [8]. Все алгоритмы классификации разделяются на четыре таксономические группы: бинарная однозначная классификация; многоклассовая однозначная классификация; бинарная многозначная

классификация; многоклассовая многозначная классификация. Однозначная классификация, базирующаяся на сопоставлении набору входных данных одного класса на выходе, хорошо разработана и представлена в множестве работ [9, 10].

Наиболее проработанной областью многозначной классификации является обработка естественных языков, медицины и изображений [11 - 13], что обусловлено постановкой задачи и спецификой исходных данных. Задачи информационной безопасности, решаемые при помощи многозначной классификации, широко представлены в новом паспорте специальностей «2.3.6. Методы и системы защиты информации, информационная безопасность (ИБ)». Сразу несколько пунктов паспорта включают в себя проблематику, решаемую аппаратом многозначной классификации, а именно: п.3; п.5; п.6; п.7; п.9; п. 16. В дополнение, разработанность проблемы многозначной классификации в области ИБ, в настоящее время, является слабой и часто базируется либо на экспертном подходе [14, 15], либо на аппарате математической статистики. Ограничения, накладываемые вышеописанными подходами, обуславливают актуальность работ по данному направлению.

Алгоритм Прогноза Многозначных Зависимостей (АПМЗ)

АПМЗ принадлежит к классу алгоритмов многозначной классификации. Основная идея алгоритма базируется на математическом аппарате точечно-множественных отображений и многозначных зависимостей [7, 16, 17] и заключается в предположении, что из одного текущего момента времени «в настоящем» может проистекать одновременно несколько исходов «в будущем». Данное предположение требует информации о «исторических данных», адекватно описывающих КС в режиме нормального функционирования.

Пусть дано множество *A*, состоящее из *m* наборов значений дискретно изменяющихся атрибутов: $A \subseteq \{A_1 \times A_2 \times ... \times A_3\}; A_j = \{a_{t,j}\}; t = \overline{1,n};\ j = \overline{1,m}.$

Введем характеристику уровня обслуживания (*Service Level Objectives, SLO*, [18]) по каждому из атрибутов КС, выраженную категориальными понятиями.

К таким понятиям относятся состояния КС - $S = \{s_1, s_2, ..., s_m\} \cup \{s_{normal}\}$, связанные с порогами, $P = \{p_1, p_2, ..., p_m\}$, ограничивающими функционирование КС в штатном режиме. Состояние S_{normal} в таком контексте будет связано с отсутствием нарушений по каждому атрибуту КС.

«Исторические данные», характеризующие поведение КС, можно представить в табличном виде: $D_n = \{(a_1, s_1), ..., (a_n, s_n) | (a_i, s_i) \in S \times A\}$. Для работы АПМЗ из исходных данных необходимо выделить столбец значений функции состояния S - информацию о состояниях КС в каждый момент времени: $f : D_n \to L; L = \{l_t\}, t = \overline{1,n}$. l_t является множеством. При одновременном превышении нескольких порогов *P* SLO, КС может находиться одновременно в нескольких состояниях (состояниях нарушения по нескольким SLO; $|l_t|>1$).

На первом этапе пользователем выбираются:

- момент времени *step*, для которого необходимо построить прогноз;
- объем «исторических данных», подвергаемый обработке алгоритмом (горизонт прогнозирования, *gor*).

Момент времени *step* следует трактовать как «сдвиг в будущее» относительно текущего момента времени. Например, *step=3* будет означать сдвиг на 3 отсчета времени «в будущее» от текущего момента времени.

Для построения прогноза из набора данных, ограниченного горизонтом прогнозирования *gor*, надо выделить все возможные зависимости значений

временного ряда «в настоящем» от τ значений временного ряда «в прошлом» через *step* отсчетов времени. Данную тройку: (τ значений временного ряда «в прошлом» ; сдвиг *step* ; значение временного ряда в «настоящем») назовем **зависимостью**. Для выделения зависимостей используется подход в виде «скользящего окна»:

$$\begin{aligned} &Lib_{step,\tau} = \left\{\left(L^* \cdot F\right)\right\}, \\ &L^* = \left\{L\left(c + j\right)\right\}, F = \left\{L\left(c + j + step\right)\right\}, \\ &c = \overline{1, gor - step - \tau},\ j = \overline{0, \tau - 1}. \end{aligned} \tag{1}$$

Иллюстрация выделения зависимостей (1) из «исторических данных» в пределах [*n-gor*; *n*] приведена на рис. 1. Областью I показана «историческая часть» получаемой зависимости; областью II – часть данных, игнорируемых скользящим окном (т.н. сдвиг *step*); конец области II, соответствует моменту времени *n*, являющийся значением временного ряда в «настоящем».

