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)

1 ноября 2022 г.

Всероссийская студенческая научно-практическая конференция

ВОПРОСЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

СБОРНИК ТРУДОВ

Москва – 2022

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.

Оглавление

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

НАУЧНАЯ СЕКЦИЯ «КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ И СЕТЕВАЯ БЕЗОПАСНОСТЬ»

НАУЧНАЯ СЕКЦИЯ «БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ»

НАУЧНАЯ СЕКЦИЯ «КИБЕРБЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ И КОМПЬЮТЕРНЫХ СИСТЕМ»

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

Хромова А.В.
Акционерное общество «Перспективный мониторинг»,
системный аналитик
РАНХиГС, аспирант
Anna.Khromova@amonitoring.ru

ТЕНДЕНЦИИ НАУЧНО-ТЕХНОЛОГИЧЕСКОГО РАЗВИТИЯ РОССИИ: СОЗДАНИЕ ЦИФРОВОГО СУВЕРЕНИТЕТА

Темпы развития современного научно-технического прогресса значительно опережают показатели даже конца прошлого тысячелетия. В рамках достижения установленных ООН Целей устойчивого развития (ЦУР) в русле реализации третьей промышленной революции мировое сообщество, как отмечается в последнем докладе ЮНЕСКО по науке, определило перспективу «двойного перехода» к будущему — одновременно к «зелёной» и цифровой экономике — основу которого составляет наука. Ведущую роль в этом процессе играют информационно-коммуникационные технологии (далее — ИКТ), которые служат драйвером современного общественного развития, поскольку именно они позволяют эффективно хранить, обрабатывать, анализировать и передавать информацию (данные) для получения новых знаний об объектах, процессах и явлениях окружающего мира.

Цифровизация активно входит в повседневную жизнь, определяя тренды современного научно-технологического развития. Скорость развития и распространения ИКТ ежегодно увеличивается, что не может не отражаться на социально-экономическом развитии регионов и стран, становясь всё более значимым его фактором. Сегодня «технологическая сфера стала ареной

противоборства ведущих держав и оказывает существенное влияние на расстановку сил в мире».

Конечно при повсеместной цифровизации науки, бизнеса, образования встает вопрос о цифровом суверенитете государств. В науке все больше исследований по цифровой тематике. Особенно сильно это повлияла пандемия, которая характеризуется повышенным эмоциональным и профессиональным выгоранием, высоким уровнем изоляции, развитием дистанционного обучения.

При изучении термина «суверенитет» стоит упомянуть Жана Бодена, который является основоположником теории государственного суверенитета. Согласно концепции, государство обладает неоспоримой полнотой власти над определенной территорией и ее населением [1].

Тем не менее, неоднородный характер развития ИКТ может способствовать и развитию рисков, важнейшим из которых является социальное неравенство. Кроме того, в контексте происходящих в 2022 году геополитических событий, обусловленных глобальным конфликтом между западными странами и Россией, возникшим в результате объявления президентом РФ В.В. Путиным, специальной военной операции на территории Украины, трансформируется и характер международного сотрудничества в области развития ИКТ — оно приобретает более национальный характер.

Способность государства обеспечивать цифровой суверенитет будет символизировать независимость в 21 веке. И.С. Ашманов определил «Цифровой суверенитет» как «право самостоятельно и независимо определять и внутренние и геополитические национальные интересы в цифровой среде; вести самостоятельную внутреннюю и внешнюю информационную политику; распоряжаться собственными информационными ресурсами и гарантировать электронную и информационную безопасность государства» [3].

С одной стороны, когда речь идет о цифровом суверенитете, то исследователи приводят в пример Китай с его «Великим китайским файерволом» и

тотальный контроль и цензура всех площадок средств массовой информации. Куба долгое время сохраняла информационную независимость, стараясь закрыться от американского влияния [2].

Российский сегмент сети Интернет является крупнейшим в мире, однако говорить о цифровом суверенитете не приходится.

Цифровой суверенитет государства зависит от множества факторов:

- научно-технологическое развитие государства;
- экономическое развитие;
- информационная безопасность;
- национальная безопасность.

Однако, если связать все вышеперечисленное, то, в целом, цифровой суверенитет строится на научно-технологическом развитии государства, как главном столпе цифровой независимости страны.

Пандемия, несмотря на все отрицательные факторы, послужила катализатором развития ИКТ и систем генерирования знаний.

Стоит выделить ключевые выводы относительно глобальных тенденций в сфере образования:

1. Расходы на науку в большинстве регионов мира выросли, но не менее 80% стран инвестируют в исследования и разработки менее 1%. Некоторые из них приведены в таблице ниже по тексту. Активный рост расходов на разработки начался в 2019-2020 гг., как раз в период развития Covid-19.

2. Наиболее активно инвестируют в разработки Республика Корея, Япония, Германия и Франция. Более того, согласно последним данным, лидерами исследований и разработок является Израиль, Республика Корея. Швеция и Бельгия, США, Япония, Австрия, Германия и Дания. Стоит отметить, что Израиль занимает лидерские позиции с начала 21 века [1]. Россия же, согласно последним данным, занимает 31 место (рис.1).

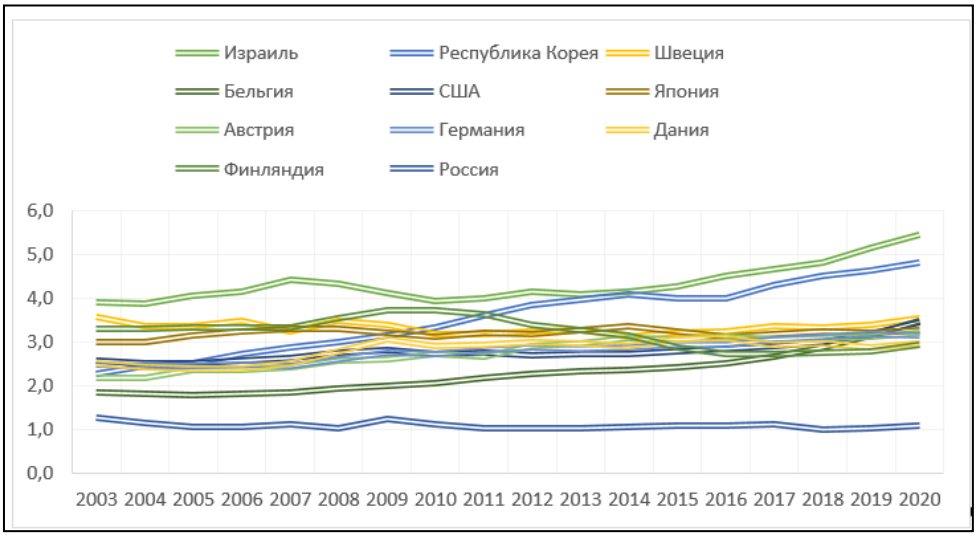


Рис. 1 - ТОП-10 стран-членов ОСЭР по расходам на исследования и разработки в мире и Российской Федерации, 2003-2020, % от ВВП (фильтр по лучшим странам в 2020 году)

Когда речь идет о глобальных тенденциях, необходимо включить высокотехнологичный сектор экономики, который отличается использованием передовых технологий. Высокотехнологичная отрасль представляет собой динамичную среду, определяемую как частыми изменениями в её составе, так и концентрацией рыночной власти за счет консолидации.

В методологических расчётах Отчёта о технологиях и инновациях UNCTAD [2] фигурируют следующие высокие технологии, применение которым уже находится в различных секторах жизнедеятельности:

- Искусственный интеллект (AI — Artificial intelligence).
- Интернет вещей (IoT — Internet of Things).
- Большие данные (Big data).
- Блокчейн (Blockchain).
- 5G.
- 3D-печать (3D printing).
- Робототехника (Robotics).

– Дроны (Drones).

– Редактирование генов, генная инженерия (Gene editing).

– Нанотехнологии (Nanotechnology).

– Солнечное фотоэлектричество (Solar photovoltaic).

В это же время, согласно «Концепции долгосрочного социально-экономического развития России» [9] к высокотехнологичным отраслям экономики относятся: авиационная промышленность, ракетно-космическая промышленность, атомный энергопромышленный комплекс, энергетическое машиностроение и ИКТ. Информационно-коммуникационные технологии (ИКТ) являются многогранными. Таким образом, понимание высокотехнологичного сектора в экономике является шире, чем на Западе.

Эксперты НИУ ВШЭ отмечают, что по масштабам научно-технологического потенциала современная Россия уверенно входит в группу ведущих мировых держав, однако выделяются следующие ключевые тренды:

– Видимость российской науки в глобальном научном пространстве усиливается, хотя она все еще недостаточно интегрирована в мировую научную повестку.

– Россия входит в группу лидеров по масштабам занятости в науке при сохранении тенденции к ее сокращению.

– Воспроизводство научных кадров сдерживается низкой эффективностью системы их подготовки.

– Влияние науки на экономическое развитие сдерживается низкой инновационной активностью бизнеса

– На фоне позитивного общественного восприятия науки в целом личный интерес россиян к ее достижениям незначителен [7].

В целом, стоит согласиться с выводом Счётной палаты РФ, которая в 2020 году постулировала, что российская «наука остаётся недостаточно продуктивной,

не формирует собственную научно-технологическую основу для создания и реализации приоритетов, реагирования на «большие вызовы», стоящие перед обществом и государством, не выступает драйвером для социально-экономического развития» [9].

Имеющиеся в России машины и оборудование являются довольно устаревшими. Так, их средний возраст в 2020 году составил 11,7 лет, при этом за последние 4 года в стране происходит устаревание машин и оборудования

Несмотря на устаревание, в России заметна тенденция формирования высокотехнологического сектора экономики. Так, если в 2017 году среднетехнологичные низкого уровня и низкотехнологичные виды деятельности незначительно отставали от высокотехнологичных и среднетехнологичных, то в 2020 году последние заметно «вырвались» вперёд, составив 12,9 % и 14,3 % соответственно. В целом, это говорит о положительной обеспеченности высокотехнологичным оборудованием в стране.

Однако, с другой стороны, нельзя не отметить, что степень износа основных фондов в России является неприлично высокой. Так, в среднем, в 2020 году она составила 50,1 %, т.е. больше половины отечественной «технологичности» изношена, при этом в среднем в динамике, с 2017 года, продолжается устаревание по всем уровням.

В этих условиях нет ничего удивительного в том, что Россия продолжает активно импортировать высокотехнологичные продукты из-за рубежа, при этом они составляют львиную долю всего импорта страны. Так, с 2013 года их доля в импорте страны значительно увеличилась с 62,4 % до 76,2 % (рис.2) [11]

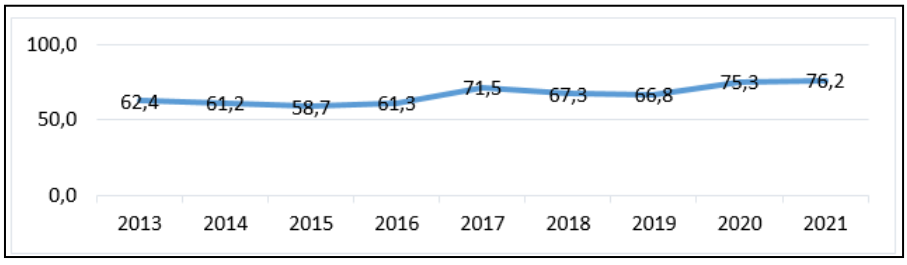


Рис. 2 - Динамика отношения высокотехнологичных товаров к общему объему импорта в Российской Федерации, 2013-2021 гг., %.

Анализ тенденций в высокотехнологичном секторе экономики России показывает, что, несмотря на некоторый рост по многим показателям научно-технологического развития, Российская Федерация продолжает оставаться в тени ведущих мировых стран. Также проблема состоит в том, что основная роль в стимулировании развития высокотехнологичного сектора экономики России принадлежит государству, а именно основанному на стратегических интересах финансированию, тогда как в мировой практике более распространённым является частное инвестирование в науку и технологии.

В рамках рассматриваемой темы сравнение показателей развития между Россией и мировыми лидерами не имеет смысла. Россия не находится на периферии мирового научно-технологического прогресса, но как минимум не входит в число лидеров по большинству показателей.

Согласно данным, которые представили НИУ ВШЭ и Министерство образования и науки РФ, доля ИКТ в ВВП страны в 2020 году составила 3,1%, когда в Концепции долгосрочного социально-экономического развития РФ до 2020 года целью ставились 10% [8]. Кроме того, если сравнивать долю ВВП с другими секторами экономики, то ИКТ находится в арьергарде национальной экономики [6].

Рис. 3 - Вклад ИКТ в ВВП Российской Федерации в 2020 году, %

Ввиду того, что повсеместная цифровизация вынуждает государства идти в ногу со временем, они активно инвестируют в разработки и высокие технологии. Лидерами по инвестициям и импорту технологий является Республика Корея, в то время, когда Российская Федерация продолжает оставаться в тени ведущих мировых стран.

Одной из основных проблем является в том числе быстрое устаревание использующихся основных фондов (транспорт, технологическое оборудование и т.д.).

Сравнивая показатели западных стран и России можно сделать следующие выводы:

1. Россия имеет возможность объединить усилия по развитию высоких технологий и созданию цифрового суверенитета с Азиатским регионом, однако это, в свою очередь, подтолкнет Китай к проведению своей интерпретации мягкой силы и его закреплению в экономике России.

2. В существующих геополитических условиях и при анализе вклада ИКТ в ВВП страны можно сделать вывод, что в данное время РФ не сможет выстроить действенную цифровую инфраструктуру.

3. Исходя из положительной динамики, можно сделать вывод, что Россия предпринимает активные попытки по раскачке технологической сферы экономики.

Список литературы

1. Data for the Sustainable Development Goals. — URL: http://uis.unesco.org/
2. UNESCO Science Report: the race against time for smarter development; executive summary, 2021. — URL: https://unesdoc.unesco.org/ark:/48223/pf0000377250
3. Ашманов И. С. Информационный суверенитет — новая реальность [Электронный ресурс]. https://files.runet-id.com/2015/tersm/tersm15-3--ashmanov.pdf
4. Бухарин В.В. Компоненты цифрового суверенитета российской федерации как техническая основа информационной безопасности. Вестник МГИМО-Университета. 2016;(6(51)):76-91. https://doi.org/10.24833/2071-8160-2016-6-51-76-91
5. Грищук В.М., Савчук Э.А. Национальная инновационная система: мировые тренды научно-технологического развития / В.М. Грищук, Э.А. Савчук // Новости науки и технологий. — 2020. — № 1 (52). — С. 3-9.
6. Индикаторы цифровой экономики: 2021: статистический сборник / Г.И. Абдрахманова, К.О. Вишневский, Л.М. Гохберг и др.; Нац. исслед. ун-т И60 «Высшая школа экономики». – М.: НИУ ВШЭ, 2021. – С. 76
7. Научно-технологическая политика России в условиях постпандемии: поиск новых решений [Текст]: докл. к XXII Апр. междунар. научн. конф. по проблемам развития экономики и общества, Москва, 13–30 апр. 2021 г. / С.В. Бредихин, В.В. Власова, М. А. Гершман и др.; науч. ред. Л. М. Гохберг; Нац. исслед. ун-т «Высшая школа экономики». — М.: Изд. дом Высшей школы экономики, 2021. — С. 18-37
8. О Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года: Распоряжение Правительства РФ N 1662-р от 17.11.2008 / СПС КонсультантПлюс. — URL: http://www.consultant.ru/document/cons_doc_LAW_82134/

9. Отчет о результатах экспертно-аналитического мероприятия «Определение основных причин, сдерживающих научное развитие в Российской Федерации: оценка научной инфраструктуры, достаточность мотивационных мер, обеспечение привлекательности работы ведущих ученых». — URL: https://fgosvo.ru/uploadfiles/Work_materials_disscusion/sp.pdf

10. Крамарова Е.Н. Международное сотрудничество и конкуренция в области научно-технологического развития на современном этапе / Е.Н. Крамарова // Проблемы национальной стратегии. — 2022. — № 1 (70). — С. 240-260.