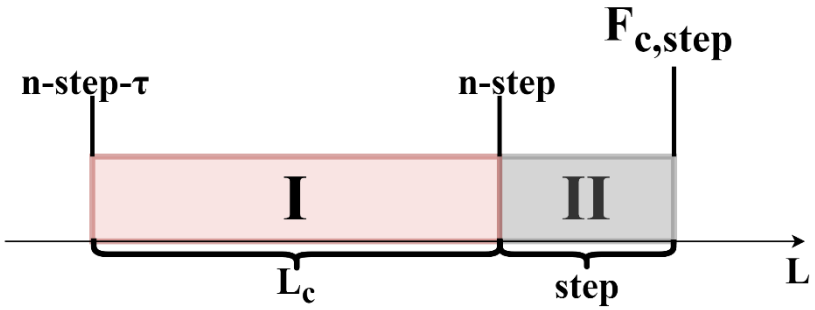


Рис. 1. Процесс порождения зависимостей из «исторических данных» при помощи «скользящего окна».

Порождение вышеописанных зависимостей есть нахождение точечно-множественного отображения. Дополнительной особенностью АПМЗ является применение математического аппарата многозначных зависимостей для расширения исходной выборки и повышения обобщающей способности алгоритма.

Каждая выявленная зависимость характеризуется упорядоченным вектором из τ значений временного ряда «в прошлом». При этом, поскольку

вектор значений временного ряда «в прошлом» формируется из «исторических данных», он жестко привязан к предыдущим наблюдениям.

Для повышения обобщающей способности некоторые позиции такого вектора можно рассматривать в качестве произвольных, «мягких», значений. Правила, определяющие «мягкие» позиции в векторе τ значений временного ряда «в прошлом», назовем масками:

$$\begin{aligned} &Mask = \left\{ msk_{(2)} \right\},\ msk = \overline{1, 2^{\tau}},\ \tau = \overline{minLength, maxLength}. \\ &minLength > 0,\ maxLength < gor - step. \end{aligned} \tag{2}$$

Процесс применения таких правил назовем наложением маски (2) на последовательность (1), а результат – шаблоном:

$$\begin{aligned} &temp_{\tau} : Lib_{step,\tau} \to \left\{ \left(L^{*} \dot{\&}\, msk_{(2)} \times M_{\tau} \cdot F \cdot W \right) \right\}, \\ &L^{*} \dot{\&}\, msk_{(2)} = \left\{ lmsk_{j} \right\},\ j = \overline{1, |\, msk_{(2)}\, |},\ lmsk_{j} = \begin{cases} 1, если\ msk_{(2)} = 1 \\ zero, иначе \end{cases}, \\ &W = \left\{ \delta^{n-c} \right\},\ c = \overline{1, gor - step - \tau}. \end{aligned} \tag{3}$$

В данной записи δ^{n-c} – коэффициент устаревания для учета смены (дрейфа) концепта [19]. Каждому шаблону возможно сопоставить весовой коэффициент δ, зависящий от удаленности шаблона от текущего момента времени (получая таким образом взвешенный шаблон).

Полученные шаблоны необходимо отобрать. Отбор в АПМЗ происходит по нескольким критериям: по удаленности от настоящего момента времени и по распространенности (частотный критерий). В дополнение стоит отметить необходимость отбора шаблонов по текущей реализации зависимости, так как именно она используется для прогнозирования [17].

Отбор (3) по удаленности происходит следующим образом. Введем в рассмотрение порог веса взвешенного шаблона *state_level(τ)*, зависящий от «размера исторической части» шаблона, τ. Регулируя данный порог, возможно проводить отбор по удаленности:

$$temp_{\tau,StateLevel(\tau)} = \left\{ temp_\tau(j) \mid W_j \geq StateLevel(\tau) \right\},$$
$$j = \overline{|1, temp_\tau|}. \quad (4)$$

Отбор по частотному критерию (4) требует формирования частотной статистики по шаблонам. Частота (надежность) считается относительно значения временного ряда в «настоящем» у каждого шаблона:

$$relrule(s \in S, reliabilitylevel)_\tau = \begin{cases} 1, stat_{temp_\tau, s \in S} \geq reliabilitylevel \\ 0, \textit{иначе} \end{cases},$$
$$stat_{temp_\tau, s \in S} = \sum_{F_j \in s} W_j,\ j = \overline{|1, temp_\tau|}. \quad (5)$$

Регулируя порог надежности взвешенного шаблона *reliabilitylevel* (5), возможно производить отбор шаблонов по частоте.

Финальные этапы работы АПМЗ посвящены голосованию о выборе наиболее релевантного значения временного ряда в «настоящем» через *step* отсчетов времени. Голосование может происходить посредством отбора уникальных значений временного ряда через суммарный вес. При этом весовая статистика считается в пределах разных «размеров исторической части» шаблона, τ. После определения победителей при разных τ, производится финальное голосование по мажоритарному принципу. Для учета минимально допустимого количества шаблонов может вводится порог голосования *wdifference*. Для учета минимально допустимого числа участников голосования может вводится порог голосования для выдачи прогноза *votelevel*. В самом простом случае решающее правило для определения победителя в голосовании определяется мажоритарным принципом: $winner = s \mid \max\left(stat_{temp_\tau, s \in S} \right)$.

После определения победителя, АПМЗ выдает прогноз, и его работа считается завершенной. Обобщенная схема работы АПМЗ приведена на рис. 2.

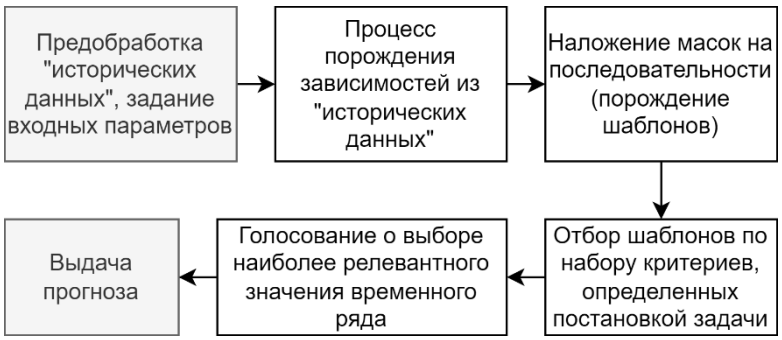


Рис. 2. Обобщенная структура работы АПМЗ.

Разработанный алгоритм прогнозирования (как и сам математический аппарат точечно-множественных отображений многозначных закономерностей), может быть обобщен на любую предметную область, содержащую «исторические данные» - экономика, логистика, кибернетика и т.д. Тип данных не имеет значения – прогнозироваться могут как категориальные, так и метрические значения функции.

Обобщающая способность алгоритма регулируется математическим аппаратом многозначных зависимостей, который, в свою очередь, требователен к вычислительным мощностям. Основным недостатком предложенного алгоритма является необходимость точной настройки входных параметров под каждый набор «исторических данных».

Выводы

Предложен **новый** алгоритм прогнозирования профиля нормального функционирования компьютерных систем, выраженных категориальными понятиями, на основе «исторических данных».

СПИСОК ЛИТЕРАТУРЫ

1. Гайфулина Д.А. Применение методов глубокого обучения в задачах кибербезопасности. Часть 1 / Гайфулина Д.А., Котенко И.В. // Вопросы кибербезопасности. 2020. № 3 (37). С. 76-86. DOI: 10.21681/2311-3456-2020-03-76-86

2. Гайфулина Д.А. Применение методов глубокого обучения в задачах кибербезопасности. Часть 2 / Гайфулина Д.А., Котенко И.В. // Вопросы

кибербезопасности. 2020. № 4 (38). С. 11-21. DOI: 10.21681/2311-3456-2020-04-11-21

3. Емалетдинова Л.Ю. Метод построения прогнозной нейросетевой модели временного ряда / Емалетдинова Л.Ю., Мухаметзянов З.И., Катасёва Д.В., Кабирова А.Н. // Компьютерные исследования и моделирование. 2020. № 4. С. 737-756. DOI: 10.20537/2076-7633-2020-12-4-737-756

4. Цымблер М.Л. Параллельный алгоритм поиска лейтмотивов временного ряда для графического процессора / Цымблер М.Л., Краева Я.А. // Вестник Южно-Уральского государственного университета. Серия: Вычислительная математика и информатика. 2020. № 3. С. 17-34. DOI: 10.14529/cmse200302

5. Shatnawi M. Real-time failure prediction in online services / Shatnawi M., Hefeeda M. // IEEE Conference on Computer Communications (INFOCOM). 2015. С. 1391–1399. DOI: 10.1109/INFOCOM.2015.7218516

6. Шелухин О.И. Мониторинг и диагностика аномальных состояний компьютерной сети на основе изучения "исторических данных" / Шелухин О.И., Осин А.В., Костин Д.В. // T-Comm: Телекоммуникации и транспорт. 2020. №4. С. 23-30. DOI: 10.36724/2072-8735-2020-14-4-23-30

7. Молодцов Д. А. Новый метод применения многозначных закономерностей / Молодцов Д. А., Осин А. В. // Нечеткие системы и мягкие вычисления. 2020. № 2. С. 83-95. DOI 10.26456/fssc72

8. Михайлова Е.Б. Проблема классификации моделей и методов прогнозирования / Михайлова Е.Б. // Учет и статистика. 2017. №1 (45).