11. Технологическое развитие отраслей экономики. — URL: https://rosstat.gov.ru/folder/11189

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

Анисимов М.А.,
студент 1 курса группы ЗРС2204
Крылов Г.О.,
МТУСИ, ст. преподаватель

СКАМ Terra Luna

ВВЕДЕНИЕ

Мир не стоит на месте и всегда появляется что-то новое. Например, в 2008 году впервые появился биткоин, который создал анонимный персонаж под именем Сатоши Накомото (до сих пор нет сведений — это один человек или группа людей). С этого времени начала развиваться криптовалюта.

Но я бы хотел рассказать вам о такой экосистеме, как Terra (Luna), которая в мае 2022 года потерпела падение в 99% от своей стоимости. На самом пике цена за монету составляла примерно 116$, на данный момент — это 0.00022$ за монету.

Данный проект собрал большую аудиторию на Азиатских рынках, а огромную популярность и поддержку приобрел в Южной Кореи, где находится офис Terra. Например, пассажир в Монголии уже мог платить водителям такси с помощью MemePay в токенах экосистемы Terra (в стейблкоинах, которые привязаны к валюте Монголии), а в некоторых магазинах люди могли моментально оплачивать свои покупки и товары с помощью приложения CHAI токенами проекта, когда в обычном приложении происходили задержки и различные ошибки.

А самым главным плюсом проекта было то, что он использовался, как обычные сервисы VISA и MASTERCARD, но был намного быстрее и брал комиссию для магазина максимум 1% (на практике было в разы меньше), когда обычные банки по 2-3% [3].

Благодаря этому проект смог завоевать популярность на рынках и был перспективным для будущих вложений. Многие участники криптомира рассматривали данный проект, как возможность увеличить свои активы.

ГЛАВА 1. ЗНАЧЕНИЕ TERRA В МИРЕ.

1.1 Что такое Terra?

Terra — это децентрализованный блокчейн протокол, который обеспечивает программируемые и стабильные деньги для Интернета. Согласно официальному техническому документу Terra, она сочетает стабильность цен и широкую поддержку фиатных валют с устойчивостью к цензуре биткоина (BTC), а также предлагает быстрые и доступные расчёты. С помощью своего протокола стабильной монеты, системы оракулов, смарт-контрактов и плана для массового использования проект создает основу для новой цифровой экономики [4].

В отличие от централизованных стейблкоинов, поддерживаемых 1:1 доллары США, такие как USDC и GUSD, стейблкоины Terra алгоритмически стабилизируются и поддерживаются собственным криптоактивом LUNA, который получает выгоду от вознаграждений за стейкинг для усиления сетевых эффектов.

Terra усиливала свои сетевые эффекты и еще больше способоствовала их внедрению за счет стейблкоинов в стиле сеньоражных акций и вознаграждений за стейкинг для держателей LUNA.

Токен LUNA действовал, как капитал, который приносил дивиденды, потому что холдеры получали 100% комиссий за транзакции, генерируемых платежами стейблкоинов.

По итогу, Terra создавала что-то революционное, предлагая конкурентоспособные программируемые платежи, логистику и инфраструктуру в сочетании с прибыльной бизнес-моделью и токеномикой [5].

1.2 Кто и когда создал Terra?

Terra была создана Terraform Labs и основана Даниэлем Шином и До Квоном в январе 2018 года.

Шин и Квон поделились идей, как можно облегчить массовое внедрение криптовалют путем создания цифровых активов с упором на стибальность цен и удобство использования. И как пример, они представили огромную платежную сеть, а также мощные продукты и сценарии их использования.

Чтобы показать данный вариант видения реализации этого проекта, они запустили свою сеть платежей в криптовалюте и блокчейне при поддержке Terra Aliance, состоящего из 15 крупных компаний электронной коммерции в Азии.

Дэниел Шин является основателем и генеральным директором Chai Corporation, одной из крупнейших платформ электронной коммерции в Азии. Также является основателем The Encore Company — стартап-студия, Ticket Monster — крупная южнокорейская платформа электронной коммерции и Fast Track Asia — инкубатор стартапов.

До Квон до Terr`ы он был основателем и генеральным директором Anyfi Inc, одноранговой телекоммуникационной компании, создающей решения для P2P-соединений с использование технологии ячеистой сети (для создания более масштабируемой, доступной и безопасной сети)

В общем, у Terra были мощные основатели с четким представлением реализации данной идеи. Но что же могло пойти не так и привести к потери почти всего капитала? [5]

ГЛАВА 2. СКАМ TERRA И ПОЯВЛЕНИЕ TERRA 2.0

2.1 Атака на Terra.

Я же хотел разобрать одну из самых популярных версий, которая показывают атаку фондов на Terra Luna. И атаки бывают не только внедрение в сеть, а еще и физического характера.

Если вдумываться и разбираться в произошедшем, то с легкостью можно понять, что атака планировалась не один день, также было не случайно выбран май 2022 года.

Некие фонды (а именно BlackRock, Citadel и Alameda — крупнейшие американские финансовые ребята) взяли в долг (даже не под проценты) у биржи Gemini 100,000 BTC и начали свою миссию по убийству Terra. Они смогли найти уязвимость в самой системе привязки монет UST и LUNA (когда для печатанья одной надо было сжигать другую по курсу 1$:1$).

Купив на 25,000 BTC токен UST (это около 1 миллиарда $), фонды решили позвонить напрямую До Квону и предложить сделку на OTC (вторичном рынке), где они хотели бы купить ОЧЕНЬ МНОГО UST, но не хотят сильно двигать рынок. До Квон же оказался очень жадным до денег и попался на удочку злоумышленников, тем самым запустив “спираль смерти” [3].

*Работа “спирали смерти”: холдеры UST начинают бояться за состояние цены LUNA, спасая свои позиции, начинают продавать свои монеты, тем самым больше провоцируя других также продать активы. А каждый UST сжигается и этим печатает еще монеты LUNA, что провоцирует падение цены основной монеты [6].

До Квон вынимает часть ликвидности для сделки, этим снижает поддержку токена UST, а наша доблестная троица атакующих сбрасывает BTC и UST по рыночной цене, обрушая цену на оба актива сразу. Из-за большего объема продаж цена на стейблкоин начала отходить от отметки в 1$.

Атаку фонды производили, базируясь уже на понимании принципов протокола Anchor, являющегося частью экосистемы Terra. Принцип же Anchor заключался в обычной финансовой пирамиде, которую можно было разрушить лишь большим оттоком средств, чем и воспользовались злоумышленники — До Квон выводит часть ликвидности, а они расшатывают оставшуюся часть монет на рынке.

А смысл атаки был в том, что у фондов была открыта позиция на понижение цены монеты (шорт), а также они хотели откупить подешевевший BTC из-за всех событий, чтобы отдать долг и жить припеваючи.

Как вы понимаете, фонды же опровергли слухи, это криптовалюта и это были не мы, просто подставили нас.

И при чем же здесь монета LUNA? Атака была же на UST! Дело в том, что LUNA являлась обеспечением UST, монетой-балансиром, поэтому из-за откреплення одной, печатается много другой, что привело к триллионам напечатанных токенов. И LUNA, цена которой доходила почти до 120$ в начале апреля, сейчас стоит около 0.0001$ [3].

2.2 Рождение Terra 2.0.

Команда Terra 2.0 не хотела, чтобы их проект, который пользовался популярностью примерно 4 года просто так погиб из-за атаки на UST и LUNA.

Они решили запустить новую монету LUNA 2.0. Данная монета уже просто продолжала свою работу без привязки к стейблкоину UST. Главной целью этого “форка” было стремление сохранить экосистему Terra с сотнями разработчиков и держателей LUNA Classic и UST Classic.

Terra удалила кошелек Terra Foundation Labs, чтобы сделать Terra полностью принадлежащим сообществу блокчейном.

А также провели раздачу новых токенов среди холдеров LUNA и UST, где выдали сразу 30% на руки участникам, а 70% оставили на разблокировку в течение 2-х лет. А в личное управление проект оставил 330 млн токенов, а комьюнити выделило 770 млн [4].

ЗАКЛЮЧЕНИЕ

Мы можем сделать вывод, что даже самые уникальные и хитрые руководители могут совершать ошибки, которые приводят к потери больших активов.

Как итог, мы имеем злоумышленников, которые смогли снизить рыночную капитализацию UST на 16,6 млрд. $, а также заработать на этой атаке минимум 1 млрд. $ прибыли. Сложно судить о потерях активов людей, потому что кто-то доверял протоколу и ждал от них большего роста, а кто-то и вовсе обходил стороной заманчивый стейкинг по 20% годовых на самих биржах [7].

Но факт остается фактом, что даже самые сильные монеты могут оказаться в такой ситуации, если у создателей есть возможность управлять активами, как это делал До Квон.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Федеральный закон от 31.07.2020 № 259-ФЗ, вступивший в силу с 01.01.2021.

2. “От золота до биткоина”. Антон Попов, Дмитрий Тарасов

3. https://alphainvestor.ru/digest-6-2022/ — статья от Блога Свободного Инвестирования.

4. https://coinmarketcap.com/ru/currencies/terra-luna-v2/ — информация по монете TerraLuna от CoinMarketCap.

5. https://1bitcoin.wiki/wiki/terra-luna-obzor-kriptovalyuty/ — обзор на экосистему от 1bitcoin.

6. https://coinpost.finance/p/spiral-smerti-dlya-terra-pochemu-upali-luna-i-ust — статья о ситуации с Terr`ой и “спирали смерти” от CoinPost.

7. https://cryptonews.net/ru/news/altcoins/6773921/ — Crypto News о ситуации с Terr`ой и UST.

Гладких Е.А., Наточий Н.М., Ананьев В.А.
Курганский государственный университет
Безопасность информационных автоматизированных систем, 2 курс
gladkih.egor@mail.ru
Человечкова А.В.
Курганский государственный университет, старший преподаватель
chelovechkova_2011@mail.ru

КВАНТОВЫЕ КРИПТОГРАФИЧЕСКИЕ ТЕХНОЛОГИИ

На сегодняшний день существует две квантовые революции. Первая квантовая революция определила путь развития физики в 20 веке. Благодаря ей появились ядерное оружие, транзисторы, лазеры, мобильная сеть и интернет. Мы проанализируем основополагающее направление второй квантовой революции – это Квантовая информатика. Она, в отличие от первой квантовой революции, разрешает задействовать свойства каждой из частиц по индивидуальности, а не групповые. Основой для появления этого направления стали квантовые феномены такие как: “кванто–запутанность”, “телепортация” и “неклонируемость” [3]. Многие компании и государства увидели перспективу в квантовых вычислениях и начали пытаться создать первый квантовый компьютер. Например, в Китае уже построена национальная лаборатория квантовой информатики и по информации ученых, Китай лидирует в этих соревнованиях. Главным преимуществом компании или государства, которые смогут создать первый квантовый компьютер в том, что такие технологии смогут взломать любую банковскую систему любого государства. То есть все шифры, которые мы используем и считаем надежными, квантовому компьютеру удастся расшифровать, а это значит, что любые государственные, военные засекреченные данные могут быть перехвачены и взломаны.

Однако существует причины, по которым мы можем пока не беспокоиться о нашей безопасности. С точки зрения нынешних технологий для того, чтобы создать квантовый компьютер потребуются десятилетия, тем более создать настолько мощный квантовый компьютер, который мог бы раскладывать самые большие числа на простые множители. На данный момент самое большое число, которое удалось получить – это около сотни, что недостаточно для взлома RSA – алгоритма ассиметричного шифрования (Rivest-Shamir-Adleman), являющегося самым распространенным в мире. RSA основан на факторизации произведения двух простых числе. Пользователь отправляет открытый ключ другому пользователю и тот с помощью него может зашифровать любое сообщение [2]. Однако расшифровать сообщение может только тот, кто изначально владел двумя простыми числами. Следовательно, алгоритмом и ключом владеет только отправитель, поэтому перехватчику потребуется раскладывать это числа на простые множители. На данный момент нет алгоритма, который бы решал эту задачу на классическом компьютере за определенное время. На то, чтобы расшифровать такое сообщение может уйти бесконечное количество времени [1].

В 1994 году был написан алгоритм Шора, который позволяет решать эту задачу на квантовом компьютере. Но все экспериментальные реализации этого алгоритма остаются на уровне демонстрации. Связано это с мощностью квантового компьютера, которая измеряется в “кубитах” [6]. Самые мощные компьютеры на данный момент имеют несколько десятков “кубитов”, а для реализации алгоритма Шора нужно в тысячу раз больше. Но, несмотря на то, что для реализации алгоритма Шора на современных компьютерах потребует несколько десятилетий, в будущем он будет представлять серьезную опасность для всех конфиденциальных данных.

Еще один фактор уязвимости распространенных методов шифрования на данный момент времени – это информация, которая хранится в течение долгого времени. Например: военная, государственная, медицинская, коммерческая тайны.

Злоумышленник может заполучить данные в виде шифра и хранить их до того момента пока не будет изобретен алгоритм, который сможет расшифровать данные за короткий промежуток времени. Либо не появиться достаточно мощный квантовый компьютер [9].

Одним из решений такой проблемы будет являться постквантовая криптография. Ее алгоритмы основаны на математических преобразованиях, инвертирование которых создает сложность для всех видов компьютеров, в том числе и квантовых. Она повышает безопасность информации, которая хранится больше 5 лет. Постквантовые алгоритмы можно считать самым надежным способом защиты, но никто не может гарантировать, что в будущем не будут созданы алгоритмы, которые найдут уязвимость [7].