9. Старовойтов В.В. Сравнительный анализ оценок качества бинарной классификации / Старовойтов В.В., Голуб Ю.И. // Информатика. 2020. Т. 17. № 1. С. 87-101. DOI: 10.37661/1816-0301-2020-17-1-87-101

10. Жуков Д.А. Задачи обеспечения эффективности машинного обучения при диагностике технических объектов / Жуков Д.А., Клячкин В.Н. // Современные проблемы проектирования, производства и эксплуатации радиотехнических систем. 2016. № 10. С. 172-174.

11. Dong Q. Imbalanced deep learning by minority class incremental rectification / Dong Q., Gong S., Zhu X. // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2019. Т. 41. № 6. С. 1367-1381. DOI: 10.1109/ТПАМИ.2018.2832629

12. Tsarev D. Using nmf-based text summarization to improve supervised and unsupervised classification / Tsarev D., Petrovskiy M., Mashechkin I. // В сборнике: Proceedings of the 2011 11th International Conference on Hybrid Intelligent Systems, HIS 2011. 2011. С. 185-189. DOI: 10.1109/HIS.2011.6122102

13. Карпович, С. Н. Многозначная классификация текстовых документов с использованием вероятностного тематического моделирования ml-PLSI / С. Н. Карпович / Карпович, С. Н. // Труды СПИИРАН. 2016. № 4 (47). С. 92-104. DOI 10.15622/sp.47.5.

14. Большаков А. С. Эффективный метод многокритериального анализа в области информационной безопасности / Большаков А. С., Раковский Д. И. // Правовая информатика. 2020. № 4. С. 55-66. DOI 10.21681/1994-1404-2020-4-55-66.

15. Большаков, А. С. Внедрение системы менеджмента информационной безопасности как мера борьбы с угрозами обществу в информационной сфере / Большаков, А. С. // Прогнозируемые вызовы и угрозы национальной безопасности Российской Федерации и направления их нейтрализации: Сборник материалов круглого стола, Москва, 25 августа 2021 года. Москва: Издательский дом «ИМЦ», 2021. С. 113-124.

16. Молодцов Д. А. Экстраполяция многозначных зависимостей / Молодцов Д. А. // Нечеткие системы и мягкие вычисления. 2017. № 1. С. 45-63.

17. Молодцов Д. А. Сравнение и продолжение многозначных зависимостей / Молодцов Д. А. // Нечеткие системы и мягкие вычисления. 2016. №2. С. 115–145

18. Rastegari Y. Optimal Decomposition of Service Level Objectives into Policy Assertions / Rastegari Y., Shams F. // The Scientific World Journal. 2015. № 3. С. 1-9. DOI:10.1155/2015/465074

19. Шелухин О.И. Алгоритмы обнаружения дрейфа концепта при потоковой классификации трафика мобильных приложений / Шелухин О.И., Барков В.В., Секретарёв С.А. // REDS: Телекоммуникационные устройства и системы. 2020. Т. 10. № 3. С. 19-27.

Соколов А. С.,
МИРЭА, студент
Шутов В. А.,
МИРЭА, преподаватель

ШИФРАТОРЫ, ДЕШИФРАТОРЫ И ИХ ЗНАЧЕНИЕ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: *Целью данной статьи является анализ одной из важнейших областей в информационной безопасности – шифрование данных. Так на примере простейшей программы на языке программирования python был изучен процесс шифрования данных, и, соответственно, его дешифрования. Таким образом, при детальном рассмотрении понятия шифр был сделан вывод о том, насколько безопасным и открытым он является, а также составить модель закрытой системы для передачи информации на основе шифрования данных.*

Ключевые слова: *информационная безопасность, шифратор, дешифратор, шифр, передача информации*

Шифр – это некая система преобразований, которая может быть позже интерпретирована, то есть прочитана с использованием некоторого ключа, уникального для каждого шифра. В настоящее время системы, работающие на принципе шифрования являются наиболее актуальными в связи с огромным количеством случаев утечек данных пользователей. С помощью системы шифров информация может быть защищена и доступна только определенному кругу лиц. Однако, если так называемый ключ, который может представлять собой буквально что угодно: от одного слова до целого предложения, попадет в руки злоумышленников, это может повлечь за собой утечку информации, что в свою очередь может стать причиной непоправимых последствий.

Взглянув на рисунок 1, на котором изображена картина известного художника Яна Брейгеля Старшего, вряд ли кто-нибудь сможет найти

отличий между изображением слева и справа, ведь никакой видимой разницы нет.

Рисунок 1 – Зашифрованная и незашифрованная картинки

Суть состоит в том, что внутри изображения справа зашифрован текст с именем автора с помощью программы на языке программирования python. Результат работы программы, которая дешифрует изображение можно увидеть на рисунке 2 (красным подчеркнуто имя автора, зашифрованное в картинке).

```
Выберете цифрой: 1 или 2
1) Встроить текст
2) Извлечь текст
Ответ: 2
Введите длину текста, которая храниться в данном изображении: 22
Извлеченный текст: jan brueghel the elder
```

Рисунок 2 – Результат работы программы-дешифратора

Все это стало возможным благодаря стеганографии – науке о скрытой передаче информации так, чтобы эта информация была недоступна третьим лицам. В качестве контейнеров для секретных сообщений могут выступать самые разные цифровые объекты (самый распространенный – цифровое изображение). Все существующие методы встраивания информации в цифровое изображение делятся на два больших класса: методы пространственного встраивания и методы частотного встраивания. Методы пространственного встраивания напрямую изменяют значения пикселей

изображения, в то время как методы частотного встраивания вносят изменения в значения частотных коэффициентов, полученных после предварительного применения некоторого частотного преобразования к матрице пикселей.

Самый простой метод пространственного встраивания – метод замены наименее значимого бита. Для встраивания секретное сообщение необходимо преобразовать в двоичную последовательность. Метод LSB предполагает замену одного или нескольких младших битов пикселей битами секретного сообщения при встраивании информации. Чтобы извлечь встроенную информацию, необходимо последовательно обойти пиксели изображения и сформировать последовательность из нужного количества младших битов каждого пикселя. При необходимости извлеченная битовая последовательность преобразуется в изображение.

Для оценки качества встраивания информации в изображения, в том числе по методу LSB, используют различные характеристики. Наиболее распространёнными из них являются незаметность и ёмкость встраивания. После ввода текста (на английском языке), который необходимо встроить, программа преобразует данный текст в двоичную форму. Программа рассчитывает количество бит, которые будут заменены в каждом цвете пикселя и встраивает текст в двоичной форме в массив, содержащий rgb данные (в двоичной форме). Чем выше разрешение исходного изображения, тем больше информации в нее можно записать. Такое изображение может быть отправлено другому пользователю, у которого есть ключ, любым доступным способом – оно будет дешифровано однозначно.

На основе вышеперечисленных способов шифровки и остальных возможностей, предоставляемых каждому пользователю для безопасной передачи своих данных, может быть создана уникальная система, аналогов которой не существует на современном рынке. Чаще всего в основе подобных систем встречается неминуемый доступ третьих лиц к данным,

например, переписке, именно поэтому многие всерьез задумываются над созданием закрытых каналов связи. Будет также существовать несколько вариантов данной закрытой системы: локальной или, так называемой, “полевой”, или более обширной, которая будет распространять свое действие на большие расстояния.

Если рассматривать более локальный вариант, то он чаще всего будет распространять свое действие на малые дистанции, так как будет реализован на базе одноплатных компьютеров таких, например, как Raspberry Pi, который имеет возможность работать как выделенный локальный сервер, пример четвертой модели можно увидеть на рисунке 3

Рисунок 3 – Raspberry Pi 4

Доступ к каналу связи получат только пользователи, которым будет выдан уникальный временный токен, например, в виде специального набора символов, дающий на ограниченное время выбранному пользователю возможность передать данные по закрытому каналу связи. Владелец такого сервера самостоятельно будет выбирать пользователя, которому будет предоставлен токен для входа, а преимуществом данного решения является ограниченность времени сессии и невозможность повторного использования данного токена. Данные, которые отправляют пользователи будут зашифрованы технологией двойного шифрования с помощью таких средств, как, например, MedusaLocker, GlobeImposter или подобных решений, и смогут быть дешифрованы однозначно при помощи токена. Данная система

может быть обширна применена во многих отраслях, ведь возможности raspberry pi практически безграничны на поприще автоматизации и программирования. Например, одноплатный компьютер может с легкостью превратиться в точку доступа wifi, стать полноценным медиа-сервером в локальной сети, с помощью которого можно воспроизводить мультимедийные файлы, SRD-приемником для воспроизведения радио, а также приема радиосигналов, ну и полноценной точкой-приемника для сервиса Flightradar24 – сервис для отслеживания публичных воздушных полетов. Все это в очередной раз доказывает, что подобная система благодаря своим особенностям наверняка найдет широчайшее применение в военной отрасли, ведь с полевых условиях может быть достигнута максимальная эффективность, а также сохранность передаваемых данных.