Успешные испытания системы квантовой криптографической защиты на высокоскоростной линии связи были проведены в Российской Федерации в прошлом году. Она приемлемая для внедрения в больших дата–центрах. Тестами занимался квантовый центр по заказу “Газпромбанка” и “С-Терра СиЭпсПи”. Особенность заключается в том, что ключи шифрования зашифрованы в квантовых состояниях фотонов, которые передаются по обычным оптоволоконным линиям. В этом методе используется один из главных законов механики – Закон Гейзенберга. Смысл закона в том, что при попытке измерить какую-либо характеристику элементарной частицы, к примеру, скорость, приведет к тому, что изменятся импульс или спин частицы. Благодаря этому криптографический ключ может мгновенно определить, что кто-то вмешался в передачу данных, а также может перехватить и дешифровать информацию [5]. Подключиться и навредить такому соединению злоумышленник попросту не успеет, а значит, пользователи могут быть уверены в том, что информация полностью конфиденциальна и достоверна. Отправлять единичные фотоны можно по обычным оптоволоконным сетям. На длинных расстояниях потери фотонов в оптическом канале неминуемы, поэтому они передаются на менее продолжительных участках между проверенными узлами

квантовой сети. Линии связи, которые используют защиту квантовой криптографии, предоставляют совершенно новый уровень защищенности, что необходимо важно в оборонной, государственной и стратегической сферах. ОАО РЖД предложили разработать национальные стандарты квантовых коммуникаций. На данный момент уже разработаны несколько стандартов и редакций в области квантовых технологий. Благодаря стандартам можно будет перейти от изучения к реализации квантовых сетей. Это позволит получить единый подход к их характеристикам и оценкам качества. К 2024 году ОАО РЖД прогнозируют более 10000 километров квантовых сетей. Сама компания выделила на это 3,5 миллиарда рублей. Еще в возможности национальной квантовой сети входит то, что она должна уметь присоединяться к сетям за рубежом. Помимо кодирования информации такими способами можно и передавать ее. Это можно осуществить с помощью Квантовой запутанности". То есть, если пара фотонов станет "квантово запутанной", то их некоторые характеристики станут взаимозависимые, хотя они больше ничем не связаны и могут находиться на большом расстоянии друг от друга. И преимуществом такой сети станет то, что информация пользователю не будет передаваться близкой к скорости света, а мгновенно [8]. Более того в отличие от компьютеров, которые используют "биты" в качестве минимальной информации, квантовый компьютер оперирует "кубитами". Преимущество "кубита" заключается в том, что у него есть такое состояние, как суперпозиция. Она создает эффект "квантовый параллелизм", который позволяет одномоментно осуществлять обработку всех вероятных состояний, при совершении унитарных операций. Благодаря ему "кубит" превосходит бит в хранении информации и в скорости выполнения операций. Главный вопрос был в том, как принимать эти частицы [10]. Так в 19 веке Юнг провел опыт, который в дальнейшем стали использовали для приема частиц. Чтобы это сделать, нужно лазером просветить особые кристаллы, проходя через которые луч делится как минимум на два потока частиц с взаимосвязанными характеристиками [4]. Однако технологии, которые

смогут хранить и транспортировать “запутанные” фотоны не созданы нигде в мире, так что в этой сфере Российская Федерация может стать первой и сделать прорыв в сфере кибербезопасности и квантовой механики. С появлением таких сетей как минимум будет решена проблема освоения космоса, так как задержки электромагнитных и радиосигналов больше не будет, сообщения будут доходить мгновенно.

Очевидно, что после создания квантового компьютера, наиболее распространенные методы шифрования и криптографии станут уязвимыми. Для того чтобы этого избежать, предлагается новый подход, основанный на принципах квантовой физики – квантовая криптография. Многие государства и компании вкладывают огромные ресурсы в развитие этой сферы, несмотря на то, что данный метод в теории защит на практике пока довольно трудно реализовать.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Долгочук А.Д. Технологии квантовой криптографии /А.Д. Долгочук, А.Н. Поликанин // Журнал Интерэкспо Гео-Сибирь. – 2021. – С. 78-83.

2. Atsin A. Coherent-pulse implementations of quantum cryptography protocols resistant to photon number splitting attacks /Atsin A. Gisin N. Skarani V. – 2003. – 187 pp.

3. B. Djordjevic I. Physical-Layer Security and Quantum Key Distribution / Djordjevic B.I. – 2019. – 487 pp.

4. Dang B. Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation / Dang B. – 2014. – 384 pp.

5. Frazer W. Quantum Information Theory: The Future of Quantum Cryptography and Computing / Frazer W. – 2017. – 96 pp.

6. Makarov V. Quantum cryptography and quantum cryptoanalysis / Makarov V. – 2007. – 158 pp.

7. M. Parker Ph.D P. The 2020-2025 World Outlook for Quantum Cryptography / M. Parker Ph.D P. – 2019. – 300 pp.

8. Quantum Cryptography/Encryption in 2022: In-Depth Guide [Электронный ресурс]. URL: https://research.aimultiple.com/quantum-cryptography/ (Дата обращения: 15.09.2022).

9. Quantum and Physical Layer Cryptography[Электронный ресурс]. URL: https://www.nict.go.jp/en/quantum/about/crypt/english.html (дата обращения: 17.09.2022).

10. How quantum-safe cryptography will ensure a secure computing future [Электронный ресурс]. URL:https://www.weforum.org/agenda/2022/07/how-quantum-safe-cryptography-will-ensure-a-secure-computing-future/ (Дата обращения: 19.09.2022).

Кушнир Д.В.,
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, доцент, к.т.н., доцент,
dmitry.kushnir@gmail.com
Шемякин С.Н.,
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, доцент, к.т.н., доцент,
s4421764@yandex.ru

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ АУТЕНТИФИКАЦИИ В РЕАЛИЗАЦИИ КВАНТОВОГО КРИПТОГРАФИЧЕСКОГО ПРОТОКОЛА

Современные коммуникации требуют высокого уровня безопасности передачи данных, что определяется зависимостью современных технологий от надежности функционирования систем связи. Существуют различные пути достижения необходимых параметров безопасности с учетом текущих требований и учетом последних достижений в различных областях науки, в том числе в стремительно развивающихся квантовых и гибридных вычислениях [1].

Одним из способов обеспечения безопасности современных коммуникаций является сквозное шифрование данных между участниками информационного обмена с предварительным распределением ключей [2]. Задача распределения ключей остается основополагающей при построении практически любых защищенных систем. Одним из способов обеспечить конечные узлы необходимым ключевым материалом является применение построение квантовых линий связи и реализации квантовых криптографических протоколов [3].

Особенностью квантовых криптографических протоколов является потенциальная возможность обеспечения законных пользователей общего ключа, который не может быть перехвачен противником без внесения изменений в передаваемую информацию. Изменение ключевых данных может быть обнаружено

законными пользователями и быть использовано как исходный материал для доказательства наличия вмешательства в линию передачи данных и принятия решения о возможности использовать переданные данные для итогового формирования ключа или полного отказа от него.

Таким образом, данный способ распределения ключа позволяет его применить, в том числе, и для последующего совершенного шифрования, т.е. предоставив для каждого возможного варианта сообщения отдельный ключ. Это обеспечивает совершенную защиту, в том числе и от противника, обладающего неограниченными возможностями, включая доступ к произвольному квантовому компьютеру.

Помимо обмена данными по квантовому каналу для работы квантового криптографического протокола требуется провести обмен данными по открытому каналу. В ходе такого обмена, который производится после завершения передачи по квантовому каналу, стороны передают исходную информацию по выбранным базисам для кодирования фотонов при их передаче и выбранным базисам на приемной стороне с информацией о наличии в тактовых интервалах фотонов. Далее стороны выполняют один из вариантов согласования полученных по квантовому каналу набора бит, чтобы устранить возникшие ошибки и не предоставить вероятному противнику дополнительной информации об итоговом ключе. В завершение стороны проверяют данные на совпадение и выполняют усиление секретности для получения итогового ключа с необходимыми параметрами секретности (Рис. 1).

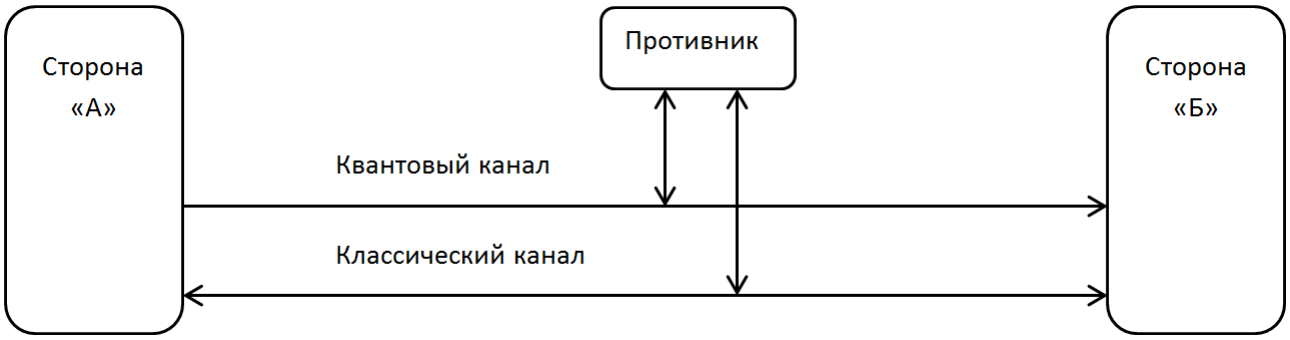


Рис. 1. Квантовый и классический канал в квантовом криптографическом протоколе

Так как успешное вмешательство в такую передачу может полностью свести на нет всю защищенность квантового протокола, то обозначенный обмен необходимо обеспечить защитой от возможности изменения со стороны противника, т.е. выполнить аутентификацию данных, которыми обмениваются законные пользователи по открытому каналу [4].

В итоге, еще до начала функционирования линии квантового распределения ключа, у законных пользователей уже должен быть в наличии некоторый набор общих секретных данных, предоставленный им на этапе инсталляции системы. Это говорит о том, что система квантового распределения ключа, скорее является системой квантового расширения ключа.

Обратим теперь внимание на такой аспект применения квантового распределения ключа, как возможность его использования для обеспечения защиты от противника с неограниченными возможностями, т.е. принимая во внимание тот факт, что данный метод предлагается как основа для построения идеально защищенного обмена. Тогда напрашивается вывод о необходимости использования идеальных методов защиты и самого процесса аутентификации или защиты процедуры обмена по открытому каналу.

Рассмотрим, как же можно обеспечить идеальную защиту при передаче данных по открытому каналу. Так как у нас уже есть предварительно

распределенные данные, то одним из возможных вариантов было бы полное шифрование всех данных, которыми дополнительно требуется обменяться. В указанном случае мы по-прежнему говорим об идеальной стойкости, что требует выполнение условий на идеальное шифрование, т.е. примерного равенства ключевых данных и объема данных в открытом канале. Для уточнения возможности такого способа защиты оценим объём необходимого обмена по открытому каналу в протоколах квантового распределения ключа. Для приближенной оценки перечислим стадии протокола, в которых требуется передача по классическому каналу. На первой стадии один из пользователей передает для каждого тактового интервала указание, какой базис использовался для кодирования двоичного значения исходной случайной последовательности. На второй стадии другой пользователь в ответ отправляет строку бит с указанием, в каких тактовых интервалах использовался тот же базис и был зафиксирован фотон. На третьей стадии пользователи должны выполнить протокол очистки от ошибок и проверки на требуемую малую вероятность оставшихся ошибок и выбора параметров для итогового усиления секретности для получения итогового ключа. Основными этапами обмена данными по классическому каналу в рамках выполнения протокола квантового распределения ключа выступают согласование базисов, чистка ошибок и итоговая выработка ключа (Рис. 2).

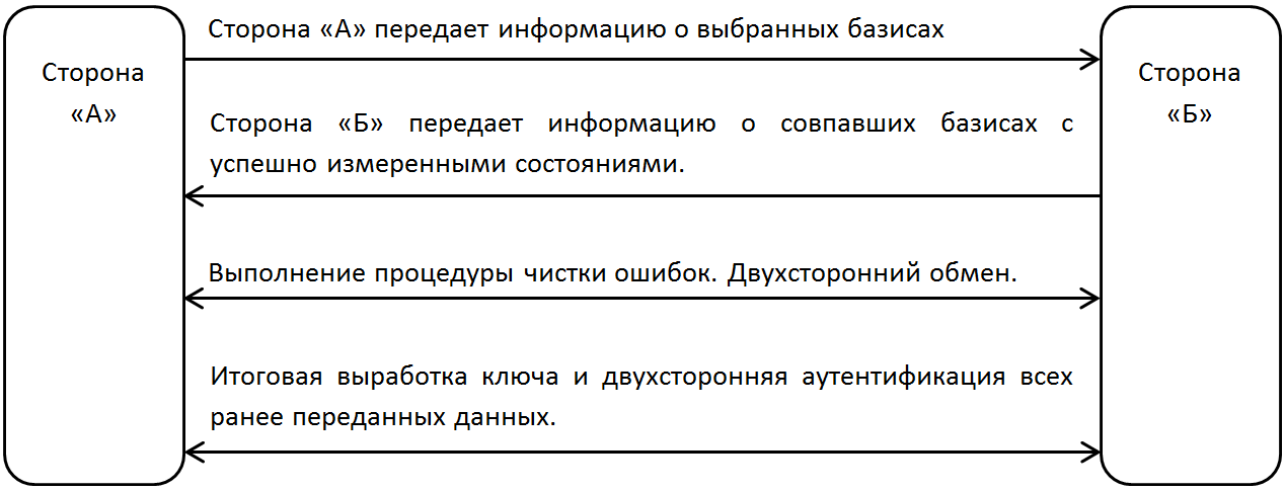


Рис. 2. Обмен данными по классическому каналу после завершения передачи по квантовому каналу

На этом этапе каждый пользователь вынужден отправить объем данных в несколько раз превышающий объём ключевых данных. В итоге мы получаем, что для распределения некоторого количества ключевых данных по квантовому каналу, мы должны задействовать количество бит заранее распределенного ключевого материала в объеме в несколько раз превышающего количество тактовых интервалов квантовой передачи, притом, что, даже если не оценивать точно сколько бит ключа можно получить из данных сырой квантовой передачи, понятно, что итоговый ключ не может превысить количество тактовых интервалов в квантовой передаче. Таким образом, для обеспечения идеальностойкой защиты обмена по классическому каналу требуется в несколько раз больший объем ключевых данных от каждого пользователя, чем тот ключ, который пользователи получат после выполнения протокола, что делает предложенное ранее идеальностойкое шифрование при обмене данными по классическому каналу в раках квантового распределения ключа бессмысленным.

С другой стороны, нам не требуется обеспечение защиты от угрозы нарушения конфиденциальности, нам нужна только аутентификация данных, передаваемых по открытому классическому каналу. Рассмотрим необходимый объем ключевых данных для обеспечения идеальностойкой аутентификации.

Наилучшую имитозащиту обеспечивают одноразовые совершенные шифры [5,6]. В классе совершенных шифров выделяют экстремальные. Для них число μ_{min} различных знаков шифртекста и количество ключей имитозащиты $\pi = \mu_{min} = \lambda^2 - \lambda + 1$ оказываются минимальными. Здесь λ - число возможных различных блоков длины n, подлежащих защите, $\lambda = 2^n$. То есть, на один бит данных требуется чуть меньше двух бит ключа.

Возможно использование почти совершенных одноразовых шифров имитозащиты [7,8]. Они требуют существенно меньшего расхода ключевого материала. Часть нового ключевого материала в ходе выполнения квантового криптографического протокола вполне может быть использована для имитозащиты открытого обмена. Характерной их особенностью является то, что они не позволяют определить открытый текст по шифртексту с вероятностью, превосходящей ε. Значение вероятности ε правильного дешифрования задаётся в качестве параметра при построении самого шифра.

В некотором смысле полученные результаты говорят о том, что мы не можем использовать совершенные методы обеспечения аутентификации. Можно ли в итоге рассуждать о возможности построения идеально защищенных систем на базе протоколов квантового распределения ключа?

В практических схемах для подтверждения подлинности данных законных пользователей используют разновидность почти совершенных шифров [9,10]. В частности, защищается результат хеширования с длиной хеша, например, 128 бит. Функция хеширования применяется по отдельности ко всему набору данных, которые передает каждый из участников в ходе протокола обмена по классическому каналу. Тогда аутентификация с заданной вероятностью защиты от навязывания и подмены может быть реализована, например, на совершенном шифре имитозащиты. Для экстремального шифра с обозначенной длиной хеша в 128 бит требуется расход ключа равный 256 бит с нижней границей вероятности навязывания $1/(2^{128})$.

В данном случае необходимо обратить внимание, что даже без вмешательства противника в открытую передачу, результирующий набор ключевых данных имеет некоторую вероятность оставшейся ошибки и, кроме того, не может гарантироваться отсутствие остаточной информации противника о результирующей строке ключевых бит. Объем остаточной информации с помощью выполнения процедуры усиления секретности можно сделать не превышающим

величину $2^{-s}/\ln 2$, где s – параметр секретности и, фактически, количество бит, забранных у формируемого ключа на последнем шаге его формирования. Кроме того, необходимо учитывать, что объем остаточной информации с некоторой, хоть и малой вероятностью, может превышать указанную величину. Конкретная вероятность определяется вероятностью успешной оценки сверху количества информации у противника и вероятностью полной очистки данных законных пользователей от ошибок.

Таким образом, хотя нет возможности использовать совершенную аутентификацию, но рекомендованные на практике подходы не ухудшают итоговые параметры секретности ключевого набора данных.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Хайретдинов, Э.И. Защита информации на предприятии методами квантовой криптографии // Э.И. Хайретдинов, Р.А. Майский Сборник: Актуальные проблемы науки и техники. – 2017. – 2017. – С. 265-268.

2. Арбеков, И. М. Критерии секретности ключа // Математические вопросы криптографии. – 2016. – Т. 7 – № 1. – С. 39–56.

3. Bennett, C. H. Experimental quantum cryptography / C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin//Journal of cryptology. – 1992. – Т. 5. – №. 1. – С. 3-28.

4. Тимофеев, А. В. О структуре открытого классического канала связи в квантовой криптографии: коррекция ошибок, целостность и аутентичность/ А.В. Тимофеев, Д.И. Помозов, А.П. Маккавеев, С.Н. Молотков//Журнал экспериментальной и теоретической физики. – 2007. – Т. 131. – №. 5. – С. 771-789.

5. Зубов, А. Ю. Криптографические методы защиты информации. Совершенные шифры: Учебное пособие / А.Ю. Зубов. – М.: Гелиос АРВ, 2005. – 192с.

6. Stinson, D. R. A construction for authentication/secrecy codes from certain combinatorial designs // Conference on the Theory and Application of Cryptographic Techniques. – Springer, Berlin, Heidelberg, 1987. – С. 355-366.

7. Зубов, А. Ю. Почти совершенные шифры и коды аутентификации //Прикладная дискретная математика. – 2011. – №. 4 (14). – С. 28-33.

8. Коржик, В. И. Основы криптографии / В.И. Коржик, В.А. Яковлев. – СПб.: Интермедия, 2016. – 312 с.

9. Ибрагимов, Б. Г. Анализ методов информационной безопасности в системах телекоммуникаций с использованием квантовой криптографии // Технические университеты: интеграция с европейскими и мировыми системами образования / Б.Г. Ибрагимов, Э.М. Джафарова. – 2019. – С. 404-410.

10. Радюкевич, М. Л. Усиление секретности криптографического ключа, сформированного с помощью синхронизируемых искусственных нейронных сетей // Информатика / М.Л. Радюкевич, В.Ф. Голиков. – 2020. – Т. 17. – №. 1. – С. 102-108.

Романов И.В.,
ПГТУ, аспирант направления «Системы автоматизации и проектирования»
ООО «ЭМБЕР», инженер-программист,
ilyarom5@gmail.com
Масленников А.Н.,
ПГТУ, студент магистратуры направления «Программная инженерия»
artyom.maslennikov@mail.ru
Сидоркина И.Г.,
профессор, д.т.н., заведующая кафедрой Информационной безопасности
Поволжского Государственного Технологического Университета
igs592000@mail.ru

УНИВЕРСАЛЬНЫЕ ПАРАМЕТРЫ ДЛЯ МОДИФИКАЦИИ МУРАВЬИНОГО АЛГОРИТМА ПРИ РЕШЕНИИ ПРОФЕССИОНАЛЬНЫХ ЗАДАЧ

Решение задач может достигаться за счет применения методов распознавания зависимостей в данных, оптимизации функции полезности в условиях неопределенности.

Одним из способов решения задач с использованием машинного обучения является реализация биоинспирированных алгоритмов **[1]**. Такие алгоритмы способны хорошо проявить себя в задачах поиска оптимальных или локально оптимальных решений. Это может быть достигнуто при интеграции новых и модифицированных версий данных алгоритмов. Этот процесс известен как «гибридизация» **[2]**.

Современные муравьиные алгоритмы имеют ряд слабых мест - например в случаях многомерных и нелинейных исходных данных точность вычисляемых значений снижается**[3**]. Предложено выполнить ряд необходимых изменений в базовых версиях алгоритмов чтобы обойти их слабые места и уязвимости. Целью данной работы является повышение эффективности муравьиного алгоритма,

устранение его слабых мест путем разработки гибридного алгоритма, реализованного на основе оценки параметров существующих биоинспирированных алгоритмов для решения задач поиска оптимальных решений в профессиональной сфере ИБ. Алгоритм предполагает использование технологии машинного обучения.

В качестве модели использована задача коммивояжера – **[4]** задача комбинаторной оптимизации. Задача относится к классу NP-сложных. При большом количестве исходных точек стандартный перебор становится неуместен ввиду её фрактальной алгоритмической сложности.

В статье для решения задач исследуется анализ эффективности муравьиного алгоритма применительно к задаче коммивояжера по различным параметрам, таким как скорость расчета и точность вычислений. Кроме этого, предложены способы гибридизации. Предложенный алгоритм способен создать предпосылки для получения наиболее точных эвристических данных. Точность данных, в свою очередь, смогут предоставить качественные выходные данные для поиска оптимального решения.

Муравьиный алгоритм.

Алгоритм основан на поведении муравьиной колонии при поиске еды **[5]**. Реализуется с использованием графов. Базируется на том, что в реальном мире муравьи, при нахождении еды прокладывают обратную дорогу с помощью феромонов. Другие муравьи обращают на это внимание и добираются до источника еды по той же феромонной тропе, укрепляя её феромонами на пути обратно. Путей до еды может быть несколько, и муравьиный алгоритм способен находить кратчайший путь. Одно из свойств феромонов - испарение. Соответственно - чем больше путь, тем слабее будет запах феромонов. Чем слабее запах феромонов - тем менее привлекательным он будет для муравьев.

В задаче коммивояжера муравей представлен как агент. Каждый агент хранит в себе список пройденных узлов. При выборе агентом следующего шага - он

отталкивается от списка узлов и выбирает возможную точку для перехода. Кроме этого, он выбирает следующий узел в зависимости от расстояния между узлами и феромонами оставленными другими агентами на ребре. Каждый шаг сопровождается оставленным феромоном на пройденном ребре. С течением времени следы феромонов испаряются а проходящие по маршруту агенты усиливают «запах» следов.

Если агент расположен в узле i, а узел j – это один из доступных для перехода весов. Обозначим вес ребра, соединяющего узлы i и j, как w_{ij}, а интенсивность феромона на нем – как t_{ij}. В таком случае вероятность перехода муравья из i в j будет равна (1.1).

$$p_{ij} = \frac{t_{ij}^{\alpha} + \frac{1}{\omega_{ij}^{\beta}}}{\sum_{l \in S_i} \left(t_{il}^{\alpha} + \frac{1}{\omega_{it}^{\beta}}\right)} \quad (1.1)$$

α и β – представляют собой регулируемые параметры при выборе пути, где α представляет собой важность составляющей веса ребра, а β- уровня феромонов.

Данный алгоритм приблизительно напоминает классический жадный алгоритм. На сегодняшний день классическая реализация муравьиного алгоритма допускает множество вариантов оптимизации, которые способны повысить его эффективность в зависимости от требований, которые накладываются на задачу **[6]**.

Модификации муравьиного алгоритма

К примеру – существует известная модификация путем добавления «элитной системы» для повышения эффективности поиска коротких путей. **[7]** В данных системах муравьи с более успешной историей достижений помечаются как «элитные». Понятие «элитный муравей» в данном контексте означает его свойство оставлять больше феромонов чем другие.

Также, существуют «колониальные» системы которые повышают уровень феромонов на кратчайших ребрах позволяющее эффективно вычислять кратчайший путь.

Известная модификация – алгоритм MinMax **[8]** схож с элитарной системой, которому свойственно отдавать предпочтения «высоко рейтинговым решениям». Его суть заключается не только в присваивании дополнительных феромонов элитарным решениям, но и разрешает оставлять феромонный след лишь самым работоспособным единицам, которые соответствуют наилучшему глобальному решению. Подобная доработка видоизменяет область потенциальных решений таким образом, что с повышением количества итераций область оптимальных решений становится все уже. Это достигается за счет того, что количество «элитных» муравьев снижается с течением времени.

Основные недостатки классического алгоритма связаны с неэффективным использованием истории поиска, кроме этого можно добиться заметных результатов если использовать более тщательный анализ областей вокруг уже найденных удачных решений.

Классический муравьиный алгоритм способен показывать эффективный результат на большом числе вершин по сравнению с другими классическими алгоритмами. Однако так или иначе вычисления требуют значительного количества времени и вычисляют лишь приблизительный результат. В рамках данной статьи предлагается увеличить скорость и эффективность алгоритма путем модификации алгоритма путем добавления исключающих соединений. Это достигается путем наложения штрафов на неоптимальные соединения. Таким образом получится сократить количество ребер в исходном графе, что в свою очередь позволит быстрее найти оптимальный путь. Данный подход можно реализовать с помощью интеграции алгоритма машинного обучения, базирующегося на методе «Имитации ожога».

Одна из сложностей данной модификации - оптимальный выбор точки остановки отжига и старт муравьиного алгоритма.

Проверим классический муравьиный алгоритм на заданном наборе данных:

Был произведен обход с помощью классического муравьиного алгоритма для 20 вершин. Обнаружено что обход выполняется примерно за треть секунды 0.28. Количество вершин и соответственно время выполнения относительно небольшое, однако если увеличить число вершин до 300 - потребуется порядка нескольких минут.

Были использованы следующие параметры:

- Коэффициент испарения равен 0.6;
- Коэффициент составляющей важность веса ребра α = 1;
- Коэффициент составляющей важности уровня феромонов β = 2;
- Количество муравьев менялось в зависимости от итераций. Для 20 вершин достаточно порядка 10 муравьев, для 300 требовалось увеличить количество до 100;
- Количество итераций квадратично количеству вершин а равно N^2

Модификация заключается в следующем - создадим N^2 нейронов. Расстояния dxy между парами городов известны. Состояние нейронов описывается как ω_{Xi} где x - город а i - позиция города в маршруте. Для решения задачи коммивояжера применяется функция энергии **[9]**. Состояние с наименьшей энергией соответствует самому короткому маршруту.

На функцию энергии накладывается ряд требований:

Функция должна поддерживать устойчивое состояние: $V = \{\omega_{Xi}\}$

- из всех решений первого пункта функция энергии должна выбирать короткие маршруты. В таком случае функция энергии будет выглядеть следующим образом (где, первы*е* три члена поддерживают пункт номер 1, четвертый - 2) (1.2)

$$E = \left(\frac{A}{2}\right)\sum_X \sum_i \sum_{j \neq i} \omega_{Xi}\omega_{Xj} + \left(\frac{B}{2}\right)\sum_i \sum_X \sum_{Y \neq X} \omega_{Xi}\omega_{Xj} +$$

$$\left(\frac{C}{2}\right)\left(\sum_X \sum_i \omega_{Xi} - n\right)^2 + \left(\frac{D}{2}\right)\sum_i \sum_X \sum_{X \neq Y} \sum_i d_{XY}\omega_{Xi}(\omega_{Y,i+1} + \omega_{Y,i+1}) \quad (1.2)$$

Исходя из выражения можно сделать ряд выводов:

1. Первый член будет равен нулю, если каждая строка X содержит не более одной единицы;
2. Второй член равен нулю, если каждый столбец i содержит не более одной единицы;
3. Третий член равен нулю, если в матрице n единиц;
4. Короткие маршруты поддерживает четвертый член. В нем индексы i берутся по модулю n для того, чтобы показать, что n -й город соседствует в маршруте с (n-1)-\mbox, т.е. v_{Y,n+j}=v_{Y,j};
5. Четвертый член численно равен длине маршрута.

Функция вычислительной энергии выглядит следующим образом (1.3)

$$E = -\left(\frac{1}{2}\right)\sum_X \sum_i \sum_Y \sum_j W_{Xi,Yj}\omega_{Xi}\omega_{Xj} - \sum_{xi} I_{Xi}\,\omega_{Xi} \quad (1.3)$$

И веса сети Хопфилда (1.4)

$$W_{Xi,Yj} = -A\delta_{XY}\left(1 - \delta_{ij}\right) - B\delta_{ij}(1 - \delta_{XY}) - C - Dd_{XY}\left(\delta_{j,i+1} + \delta_{j,i-1}\right), I_{Xi} = C_n \quad (1.4)$$

Где δ - индексатор равенства элементов (символ Кронекера)

Такое решение позволит найти маршруты, чуть лучше, чем случайные. Следующим этапом целесообразно пометить маршруты как наиболее

предпочтительные. Этого можно достичь путем увеличения числа феромонов или уменьшения коэффициента испарения на них.

Найденное решение не имеет смысла на небольшом количестве вершин, т.к. затраты на выделение памяти и поиск неоптимальных путей будет излишним и потребует больше итераций и времени. Сеть Хопфилда была запущена 1 раз.

Анализируя эффективность найденного решения, были сделаны следующие выводы:

- При большом количестве вершин и ребер предварительный отжиг действительно дает ускорение поиска приближенного решения примерно на 10-20%;
- При повышении количества вершин и ребер эффективность сохраняется. Точность решения повышается за счет отжига неоптимальных путей. Однако были замечены кейсы когда производился отжиг ребер, которые являлись частью оптимального пути;
- Показатели точности увеличиваются несущественно, примерно на 5-10%.