Обширное же решение будет работать по такому же принципу, однако будет осуществляться на базе выделенного сервера, который является доступным решением для всех пользователей. С его помощью передача зашифрованных данных может производиться из любой точки мира. Единственным препятствием на пути полной конфиденциальности такой системы является возможность третьих лиц получить доступ к локальному каналу связи, но она будет решена на основе новейшего программного обеспечения и перечисленных выше методов шифрования.

Таким образом использование доступных обычным рядовым пользователям инструментов способно в достаточном объеме защитить их данные, именно поэтому представленная выше система является универсальным решением и не имеет аналогов на рынке. Бесспорно, не существует идеально защищенных систем, именно поэтому государство должно особенно заинтересовано во введении и разработке новых безопасных моделей систем безопасности, а также помогать организациям, специализирующихся на этой теме с целью развития данного направления.

СПИСОК ЛИТЕРАТУРЫ

1. Мао В. Современная криптография. Теория и практика. – М.: Вильямс, 2005. – 763 с.

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

3. Сингх С. Книга шифров. Тайная история шифров и их расшифровки. М.: Аст, Астрель, 2006. – 447 с.

4. Ростех [Электронный ресурс] / Режим доступа: https://rostec.ru/news/kriptografiya-istoriya-shifrovalnogo-dela, свободный (дата обращения 03.10.22).

5. Хабр: 5 способов полезного использования Raspberry Pi [Электронный ресурс] / Режим доступа: https://habr.com/ru/post/472778/, свободный (дата обращения 06.10.22).

6. Научная электронная библиотека «КиберЛенинка»: Оценка эффективности методов стеганографического встраивания информации в спектральную область изображений [Электронный ресурс] / Режим доступа: https://cyberleninka.ru/article/n/otsenka-effektivnosti-metodov-steganograficheskogo-vstraivaniya-informatsii-v-spektralnuyu-oblast-izobrazheniy/viewer, свободный (дата обращения 06.10.22).

7. Исследование различных критериев оценки серии оптических изображений в методе датчика деформации интегрального типа [Электронный ресурс] / Режим доступа: http://www.ict.nsc.ru/jct/getfile.php?id=1599, свободный (дата обращения 06.10.22).

Штеренберг Станислав Игоревич
Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики», доцент, к.т.н.,
stas.shterenberg.89@mail.ru

ИССЛЕДОВАНИЯ РАЗВИТИЯ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ В РАМКАХ КОНЦЕПЦИИ РАЗВИТИЯ ЧЕТВЕРТОЙ ПРОМЫШЛЕННОЙ РЕВОЛЮЦИИ «ИНДУСТРИЯ 4.0»

Введение. Тематика четвертой промышленной революции (далее - Индустрия 4.0) затронута неслучайно. В данном тезисе делается направление на исследования для мультиагентных систем искусственного интеллекта (далее - ИИ). Будет объяснено почему данный путь развития отечественных ИИ-систем, может быть, в определённой части прорывным и правильным с точки зрения построения как раз систем защиты информации (далее – СЗИ). Программный агент (далее – ПА, он же «нейрон») имеет ключевую важность в построении перцептрона, а и в дальнейшем всей нейросети ИИ. Это и становится важной и отправной точкой в развитии биоаналогичного ИИ способного встроиться в общую технологическую сингулярность и сохранить технологическую базу РФ в рамках концепции Индустрия 4.0.

Более подробный путь развития отечественных СЗИ в рамках концепции Индустрия 4.0 возможно наиболее удачным образом выразил С.А. Петренко в своих работах [1,2]. Большинство экспертов по кибербезопасности считают, что созданные киберсистемы на основе технологий Индустрии 4.0 не обладают требуемой киберустойчивостью, из-за высокой структурной и функциональной сложности названных систем [3,4]. Для воплощения противостоянию разнородно-массовых [1] компьютерных атак требует решение главной научной проблематики – организации самовосстанавливающейся модели СЗИ, имеющей принципы и технологии сбора и обработки Больших данных, потоковой работы по глубокому обучению ИИ систем.

Подобных систем не существует в мире или они проходят стадию прототипа. Технологии ИИ направлены на обеспечивание «человеческих нужд» в плане обеспечения СЗИ прочего софта или частных решений крупных и малых ИТ-компаний [5]. Сейчас, в 21 веке проблема выглядит еще

более усугубленной из-за огромного присутствия на рынке гаджетов и ИИ-помощников, но во всех случаях ИИ не обеспечивает защиту сам себе. Почему это важно? Существует версия, что в «нейроне» не присутствует так называемая «иммунная защита» [6]. Общий искусственный интеллект в данной работе [6] больше обращается к мультиагентному подходу и каждый ПА в разной степени уязвим. Каждый ПА в новом ИИ это синтез логики и вероятности, использования адаптивных механизмов и экспертных систем.