Такое решение, а также упомянутые способы повышения эффективности муравьиного алгоритма - имеют место в решении задач коммивояжера **[10]**, а следовательно и в задачах поиска оптимальных решений универсального характера при решении профессиональных задач в области [11] ИБ. Однако, приведенный способ имеет существенный недостаток - в сравнении с классическим алгоритмом данное решение требует больше памяти. В задачах поиска оптимальных решений наибольшую ценность имеет критерий точности, который в рамках данного решения улучшился лишь незначительно. Стоит заметить, что даже незначительные улучшения могут сильно повлиять на точность алгоритма при наличии особо большого дерева потенциальных решений.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Colin Richard Reeves, Genetic Algorithms. 2010; (1)
2. Остроух Е.Н., Требухин А.В., Чернышев Ю.А., Панасенко П.А., Разработка и анализ гибридного алгоритма решения нелинейных задач оптимизации., 2018; (2)
3. Монахов О.Г., Гибридные биоинспирированные алгоритмы для оптимизационных задач в финансовой математике., 2014; (3)
4. Dr. Leena Jain, Mr. Amit Bhanot., Traveling Salesman Problem: A Case Study. Dr. Leena Jain, Mr. Amit Bhanot., 2014; (4)
5. Штовба С. Д., Муравьиные алгоритмы, 2003; (5)
6. Yuan Sun, Sheng Wang, Yunzhuang Shen, Xiaodong Li., Boosting Ant Colony Optimization via Solution Prediction and Machine Learning., 2015; (6)
7. Marco Dorigo, Thomas Stu¨tzle, Ant Colony Optimization, 2004; (7)
8. A Pheromone Trails Model for MAX-MIN Ant System., Nikola Ivkovic, M. Golub, Mirko Maleković 2011; (8)
9. Solving optimization problems using Hopfield neural network. Hassanin Hatem, Mohamed Abdel Maksoud 2015; (9)
10. Товстик Т.М., Жукова Е.В., Алгоритм приближенного решения задачи коммивояжера., 2013; (10)
11. Фомин Е.В., Масленников А.Н., Сидоркина И.Г., Разработка метода кластеризации угроз банка данных ФСТЭК по объекту воздействия., 2021

НАУЧНАЯ СЕКЦИЯ
«Безопасность телекоммуникационных систем»

Руководитель: **Перфилов Олег Юрьевич**,
Московский технический университет связи и информатики, доктор технических наук, старший научный сотрудник, профессор кафедры «Безопасность радиосвязи»

Секретарь: **Буряков Виктор Михайлович**,
Московский технический университет связи и информатики, аспирант

Алейников А.В.,
ЮРГПУ(НПИ) им.М.И. Платова,
информационная безопасность, 6 курс, специалитет,
Загорулько А.Ф.,
ЮРГПУ(НПИ) им.М.И. Платова
информационная безопасность, 1 курс, магистратура
Сухоносов Ф.А.,
ЮРГПУ(НПИ) им.М.И. Платова,
доцент кафедры информационная безопасность

АНАЛИЗ СОВРЕМЕННЫХ СИСТЕМ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ

Суть проблемы данной статьи сводится к выработке понимания того, как работает современные системы обнаружения и предотвращения вторжений.

Ключевые слова: система обнаружения вторжений (СОВ), система предотвращения вторжений (СПВ), уязвимость, сетевая атака.

Целью данной статьи является рассмотрение структуры современных систем обнаружения вторжений, анализ используемых методов и моделей в системах обнаружения и предотвращения вторжений.

Сетевая атака - это преднамеренное действие третьих лиц, направленное на получение контроля над локальным или удаленным компьютером или компьютерной системой. В результате атак злоумышленники могут нарушить работу сети, изменить права учетной записи, зарезервировать персональные данные пользователей и реализовать другие цели.

Для предотвращения подобных атак актуальной задачей становится обнаружение попытки осуществления сетевой атаки. Класс программ, предназначенных для выполнения этой задачи является система обнаружения и предотвращения вторжений.

IDS (Intrusion Detection System) и IPS (Intrusion Prevention System) это программные и аппаратные инструменты для защиты сетей от несанкционированного доступа, являющимися важными элементами любого плана сетевой безопасности. В их основные функции входят обнаружение и предотвращения фактов вторжения, оповещая ответственных специалистов.

Классификация IDS

Рассмотрим две классификации, которые важны при выборе того или иного решения.

По виду анализируемого трафика IDS:

- основанные на протоколе (PIDS);
- основанные на прикладных протоколах (APIDS).

IDS основанная на протоколе (PIDS) производит мониторинг коммуникационных протоколов, используемых компьютерной системой.

Второй вид IDS основан на прикладных протоколах (APIDS), данный вид IDS проводит мониторинг и анализ на конкретном прикладном протоколе или протоколах, используемых вычислительной системой.

От места расположения в сети IDS делят на:

- Network Intrusion Detection System (NIDS);
- Host-based Intrusion Detection System (HIDS).

Сетевые системы обнаружения вторжения (NIDS).

Технология NIDS отслеживает данные из сетевого трафика, анализируя входящий/исходящий трафик всех устройств сети, также данные с одного или нескольких хост-компьютеров для обнаружения вторжений. IDS на основе сети проверяет заголовки пакетов, которые обычно не видны IDS на основе хоста. Это позволяет обнаруживать атаки типа "Отказ в обслуживании" (DoS) и другие типы атак, которые могут не обнаруживаться IDS на основе хоста.

Системы обнаружения вторжений на основе хоста (HIDS).

IDS на основе хоста - это система, в которой программное обеспечение устанавливается на один хост внутри сети. Система HIDS работает по принципу создания снапшотов файлов: делает снимок текущей версии и сравнивает его с предыдущей, тем самым выявляя возможные угрозы. Система на базе хоста обычно проверяет файлы журналов на компьютере для поиска сигнатур атак. Важные системные файлы и исполняемые файлы также могут периодически проверяться на предмет непредвиденных изменений. Хост-система также будет отслеживать порты и вызывать оповещение при доступе к определенным портам. Данный тип IDS эффективней NIDS в том случае, если надо защитить один конкретный компьютер.

Виды IDS по принципу действия

Все системы обнаружения вторжений IDS работают по принципу – поиск угроз путем анализа трафика. Отличия кроются в самом процессе анализа. Существует три основных вида: сигнатурные (обнаружение злоупотреблений), основанные на аномалиях и основанные на правилах.

Сигнатурные IDS.

IDS этой разновидности работают по схожему с антивирусным программным обеспечением принципу. IDS ищет трафик и поведение, соответствующие шаблонам известных атак. Эффективность зависит от базы данных сигнатур, которую необходимо обновлять. Система ищет в реальном трафике и поведении приложений паттерны, которые есть в базе. Подавляющее количество современных систем используют этот подход. Главный плюс данного метода, после срабатывание сигнатуры на трафик, мы можем взглянуть на ее текст, обратиться к логам системы, базе сигнатур и разобраться, что конкретно произошло. Главная проблема с сопоставлением шаблонов заключается в том, что она не может перехватить новые атаки, для которых программное обеспечение не имеет определенной сигнатуры в своей базе данных.

IDS, основанные на аномалиях.

Обнаружение на основе аномалий отслеживает отклонения от обычных моделей использования. Для этого сначала требуется установить базовый профиль, чтобы определить, что является нормой, а затем отслеживать действия, которые выходят за рамки этих нормальных параметров. Это позволяет обнаруживать новые вторжения или атаки, которые еще не имеют известной сигнатуры. Система анализирует работу сети на данный момент, сравнивает с аналогичным периодом и выявляет аномалии.

IDS, основанные на правилах. Данные IDS использует программирование на основе правил «ЕСЛИ *ситуация* ТОГДА *действие*». Данный тип IDS, основан на правилах. В данном случае знания – это правила, а анализируемые данные можно назвать фактами, к которым применяются правила.

Отличие IPS/IDS от межсетевых экранов

Некоторые организации зависят от своих брандмауэров для IDS / IDP, и крупные поставщики брандмауэров встраивают в свои продукты некоторые функции обнаружения и предотвращения вторжений. Однако выделенное устройство IDS / IDP может обнаруживать гораздо более широкий спектр вредоносных действий, чем те, которые встроены в большинство брандмауэров.

Основная функция брандмауэра - контроль доступа на сетевом уровне. Брандмауэр сообщает вам, какие компьютеры могут получить доступ к сетевым разделам на основе определенного набора разрешенных правил. То есть пропустить некоторый трафик, запретить остальное. В свою очередь, IPS/IDS работает наоборот - блокирует проблему безопасности (например, пакет), пропускает все остальное (если нет причин подозревать вторжение).

Помимо вышесказанного есть и технические отличия. Брандмауэры хорошо работают на 2-4 уровнях модели OSI. Для приемлемой работы на более высоких уровнях у них мало встроенного функционала. Таким образом брандмауэры в

основном анализирует только параметры сессии: состояние соединение, номера портов, IP. Системы IPS и IDS позволяют работать на более высоких уровнях, анализируя не только заголовки и их небольшие фрагменты, но и содержимое пакетов. А если есть возможность распаковать пакет, то можно проверить передаваемые данные на предмет негативного поведения.

Перспективы развития систем обнаружения и предотвращения вторжений

Не смотря возраст данной технологии она постоянно развивается и можно выделить следующие наиболее актуальные тенденции развития систем обнаружения вторжений.

На уровне обнаружения вторжений. С одной стороны, это расширение спектра поддерживаемых прикладных протоколов, особенно с учетом развития индустрии IP-телефонии, технологии VoIP и растущей популярности сервиса Video-On-demand, практически повсеместного использования систем мгновенного обмена сообщениями и т.п. Во-вторых, добавление поддержки мобильных устройств и механизмов анализа взаимодействия с мобильными устройствами. В-третьих, более глубокое изучение алгоритмов функционирования уже поддерживаемых прикладных протоколов, включая механизмы контроля состояния сеанса; как следствие; повышение гибкости определения факта вторжения. И, в-четвертых, использование систем предотвращения вторжений для предотвращения утечки конфиденциальной информации из организации по различным каналам.

На функциональном уровне. С одной стороны, это добавление функций профилирования трафика и внедрение механизмов обеспечения качества обслуживания на уровне систем предотвращения вторжений. Второе - это расширение централизованного управления системами предотвращения вторжений. В-третьих, разработка средств преобразования элементарных событий безопасности в "макро" события, удобные для оператора.

На уровне инфраструктуры IPS. Здесь возможны два момента. Во-первых, улучшенная интеграция систем предотвращения вторжений хоста и сети для

повышения точности обнаружения вторжений. И, во-вторых, улучшение возможностей для интеграции продуктов разных производителей, унификация форматов передачи данных и управляющих воздействий.

С развитием систем предотвращения вторжений их возможности по анализу взаимодействия с определенными прикладными протоколами будут увеличиваться. В то же время повышается гибкость описания термина "вторжение", что дает большие возможности для настройки решения под конкретную среду.

Таким образом в ходе написания статьи были проанализированы современные системы обнаружения и предотвращения вторжений. Был проведен сравнительный анализ методов обнаружения и предотвращения вторжений. Исследованы перспективы роста и развития данной технологии. В ходе анализа методов СОВ можно сделать вывод, что наиболее надежным является сигнатурный метод ввиду низкого уровня ложных срабатываний.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. 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;

2. Об информации, информационных технологиях и о защите информации: Федеральный закон № 149-ФЗ от 27 июля 2006 года :принят Государственной Думой 8 июня 2006 года // Одобрен Советом Федерации 14 июля 2006 года. - 2006;

3. Городецкий В.И., Котенко И.В., Карсаев О. В., Хабаров А.В. Многоагентные технологии комплексной защиты информации в телекоммуникационных системах. ISINAS – 2000. Труды. – СПб., 2000.

4. J. Allen, A. Christie, W. Fithen, J. McHuge, J. Pickel, E. Stoner, State of Practice of intrusion detection technologies // Technical Report CMU/SEI-99-TR-028. Carnegie Mellon Software Engineering Institute. 2000,

5. D. Denning, An Intrusion Detection Model. // IEEE Transactions on Software Engineering, v. SE-13, № I, 1987, pp. 222-232,

6. H. Debar, M. Becker,D. Siboni. A neural network component for intrusion detection systems // In proceeding of the 1992 IEEE Computer Society Symposium on Research in Security and Privacy, pages 240 – 250, Oakland, CA, USA, May 1992.

7. K. Cheng. An Inductive engine for the Acquisition of temporal knowledge. // Ph. D. Thesis, Department of computer science, university of Illinois at Urbana-Champain 1988.

8. Бирюков А.А. Информационная безопасность: защита и нападение. – М.: ДМК, 2017. – 434 с.

9. Платонов В. Программно-аппаратные средства защиты информации. М.: Академия, 2013. – 336 с.

10. Технологии обнаружения атак [Электронный ресурс]. URL: http://ypn.ru/448/intrusion-detection-technologies (дата обращения: 18.12.19)

Сухоносов Ф.А.,
Доцент кафедры Информационная безопасность,
Басак В.В.,
Студент кафедры Информационная безопасность

СОВЕРШЕНСТВОВАНИЕ МЕТОДИКИ ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПРОВЕРКЕ ТЕЛЕКОММУНИКАЦИОННЫХ ПРЕДПРИЯТИЙ И ВЕДОМСТВ «УПРАВЛЕНИЯ ПЕРСОНАЛОМ»

Суть проблемы данной статьи сводится к совершенствованию методики проведения аудита информационной безопасности (ИБ) при проверке телекоммуникационных предприятий и ведомств «Управления персоналом».

Аудит - форма независимого, нейтрального контроля какого-либо направления деятельности коммерческого предприятия, широко используемая в практике рыночной экономики, особенно в сфере бухгалтерского учета. Не менее важным с точки зрения общего развития предприятия является его аудит безопасности, который включает анализ рисков, связанных с возможностью осуществления угроз безопасности, особенно в отношении информационных ресурсов, оценку текущего уровня защищенности информационных систем (ИС), локализацию узких мест в системе их защиты, оценку соответствия ИС существующим стандартам в области информационной безопасности и выработку рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС.

В современных условиях, когда информационные системы пронизывают все сферы деятельности предприятия, а с учетом необходимости их связи с Интернетом они оказываются открытыми для реализации внутренних и внешних угроз, проблема информационной безопасности становится не менее важной, чем экономическая или физическая безопасность.

Объектом исследования являются процессы аудита информационной безопасности ведомств «Управления персоналом».

Предметом исследования являются методы совершенствования внутреннего аудита информационной безопасности контрольной среды подпроцесса «Формирование кадровой политики».

Решаемые задачи для достижения поставленных целей:

1. Анализируется модель построения системы информационной безопасности (ИБ), учитывающая угрозы, уязвимости, риски и принимаемые для их снижения или предотвращения контрмеры;

2. Рассматриваются методы анализа и управления рисками;

3. Излагаются базовые понятия аудита безопасности и дается характеристика целей его проведения;

4. Изучаются основные международные и российские стандарты, используемые при проведении аудита ИБ;

5. Показываются возможности использования программных средств для проведения аудита ИБ;

6. Даются практические рекомендации по проведению аудита ИБ на предприятии.

Рассмотрен термин контрольной среды организации и его роль в системе внутреннего контроля. Введено понятие аудита информационной безопасности системы внутреннего контроля организации. Проанализированы существующие методики и подходы к аудиту, проведён поиск путей оптимизации аудита ИБ и предложен способ повышения эффективности данного вида аудита с помощью проведения аудита контрольной среды бизнес-процесса. Рассмотрены существующие методики оценки эффективности контрольной среды, предложена технология аудита контрольной среды организации.

На стадии планирования аудита контрольной среды бизнес-процесса в соответствии с предложенной технологией оценки «Формирование кадровой

политики» разработана методика количественной оценки рисков анализируемого процесса.

Оценка контрольной среды бизнес-процесса «Формирование кадровой политики», включает в себя формулировку рекомендации по повышению эффективности контрольной среды рассматриваемого процесса, а также аудита системы внутреннего контроля бизнес-процессов в целом.

В данной статье для построения модели оценки риска «Формирования кадровой политики» будут применены эвристические методы такие, как морфологический анализ, метод анализа иерархий, ранжирование и тестирование.

Научная новизна работы:

1. Обоснование необходимости совершенствования существующих подходов к аудиту контрольной среды организации;
2. Постановка проблемы необходимости поиска путей оптимизации и повышения эффективности аудитов системы внутреннего контроля бизнес-процессов компании;
3. Разработка технологии аудита контрольной среды, позволяющей ранжировать аудиторские проекты ИБ по степени их важности и влияния на достижение целей компании;
4. Разработка модели количественной оценки рисков бизнес-процесса «Управление персоналом» (подпроцесса «Формирование кадровой политики»);
5. Предоставление рекомендаций по повышению эффективности аудитов ИБ.

Представленный материал может быть полезен руководителям и сотрудникам служб безопасности и служб защиты информации предприятия для подготовки и проведения внутреннего и обоснования необходимости внешнего аудита информационной безопасности.

Разработанные методики совершенствования процедуры проведения аудита ИБ при проверке телекоммуникационных предприятий ведомства «Управления персоналом» в дальнейшем могут быть успешно использованы с целью внедрения в будущие методики аудита, проводимые на предприятии.

Таким образом, в ходе написания научной статьи по теме: Совершенствование методики проведения аудита информационной безопасности при проверке телекоммуникационных предприятий ведомств «Управления персоналом» нам удалось выявить ряд нюансов и недостатков при проведении процедуры аудита информационной безопасности. Основные выводы, которые можно извлечь из работы, заключаются в том, что в целях достижения эффективности внутреннего аудита и поиска реальных областей для улучшения процессов правильнее вначале оценить основу процесса, то есть его контрольную среду. Результаты, которые могут быть получены от данного аудита, намного облегчат работу аудиторов путем существенного сужения перечня объектов аудита.

Таким образом, в результате проведено разграничение объектов аудита системы внутреннего контроля в зависимости от оценки эффективности контрольной среды бизнес-процесса и величины его риска. Подобная классификация:

- с одной стороны, позволяет руководству организации иметь представление о состоянии контрольной среды бизнес-процессов, делать определенные выводы и принимать на их основе управленческие решения;
- с другой стороны, предоставляет аудиторам возможность оптимального использования своих ограниченных ресурсов и достижения эффективности аудитов путем выбора того бизнес-процесса, система внутреннего контроля которого с наибольшей вероятностью будет неэффективна.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

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

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

3. Вострецова, Е.В. Основы информационной безопасности: учебное пособие для студентов вузов / Е.В. Вострецова.— Екатеринбург : Изд-во Урал.ун-та, 2019.— ISBN 978-5-7996-2677-8.- 204 с.;

4. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. — М.: ГЛТ, 2016. — 280 с.;

5. Родичев Ю. А. Информационная безопасность. Национальные стандарты Российской Федерации / Ю. А. Родичев — «Питер», 2019 — (Учебник для вузов (Питер)) ISBN978-5-4461-1275-3. - 304 с.;

6. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. — М.: ДМК, 2017. — 702 с.;

7. Ярочкин, В.И. Информационная безопасность: Учебник для вузов / В.И. Ярочкин. — М.: Акад. Проект, 2018. — 544 с.;

8. Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации : Рекомендации по стандартизации. - введ. 2006-01-01. - М. : Изд-во стандартов, 2005. - 13 с.

9. Р 50.1.056-2005. Техническая защита информации. Основные термины и определения : Рекомендации по стандартизации. - Введ. 2006-06-01. - М. : Изд-во стандартов, 2005. - 20 с.

10. Оформление работ: Госстандарт России. - Москва «Издательство стандартов», введ. 2000 г., - с. 43.;

Бобрешов А.Ю.,
ЮРГПУ(НПИ) имени М. И. Платова, студент, информационная безопасность,
группа 100502-ЗИСа-о17,
mosesrosen@outlook.com
Научный руководитель:
Лобов Н.Б.,
ЮРГПУ(НПИ) имени М. И. Платова, профессор кафедры ИБ, д.т.н.,
blobov@yandex.ru

МЕТОДИКА СОВЕРШЕНСТВОВАНИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ WI-FI СЕТЕЙ

Суть проблемы данной научной работы состоит в разработке методик по совершенствованию системы обеспечения безопасности Wi-Fi сетей.

Такая технология беспроводной сети, как “Wi-Fi”, является самой распространенной беспроводной технологией в любых сферах, где используется интернет-соединение. Этим объясняется актуальность исследования данной темы.

Цель исследования – решение задач по совершенствованию системы обеспечения безопасности Wi-Fi сетей.

Задачи по совершенствованию:

1. Рассмотрение систем защищенности беспроводных сетей.
2. Анализ уязвимостей рассматриваемой или рассматриваемых сетей
3. Разработка методических рекомендаций по улучшению защиты

Объект нашего исследования – Wi-Fi сети, в которых требуется улучшить систему защиты

Предмет исследования – непосредственно протоколы. стандарты и механизмы защиты, которые обеспечивают безопасность беспроводной сети

Результатом работы является детальное изучение системы обеспечения безопасности беспроводных сетей и создание перечня рекомендаций по ее улучшению.

Беспроводная локальная сеть (LAN) получила широкое признание в качестве жизнеспособного экономически эффективного решения общего назначения для обеспечения высокоскоростного доступа к информации в режиме реального времени. С помощью беспроводной сети пользователи могут получить доступ к общей информации, не привязываясь к фиксированной точке подключения. Беспроводные сети передают и принимают данные по воздуху и, таким образом, в совокупности сочетают возможность передачи данных с простотой мобильности. Это радиочастотная передача данных. WLAN обеспечивает беспроводной доступ к предприятиям с несколькими местоположениями, малым и средним предприятиям. Он может заменить проводную локальную сеть или просто использоваться в качестве расширения проводная инфраструктура, поэтому беспроводные сети продолжают набирать обороты на рынке. Помимо всех этих преимуществ, беспроводные сети также сталкиваются с серьезными проблемами безопасности. Таким образом, безопасность - это тот аспект, в котором работает большинство исследователей. В этом мы обсуждаем основные вызовы безопасности, проблемы, атаки и решения этих проблем и цели этого исследования. В дополнение к удобству и экономическим преимуществам по сравнению с традиционными проводными сетями некоторые из преимуществ включают масштабируемость, мобильность, простоту, снижение затрат и скорость установки. Поэтому необходимо обеспечить безопасность WLAN, равную проводной локальной сети.

В первую очередь важно выявить проблемы беспроводной сети, главными из которых являются:

1.Точки доступа для мошенников:

Неизвестные и неуправляемые устройства внутри сети станут главными уязвимостями, это также обеспечивает простые маршруты для вредоносных программ, которые должны войти, и информацию, чтобы покинуть сеть. Первое, что нужно сделать, чтобы противостоять этой проблеме, — это ввести запретные зоны беспроводной связи, гарантируя, что точки доступа не появятся там, где они не разрешены.

2. Неправильная конфигурация:

Неправильная настройка коммутаторов и точек доступа, которая по-прежнему представляет собой огромную проблему, поскольку Wi-Fi — новая технология, и ее администраторы имеют гораздо меньше опыта, чем проводные сети.

3. Неуправляемое использование беспроводной связи вне предприятия:

Большое количество сотрудников становятся зависимыми от мобильных устройств, используя устройства в открытых сетях и за их пределами. что может оставить их в уязвимом или вредоносном трафике.

4. Хакеры:

Активные атаки, проводимые с помощью беспроводных соединений, представляют собой очень большую растущую проблему, поскольку мобильные и беспроводные вычисления действительно представляют собой привлекательные цели для хакеров. когда устройство становится достаточно мощным и если содержащаяся в нем информация становится достаточно ценной.

Также следует указать основные стандартные меры по защите информации в Wi-Fi сетях. К стандартным мерам защиты относятся программные и аппаратные средства, предназначенные для решения следующих задач:

1) Предотвращение несанкционированного подключения к беспроводной сети пользователей;

2)Предотвращение доступа к запрещенным ресурсам уже подключившихся пользователей;

3)В случае уже произошедшего доступа, выполнить меры по сбору информации для предотвращения следующего инцидента доступа.

Как правило, в большинстве случаев выполняются следующие стандартные меры по повышению уровня защиты беспроводной сети :

1) Замена ключей доступа на более комплексные;

2)Смена протоколов шифрования на более современные и устойчивые к взлому методом перебора;

3)Установка программного обеспечения для протоколирования доступа пользователей к ресурсам внутри сети. Отдельными средствами являются меры, направленные на противодействие социальным методам взлома, таким, как доступ легальными техническими мерами с нелегальными целями, или подменой лица доступа из-за удаленности терминала. В общем случае, противодействие таким методам не является задачей технических мероприятий, однако, предлагаемая система аппаратно-программной защиты несколько снижает вероятность взлома за счет «обезличенности» мер защиты и независимости от линейного персонала, обеспечивающего безопасность сети.

Природа беспроводной связи создает три основные угрозы: перехват, изменение и нарушение. Ниже приведены некоторые решения безопасности для преодоления вышеупомянутых атак и угроз безопасности. 5.1 Защита беспроводной сети. Если мы сможем защитить беспроводные сети, то вероятность угроз безопасности и атак может снизиться. Ниже приведены некоторые идеи для защиты вашей беспроводной сети. 1) Использование технологии брандмауэра. Компьютер в беспроводной сети нуждается в некоторой защите, как и любой компьютер, подключенный к Интернету. Если ваш брандмауэр был поставлен в выключенном состоянии, включите его.

2) Использование технологии шифрования и дешифрования. Одним из наиболее эффективных способов защиты беспроводной сети является использование технологии шифрования и дешифрования. Большинство

беспроводных устройств имеют встроенный механизм шифрования и дешифрования.

Таким образом, в данной статье приводятся только нахождение проблем в беспроводных сетях и рекомендации методики совершенствования системы обеспечения безопасности Wi-Fi сетей

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

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. Родичев Ю. А. Информационная безопасность. Национальные стандарты Российской Федерации / Ю. А. Родичев — «Питер», 2019 — (Учебник для вузов (Питер)) ISBN978-5-4461-1275-3. - 304 с.;

5. Вострецова, Е.В. Основы информационной безопасности: учебное пособие для студентов вузов / Е.В. Вострецова.— Екатеринбург : Изд-во Урал.ун-та, 2019.— ISBN 978-5-7996-2677-8.- 204 с.;

6. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.1 — Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г Милославская. — М.: ГЛТ, 2017. — 536 с.;

7. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 — Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. — М.: ГЛТ, 2018. — 558 с.;

8. Малюк, А.А. Информационная безопасность: концептуальные иметодологические основы защиты информации / А.А. Малюк. — М.: ГЛТ, 2016. — 280 с.;

9. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. — М.: Гелиос АРВ, 2017. — 336 с.;

10. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. — М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2017. — 416 с.;

11. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. — М.: ДМК, 2017. — 702 с.;

12. Ярочкин, В.И. Информационная безопасность: Учебник для вузов / В.И. Ярочкин. — М.: Акад. Проект, 2018. — 544 с.;

Данилова Ю.С.

Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, 10.04.01 - Информационная безопасность, 2 курс, danilovajulia123@gmail.com

Научный руководитель:

Штеренберг С.И.,

Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики», доцент кафедры ИБ, к.т.н., shterenberg.stanislaw@yandex.ru

АНАЛИЗ ЭФФЕКТИВНОСТИ ВЫЯВЛЕНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПОМОЩЬЮ SIEM MAXPATROL

В России в последние годы резко возросло количество преднамеренных вмешательств в работу информационных систем государственных и коммерческих организаций. Согласно статистическому отчету PositiveTechnologies [1] «Актуальные киберугрозы: II квартал 2022 года» чаще всего атакам подвергались государственные учреждения. Главным образом действия злоумышленников приводили к утечкам конфиденциальной информации и нарушению деятельности госучреждений. Отмечается возросшая активность шифровальщиков: почти треть атак всего квартала была совершена с использованием программ-вымогателей, а доля использования шифровальщиков среди остального ВПО составила 62%, что схоже со значениями конца 2021 года. Группировки внедряют новые способы давления на жертв, дополняют вредоносное ПО новыми функциями и даже запускают программы bug bounty.

Практически во всех случаях, после осуществления кибератак, работа организаций была заблокирована от нескольких часов до нескольких дней, что

влечет большие потери, как финансовые, так и репутационные. Поэтому от степени безопасности используемых информационных технологий сейчас зависят не только стабильность и надёжность функционирования государственных институтов и коммерческих организаций, но зачастую и жизнь многих людей. А для защиты от информационных и киберугроз появляются новые продукты, технологии и решения.

Лучший подход для предотвращения киберугроз - организация Security Operation Center (SOC). Лучше предотвратить возникновение атак, чем реагировать на нарушение после того, как оно произойдет. Наиболее эффективная команда SOC будет обеспечивать безопасность и мониторинг периметра сети, данных, клиентов и удаленных пользователей, чтобы SOC мог обнаруживать, анализировать и немедленно реагировать на угрозы 24/7/365 [2].

Стоит отметить, что в качестве базовой платформы для организации SOC, как правило, покупается SIEM-система (Security Information and Event Management) [2]. SIEM - это решение для мониторинга информационных систем, анализа событий безопасности и обнаружения событий информационной безопасности. SIEM традиционно используются для решения проблемы накопления и оперативной обработки данных о событиях безопасности, поэтому основной задачей, решаемой в каждом проекте, является сбор, хранение и обработка событий информационной безопасности. SIEM является совокупностью двух терминов, обозначающих область применения программного обеспечения: SIM (Security Information Management) –управление информацией о безопасности, и SEM (Security Event Management) - управление событиями безопасности [3].

Основные задачи SIEM-систем:

- сбор событий с разных компонентов информационной инфраструктуры в реальном времени и их обработка;
- оперативное выявление инцидентов и атак, формирование базы знаний по инцидентам и атакам;

- проведение расследований инцидентов и атак;
- выявление нарушений принятых в компании политик;
- оценка уровня угроз для информационной инфраструктуры.