Текущая кризисная ситуация в экономике России, сопровождающаяся падением ВВП, снижением платежеспособности населения страны, а также ростом инфляции сделали невозможным поддержание импорта на прежнем уровне. В то же время именно сейчас появились предпосылки для наиболее эффективной реализации импортозамещающей политики, необходимость реализации которой в современной России определяется как возможность избавления от импортозависимости и обеспечения информационной безопасности государства. Информационная безопасность является важной проблемой, внимание к которой усилилось после перехода на стратегию импортозамещения. Так В.В. Путин утвердил в 2016 году «Доктрину информационной безопасности Российской Федерации» (далее Доктрина) [3,4]. Данная Доктрина содержит указания на реализацию стратегии импортозамещения в области защиты информации.

Идея будет казаться примитивной, но одновременно и сложной в реализации. Однако такой подход обеспечит её развитие на годы вперед. Сначала необходимо произвести по отдельности ПА, затем объединить их в общем вычислительном процессе единого перцептрона. Сам перцептрон – это и будет первая модели полноценной нейросети, которая сложится за счет датчиков с ассоциативными элементами в единый программный комплекс. Все ПА будут выполнять отдельные функции (например, стегозащита, реагирование на вирусные атаки, символьные вычисления и др.). В последствии приобретенных «навыков» ИИ-система будет собираться воедино, но при сигнале атаки на них уничтожаться и сохраняться в виде децентрализованной мультиагентной системы. По первому же сигналу, оповещаемому о безопасности среды, мультиагентная система соберется вновь в единый перцептрон. Данная концепция берет свое начало из теоремы сходимости перцептрона, описанной и доказанной Ф. Розенблаттом [7]. Однако она же и была опровергнута ввиду того, что Марвин Минский не знал еще о существовании Больших данных [8]. Но теперь в современном мире такие возможности есть. И именно Большие данные и будут

использоваться при обмене, накоплении ассоциативной памяти у зарождающегося ИИ.

Важно отметить, что большинство из программного обеспечения чаще представлены на блок-схемах. Задача лишь состоит в том, чтобы найти составные части общего алгоритма и стабилизировать процесс глубокого обучения в дальнейшем при сборке при помощи ПА в правильную самоорганизующуюся карту нейронов. В докладе не постулируются научные результаты сформулированные Ф. Розенблаттом за основные, т.к. его примитивный нейрокомпьютер и понятия не моги иметь о современных языках программирования. Возможность построения нейросетей с достойными механизмами машинного обучения представляется в работах [9-12]. Ключевая технология искусственных нейронных сетей, идея которых состоит в том, чтобы максимально близко смоделировать, ну скажем, человеческий мозг, возможна потому как имеет стало возможным формировать ассоциативную память у ИИ в распределённой информационной системе. Но опять же, защиты самого ИИ в такой ИИ системе не предусмотрено. Развитие ИИ-систем должно обходиться без деструктивного воздействия со стороны человеческого фактора.

В настоящее время уже ведутся исследования по вопросам защиты ИИ. Имеются работы по способам построения ПА [13-15], работы по применению технологии Больших данных для задач ИИ и СЗИ [16,17], а также внедрения интеллектуального ПО в технологических процесс задач защиты информации [18]. Поэтому первичные задачи в его построении возможно сформулировать так:

1. произвести автоматическую генерацию кода программного автоматизированного агента (он же «нейрон») в защищаемом программном обеспечении с поддержкой протоколирования Больших данных;
2. воспроизвести логическую схему перцептрона с описанием всех связей, сигналов, входов и выходов;
3. разработать методику построения самоорганизующейся карты программных агентов (далее – ПА, он же «нейрон») действующих в составе системы обнаружения вторжения (далее - СОВ);
4. смоделировать процесс обработки Больших данных при помощи разработанного перцептрона, применяющего ассоциативную память ИИ;
5. построить единую архитектуру ИИ с применением механизмов глубокого обучения для реагирования на компьютерные атаки направленные на нарушение целостности ПО;
6. обеспечить децентрализацию самоорганизующейся карты ПА, а затем и синхронизацию отдельных ПА в составе ИИ;

7. в рамках квазибиологической парадигмы обеспечить «выживание» ИИ и оценить его защищенность в распределенной информационной системе.

Т.о. обеспечив «самостоятельность» перцептрона возможно иметь исходный материал для развития ИИ в задачах уже большего масштаба, нежели СЗИ. Лишь тогда на первой стадии исследования, возможно, получения следующих результатов:

1. Модификация методики построения самоорганизующейся карты программных агентов (нейронов) для СОВ;
2. Ассимиляционная модель обработки Больших данных в РИС с использованием перцептрона, которая в отличие от существующих решений применяет ассоциативную память ИИ;
3. Новая архитектура системы ИИ в едином программном комплексе с синхронизацией компонентов мультиагентной нейронной системы, имеющая в основе квазибиологическую парадигму;
4. Новая методика обеспечения «жизнеспособности» ПА в РИС, в которой сформулирован новый принцип киберустойчивости архитектуры системы ИИ, обеспечивающий «переключение» на децентрализацию самоорганизующейся карты ПА.