Стоит заметить, что интеллектуальные системы справляются с разбором событий в разы лучше человека. Во-первых, SIEM-системы способны рассматривать и оценивать риски с разных аспектов. Это важно, так как игнорирование даже одного аспекта может нарушить стабильность и целостность анализа. Во-вторых, SIEM-системы способны с большой скоростью анализировать данные, полученные с разных источников. Интеллектуальные решения могут справиться с большинством задач в разы быстрее, чем человек.

В текущей статье будет рассмотрено SIEM решение MaxPatrol от компании Positive Technologies и продемонстрировано, каким образом данная система способна выявлять инциденты из тысячи событий, поступающих из разных систем.

Работа с группами активов в MaxPatrol SIEM

Актив в контексте ИБ – это сущность, имеющая ценность для организации, использующаяся для достижения целей организации, являющаяся объектом защиты и атаки с целью нарушения свойств безопасности. Защита активов информационной безопасности – основная обязанность данного направления. В MaxPatrol SIEM используется иерархическая структура групп активов [4], в которой предусмотрены следующие типы групп:

- системные группы;
- пользовательские группы, которые могут быть динамическими или статическими.

Группировку активов рекомендуем использовать для решения следующих задач процесса управления активами:

- систематизация сведений об активах;
- присвоение значимости активам;

- автоматизация поиска и аудита активов;
- мониторинг состояния активов

Наличие информации об активах в MaxPatrol SIEM и применение механизма группировки позволяют решить ряд задач процессов управления событиями и инцидентами ИБ:

- автоматизация активного сбора событий;
- учет особенностей активов при корреляции событий;
- предварительная группировка событий;
- локализация затронутых инцидентом участков ИТ-инфраструктуры

Автоматизация активного сбора событий. Активные методы сбора событий требуют формирования пары «метод сбора событий <—> цель сбора событий (источник)» [6]. По аналогии с аудитом активов для автоматизации сбора событий рекомендуем операторам MaxPatrol SIEM в качестве целей использовать группы активов, имеющие в своем составе источники событий. При этом стоит учитывать, что методы сбора событий непосредственно связаны с ПО, с которого происходит сбор, а значит формирование групп во многом зависит от источников событий, подключаемых к MaxPatrol SIEM. Если после аудита будет выявлен источник событий на активе, то он автоматически попадет в соответствующую ему группу источников, и MaxPatrol SIEM будет собирать события с данного источника без дополнительных действий со стороны оператора.

Корреляция событий по группам активов. Тонкая настройка правил корреляции снижает количество ложных срабатываний, тем самым снижая нагрузку на операторов в части разбора событий, ошибочно признанных инцидентами. Ниже приведена часть алгоритма правила корреляции, определяющего тип заражения вредоносным ПО (внутреннее, внешнее) и порядок создания инцидента (Рис.1).

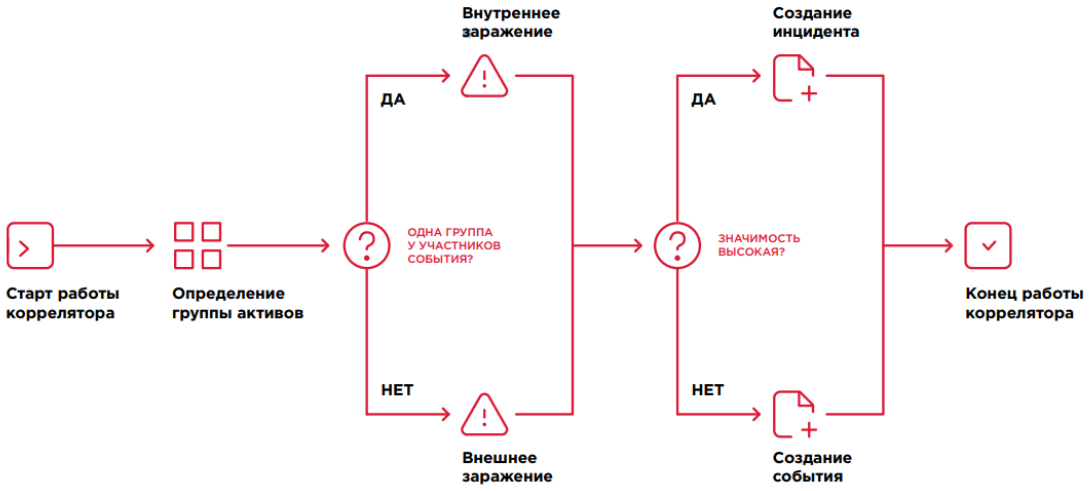


Рис. 1. Алгоритм правила корреляции, определяющего тип заражения вредоносным ПО

Предварительная группировка событий и инцидентов ИБ. При работе с событиями и инцидентами рекомендуем операторам MaxPatrol SIEM использовать сформированные группы активов в качестве первичного фильтра событий по источнику и участникам события [5]. Например, если необходимо выполнить поиск инцидентов в серверной группе, можно выбрать группы по IP-адресам серверов или группы по ролям серверов.

Определение масштаба влияния инцидента на инфраструктуру. При регистрации инцидента с ним автоматически сопоставляются активы-участники, перечень которых определяет правило корреляции, и связанные с ним события. На основе этой информации MaxPatrol SIEM указывает в карточке инцидента все группы активов, связанные с активами — участниками инцидента. Например, произошел инцидент заражения сервера SAP сетевым червем. При изучении карточки инцидента оператор может получить сведения о том, что он является членом групп «Подсеть 10.15.64.0/24», «Серверы», «SAP» и т. п. Анализируя возможности вредоносного ПО и принятые меры защиты, можно сделать вывод о том, что червь потенциально может распространиться по активам подсети

Отчетность по итогам разбора эскалации инцидентов

Доступ к сведениям об активах, событиях и инцидентах обеспечивается на основе созданных групп активов. Это позволяет предоставлять оператору доступ к информации, связанной только с выбранными группами, а значит отдельные категории пользователей не смогут ознакомиться с недоступной для них информацией. MaxPatrol SIEM позволяет формировать отчетность по процессам управления активами, событиями и инцидентами ИБ. Функция группировки активов обеспечивает возможность предварительной фильтрации информации, поступающей в отчет (Рис.2).

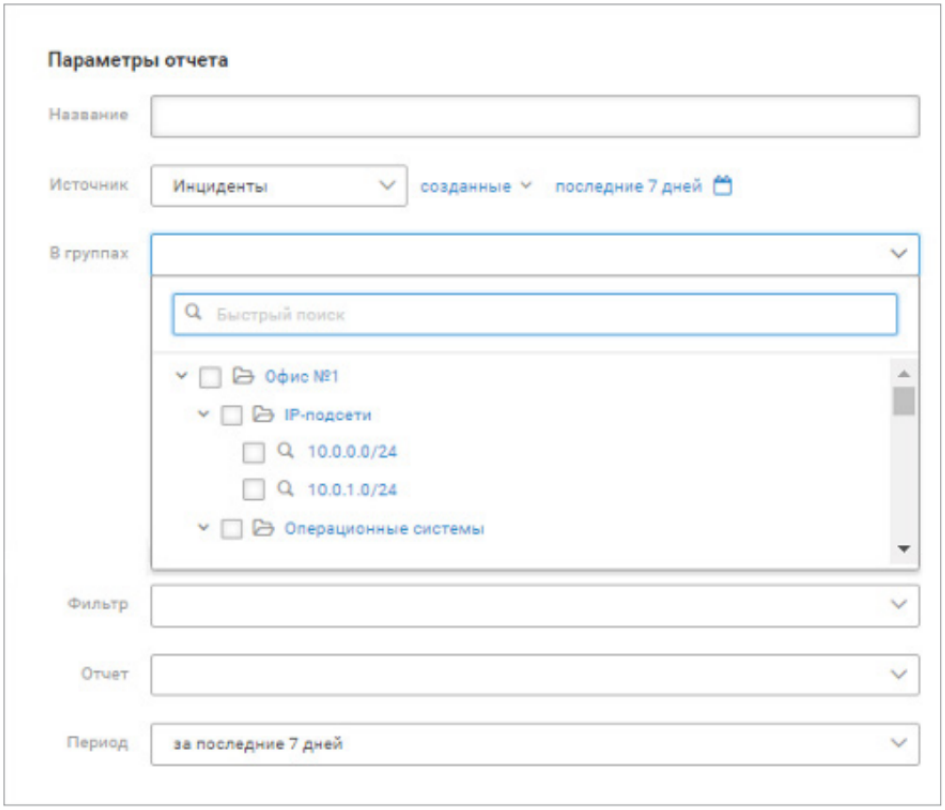


Рис.2. Отчетность по инцидентам

Примеры выявления инцидентов

Пример №1 – Обнаружение вредоносного ПО.

Вредоносное ПО – одна из самых актуальных угроз информационной безопасности. Причем большинство из них (порядка 85%) связаны с фишинговыми рассылками. Злоумышленников в основном интересуют корпоративные банковские счета, поэтому фишинговые письма адресуют бухгалтерам и финансистам, имитируя переписку с финансовыми структурами. Темой такого письма может быть, например, «Заявка на возврат», «Пакет документов за прошлый месяц» или «Паспортные данные сотрудников».

MaxPatrol SIEM использует внутренние сигнатуры для выявления вредоносной активности. То есть с некой регулярность система способна проводить сканирования, выявлять вредоносное ПО, фиксировать информация о самом выявленном вредоносном ПО, хосте, на котором оно было обнаружено, и иную другую информацию, указанную на рисунке 3.

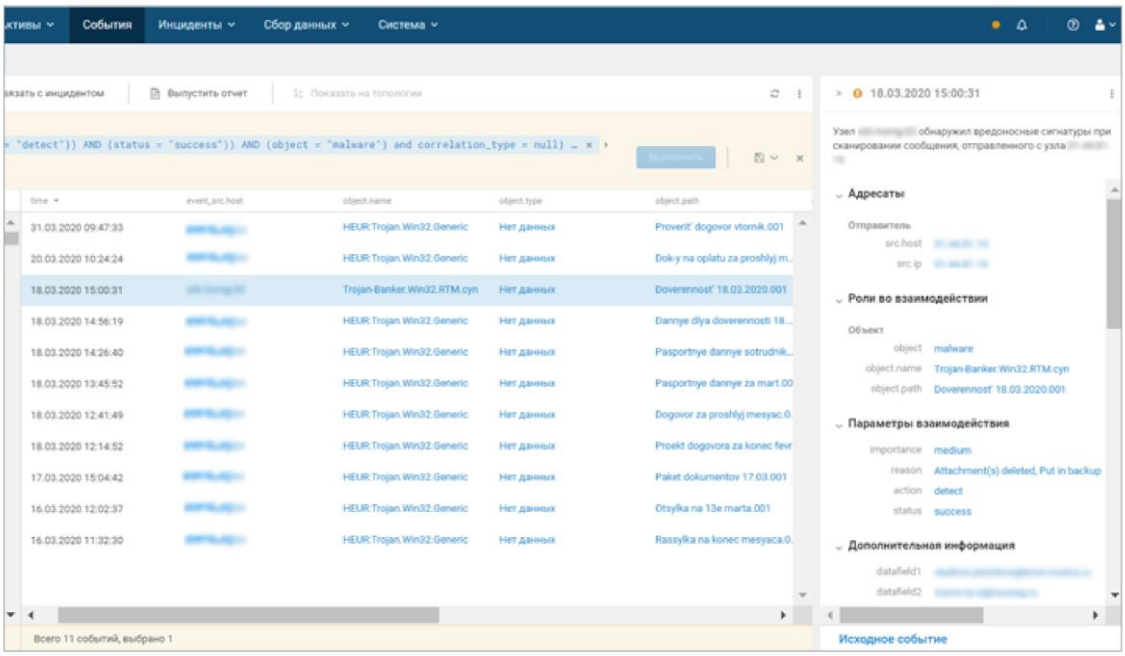


Рис. 3. Инцидент обнаружения вредоносного ПО

Пример №2 – Аномальное поведения пользователей.

Аномалии в поведении пользователей должны служить поводом для более подробного изучения событий. Такие действия иногда сложно отличить от

повседневной деятельности пользователей или администраторов, но они могут указывать на скрытое присутствие злоумышленников. Примеры событий, на которые стоит обратить внимание сотрудникам службы ИБ, — это, например, попытки выгрузки списков локальных групп или пользователей, создание нового аккаунта сразу после авторизации, использование одной учетной записи на нескольких рабочих станциях или работа сотрудника в ночное время (Рис.4.)

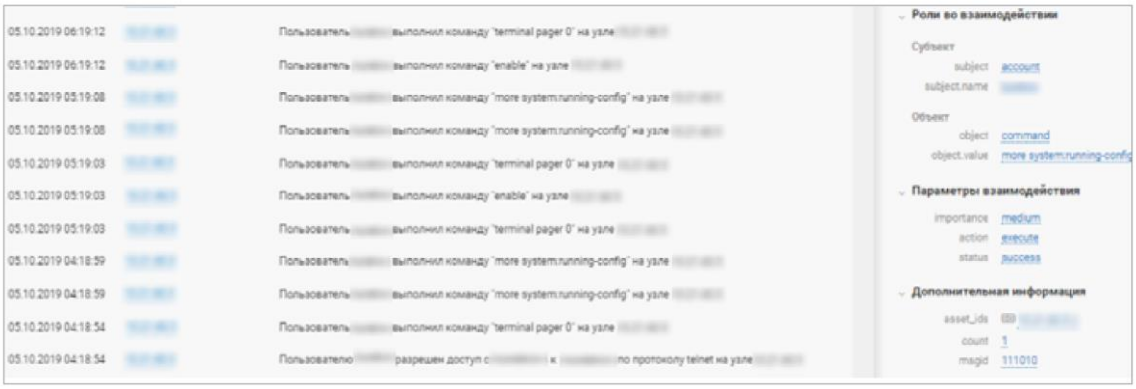


Рис.4. Инцидент обнаружения событий работы сотрудника в ночное время

Пример 3. Нарушение политик ИБ

Еще одна категория инцидентов — это нарушения политик ИБ. Речь идет о выявлении фактов несоответствия требованиям нормативных документов, таких как PCI DSS, приказ ФСТЭК № 21, а также корпоративным политикам ИБ. Как правило, компаниям рекомендуется ограничить список узлов, на которых может использоваться ПО для удаленного доступа. Соответственно, ниже в примере рассмотрен инцидент ИБ, связанный с установкой ПО, запрещенного политиками (Рис. 5). В качестве такого ПО выступает TeamViewer - ПО, используемое для

удаленного подключения к серверам и ПК.