В заключении доклада будет представлен прототип перцептрона и всей ИИ системы, а в перспективе и свойства «живучести» под атаками направленных на нарушение целостности ПО.

Данное исследование выполнено при финансовой поддержке Минцифры России (грант ИБ) в рамках научного проекта, Соглашение №. 40469-05/2022-д от 30.06.2022 г.

СПИСОК ЛИТЕРАТУРЫ

1. Петренко С.А., Киберустойчивость Индустрии 4.0: научная монография / СПб. «Издательский дом «Афина», 2020. 226 с.
2. Петренко С.А., Ступин Д.Д., Национальная система раннего предупреждения о компьютерном нападении: научная монография / под общей редакцией С.Ф. Боева. – 2е изд. – Университет Иннополис. – Иннополис: «Издательский Дом «Афина», 2018. – 448 с.
3. Слагода, В. Г. Основы экономической теории: учебник / В.Г. Слагода. — 3-е изд. — Москва: ФОРУМ: ИНФРА-М, 2021. — с. 252-253, 269 с.
4. Чернова В.Ю. Импортозамещение как фактор модернизации внешнеторговой и структурной политики России в современных

условиях (на примере агропродовольственного сектора): Автореф. дис. док. пс. наук. — Москва: РУДН, 2020 — 4 с
5. Джон Брокман, Искусственный интеллект – надежды и опасения: [сборник: перевод с английского В. Желнинова] / под ред. Джон Брокмана. – Москва: Издательство АСТ, 2020 – 384 с. – (Наука, идеи, ученые)
6. Александр Ведяхин, Сильный искусственный интеллект: Не подступах к сверхразуму / Александр Ведяхин [и др.]. – М.: Ителлектуальная Литература, 2021. – 232 с.
7. Фрэнк Розенблатт. Принципы нейродинамики: перцептроны и теория механизмов мозга / Перевод с английского В.Я. Алтаева, Б.А. Власюка, Ю.А. Крутикова, Ю.А. Патругина — М.: «Мир», 1965.
8. М. Минский, С. Пейперт. Персептроны / Перевод с англ. Г.Л. Гимельфарба, В.М. Шарыпанова— М.: «Мир», 1971.
9. Николенко С., Кадурин А., Архангельская Е., Глубокое обучение. — СПб.: Питер, 2018. — 480 с.: ил. — (Серия «Библиотека программиста»).
10. Хапке Х., Нельсон К., Разработка конвейеров машинного обучения.Автоматизация жизненных циклов модели с помощью TensorFlow / пер. с анг. Н. Б. Желновой. – М.: ДМК Пресс, 2021. – 346 с.: ил.
11. Нильсен, Эйлин., Практический анализ временных рядов: прогнозирование со статистикой и машинное обучение. : Пер. с англ. — СПб. : ООО “Диалектика”, 2021. — 544 с.: ил. — Парал. тит. Англ
12. Уорр Кэти, Надежность нейронных сетей: укрепляем устойчивость ИИ к обману. — СПб.: Питер, 2021. — 272 с.: ил. — (Серия «Бестселлеры O’Reilly»)
13. Штеренберг С.И., Красов А.В., Разработка методики построения доверенной среды на основе скрытого программного агента. Часть 1. Исследование // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 2. С. 14-20.
14. Штеренберг С.И., Красов А.В., Разработка методики построения доверенной среды на основе скрытого программного агента. Часть 2. Тестирование и оценка эффективности // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 3. С. 3-8.
15. Штеренберг С.И., Красов А.В., Разработка методики построения доверенной среды на основе скрытого программного агента. Часть 3. Принцип действия программного агента и проверка его работоспособности // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 4. С. 34-40.

16. Штеренберг С.И. Методика управления системами обработки и сбора больших данных с поддержкой мониторинга встроенными программными агентами // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 4. С. 26-35.
17. Красов А.В., Штеренберг С.И., Голузина Д.Р., Методика визуализации больших данных в системах защиты информации для формирования отчетов уязвимостей // Электросвязь. 2019. № 11. С. 39-47.
18. Штеренберг С.И., Стародубцев И.В., Шашкин В.С., Разработка комплекса мер для защиты предприятия от фишинговых атак // Защита информации. Инсайд. 2020. № 2 (92). С. 24-31.