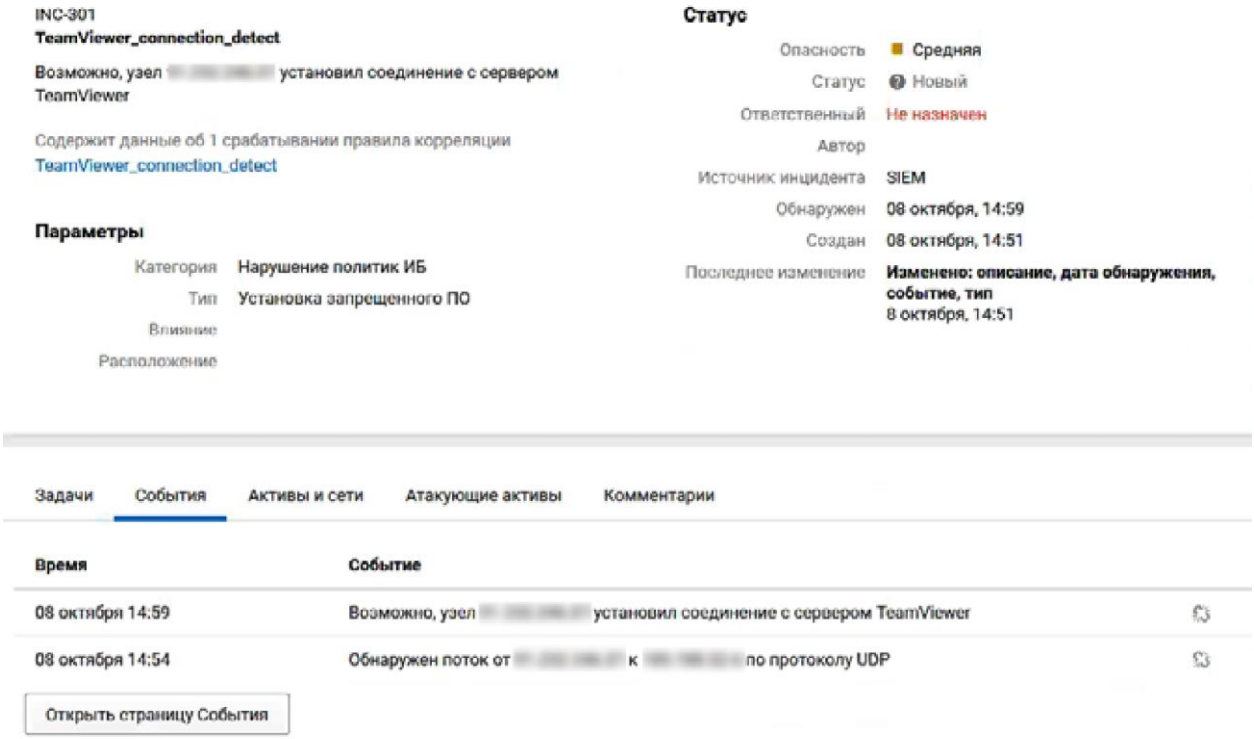


Рис. 5. Выявление инцидента по установке запрещенного ПО

В данной статье представлено лишь несколько примеров инцидентов, на основании которых проводился анализ эффективности SIEM решения MaxPatrol. Также были рассмотрены инциденты фишинга, DDoS-атаки, Kerberoasting атака.

Проведенный анализ позволил выявить, что MaxPatrol SIEM, благодаря встроенным правилам корреляции, позволяет выявлять актуальные техники атак без дополнительной настройки. Кроме того, MaxPatrol SIEM обладает правилами детектирования популярных техник атак (используется классификация MITRE ATT&CK), что позволяет обнаружить активность злоумышленников на ранних этапах.

Благодаря такому внедрению, компания сможет оценить эффективность инвестиций в развитие IT-инфраструктуры и обеспечить контроль за эффективностью работы систем информационной безопасности. Более того

технические специалисты начинают работать эффективнее за счет того, что периодический мониторинг миллионов событий будет автоматизирован.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Актуальные киберугрозы: III квартал 2021 года // Positive Technologies. [Электронный ресурс] — Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/ (дата обращения: 13.09.2022).
2. Бочкарев О.И. Создание собственного SOC в условиях международной изоляции/ О.И Бочкарев // Информационная безопасность и международная коммуникация в контексте цифровой трансформации. – С. 129-137
3. Штеренберг С. И. Разработка методики внедрения и выявления эффективности SIEM-системы / С. И. Штеренберг, Ю. С. Данилова // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – № 3. – С. 40-45.
4. MaxPatrol SIEM // Positive Technologies [Электронный ресурс]. — Режим доступа: https://www.ptsecurity.com/ru-ru/products/mpsiem (дата обращения: 13.09.2022).
5. Выявление инцидентов ИБ с помощью SIEM: типичные и нестандартные задачи // Positive Technologies [Электронный ресурс]. — Режим доступа: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/incidents-siem-2020-rus.pdf (дата обращения: 13.09.2022)
6. Как использовать механизм табличных списков в MaxPatrol SIEM// Positive Technologies [Электронный ресурс]. — Режим доступа: https://www.ptsecurity.com/upload/corporate/ru-ru/products/mpsiem/Mechanism-of-table-lists-mp-siem-a4-rus-0002-01-jun-23-2021.pdf (дата обращения: 13.09.2022)
7. Хлестова Д.Р. Анализ актуальности использования SIEM систем на предприятиях/ Д.Р. Хлестова, К.Г. Попов // Символ науки. – 2016. – №7/2016. – С. 33-36

Елецкий А.Е.,
МТУСИ, студент 1 курса,
Крылов Г.О.,
МТУСИ, ст. преподаватель

ИМПОРТОЗАМЕЩЕНИЕ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РФ

Тема импортозамещения в сфере иб начала активно набирать популярность в последние годы в связи с масштабными санкциями против нашей страны. Важно понять, почему нам необходимо продолжать развивать эту сферу в нашей стране, узнать, какие успехи и проблемы есть в данном вопросе.

Почему же мы не можем просто взять иностранные решения, а должны развивать именно Российские технологии?

Во-первых, в любой иностранный продукт может быть внедрён бэкдор (бэкдор- это дефект алгоритма, который намеренно встраивается в него разработчиком и позволяет получить несанкционированный доступ к данным или удалённому управлению операционной системой и компьютером в целом), программы по сбору данных, дистанционному доступу.

Во-вторых, многие иностранные компании имеют возможность заблокировать доступ к своему ПО

Примеры проблем, которые возникают в связи с отсутствием отечественных решений

Разберем конкретные примеры. В 2021 Positive Technologies (ведущая компания России в сфере иб) нашли в процессорах Intel Apollo Lake, Gemini Lake и Gemini Lake Refresh новую уязвимость. Она позволяет злоумышленникам войти в отладочный режим работы данных процессоров. В нем вполне возможно извлечь данные и легко запустить шпионское ПО, считают специалисты. Серии данных процессоров используются во многих устройств — в нетбуках, вещах с

устройствами подключения к Интернету и в автомобилях. «Указанные процессоры могут применяться в составе различного рода импортируемых и отечественных программно-аппаратных комплексах защиты информации», — считает руководитель департамента информационной безопасности Информационной внедренческой компании (ИВК) Игорь Корчагин. Как вы понимаете, данная уязвимость представляет опасность и Российским компаниям

Также в 2019 году эксперты из той же Positive Technologies обнаружили еще одну уязвимость , В составе хаба PCH и в процессорах Intel был обнаружен многофункциональный логический анализатор сигналов VISA (Intel Visualization of Internal Signals Architecture). Точнее, VISA — это инструмент Intel по проверке процессоров на исправность. Документация на блок не находится в открытом доступе, но это не значит, что её нет. Изучение VISA выявило, что изначально деактивируемый на заводе Intel анализатор может быть активирован злоумышленником, и он обеспечит доступ как к информации в памяти ПК, так и к сигнальным последовательностям периферии.

Также актуальной проблемой является то, что многие иностранные компании просто запретили нам пользоваться их решениями, большой ущерб это принесло компаниям, которые были зависимы от иностранного ПО

Как подходят к импортозамещению в сфере иб в других странах

А) Импортозамещение в Китае

Важно также рассмотреть подходы других стран к импортозамещению

9 Декабря 2019 года Китай объявил о плане полного отказа от зарубежных компьютеров и программного обеспечения, чтобы никакая важная информация не смогла попасть за пределы Китая. 100-процентное импортозамещение власти хотят реализовать к 2022 году.

Как пишет газета The Guardian, в общей сложности планируется заменить 20-30 млн образцов техники, используемой госучреждениями КНР. 30% от этого

количества должно быть заменено на китайское оборудование в 2020 году, 50% - в 2021-м и 20% - в 2022-м.

Также Китай уже давно ведет разработку процессоров на собственной архитектуре, видеокарт, жесткий дисков и собственного ПО.

Б) Импортозамещение на западе (США)

США также проводит политику импортозамещения. Они уже долгое время пытаются полностью отказаться от Китайской техники в области информационной безопасности, так как опасаются тех же бэкдоров и вредоносных программ, встроенных в устройства.

Санкции против китайских компаний начались еще в 2018 году. В этот год китайскую компанию Huawei под разными предлогами начали обкладывать санкциями.

Старт отмене компании начали спецслужбы США, они в феврале 2018 года заявили, что не рекомендуют американцам пользоваться смартфонами компаний Huawei и ZTE.” Это создает риски давления на нашу телекоммуникационную инфраструктуру. Это также означает опасность кражи информации и шпионажа, — заявил директор ФБР Кристофер Рэй (Chris Wray), поясняя, почему не стоит пользоваться гаджетами Huawei и ZTE.” Эту идею поддержали в правительстве и началась разработка проекта по запрету продажи и использования оборудования Huawei, который в скором времени вступил в силу.

28 января 2019 года правительство США предъявило Huawei официальные обвинения в промышленном шпионаже и мошенничестве. После этого началась полная замена всего китайского оборудования на отечественное. Также США начали давить на другие компании с целью разорвать все связи с компанией Huawei

В целом, большинство развитых стран начали активнее развивать сферу информационной безопасности в связи с деглобализацией и обострением международных конфликтов.

Импортозамещение в области иб в России

А) Когда началось импортозамещение

Импортозамещение в России в основном началось с введения санкций 2014-2015 года, конечно, и до этого момента разработки велись, но именно после событий Крыма начался наибольший ажиотаж над этой темой, именно тогда все окончательно поняли, что нужно развивать собственные разработки и стараться отказываться от зарубежных решений. Так, о необходимости преодоления критической зависимости от зарубежных технологий и промышленной продукции говорилось в послании Президента РФ Федеральному Собранию в конце 2014 года. После этого началась разработка нормативной базы. В 2015-16 году началось активное принятие законов об импортозамещении в сфере ИБ:

Приказ Минкомсвязи России от 31.12.2015 № 623 «Об утверждении состава Экспертного совета по российскому программному обеспечению при Министерстве связи и массовых коммуникаций Российской Федерации»

Приказ Минкомсвязи России от 20.06.2016 № 269 "Об утверждении Положения об Экспертном совете по российскому программному обеспечению при Министерстве связи и массовых коммуникаций Российской Федерации" (Зарегистрировано в Минюсте России 02.08.2016 N 43067)

Приказ Министерства связи и массовых коммуникаций Российской Федерации от 20 июня 2016 года N 269 «Об утверждении Положения об Экспертном совете по российскому программному обеспечению при Министерстве связи и массовых коммуникаций Российской Федерации»

Министерство связи и массовых коммуникаций Российской Федерации 17 октября 2016 года опубликовало статистические данные о структуре реестра отечественного программного обеспечения (ПО).

Приказ Минкомсвязи России от 01 апреля 2015 года № 96 «Об утверждении плана импортозамещения программного обеспечения»

Федеральный закон от 29 июня 2015 года №188-ФЗ "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и статью 14 Федерального закона " О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд"

Постановление правительства РФ от 16 ноября 2015 года №1236 «Об установлении запрета на допуск иностранного программного обеспечения при закупках для государственных и муниципальных нужд»

24 февраля 2016 года на официальном портале правовой информации http://publication.pravo.gov.ru/ опубликованы приказы Минкомсвязи:

приказ Министерства связи и массовых коммуникаций Российской Федерации от 31.12.2015 № 621 «Об утверждении классификатора программ для электронных вычислительных машин и баз данных»;

приказ Министерства связи и массовых коммуникаций Российской Федерации от 31.12.2015 № 622 «Об утверждении правил применения классификатора программ для электронных вычислительных машин и баз данных» ;

приказ Министерства связи и массовых коммуникаций Российской Федерации от 30.12.2015 № 614 «Об определении официального сайта оператора единого реестра российских программ для ЭВМ и баз данных в информационно-телекоммуникационной сети «Интернет».

Приказ Минкомсвязи России от 31 декабря 2015 г. N 621 «Об утверждении классификатора программ для электронных вычислительных машин и баз данных»

Приказ Минкомсвязи России от 01.04.2016 г. №134 «О внесении изменений в Классификатор программ для электронных вычислительных машин и баз данных … »

Приказ Минкомсвязи России от 30.12.2015 № 615 «Об утверждении Положения об Экспертном совете по российскому программному обеспечению при Министерстве связи и массовых коммуникаций Российской Федерации»

Минкомсвязью России в апреле 2015 года утверждён отраслевой план импортозамещения ПО:

План импортозамещения программного обеспечения

№ п/п	ОКПД (преимущественно)	Направление	Срок реализации проекта	Доля импорта в 2014 г.	Максимальная доля импорта к 2020 г.	Максимальная доля импорта к 2025 г.
Сегменты рынка корпоративного программного обеспечения, по которым уже имеется задел в виде конкурентоспособных отечественных продуктов - преференции отечественной продукции информационных технологий при осуществлении закупок за государственный счет						
1	58.29.21.000	Бизнес-приложения (ERP, CRM, BI, СЭД, управление проектами и т.д.)	2015-2025	75%	50%	25%
2	58.29.21.000	Антивирусное программное обеспечение и программное обеспечение информационной безопасности	2015-2025	60%	50%	40%
Сегменты рынка корпоративного программного обеспечения, по которым нет достаточного задела в виде конкурентоспособных отечественных продуктов - поддержка коллективной разработки программного обеспечения						
4	58.29.11.000	Клиентские и мобильные операционные системы	2015-2025	95%	75%*	50%*
5	58.29.11.000	Серверные операционные системы	2015-2025	75%	60%*	50%*
Сегменты рынка программного обеспечения, связанные с отраслевой спецификой						
9	58.29.21.000	Программное обеспечение для промышленности (PLM, CAD,CAM, CAE)	2015-2020	88%	60%*	50%*
10	58.29.21.000	Программное обеспечение для ТЭК	2015-2020	95%	70%*	50%*

Б) Импортозамещение на программном уровне

Хочется отметить, что по многим классам средств защиты есть аналоги, некоторые из них не уступают в качестве западным вендорам, например, межсетевые экраны, системы обнаружения вторжений, а по некоторым даже превосходят западные аналоги, например, антивирусные системы, DLP, полный список аналогов в таблице ниже

Класс продукта	Зарубежное ПО	Российские аналоги
Межсетевой экран следующего поколения NGFW	- Palo Alto Networks NGFW - Check Point Firewall - Fortinet FortiGate - Cisco FTD - Sophos XG Firewall - Juniper SRX	- UserGate UTM - Ideco UTM - Код Безопасности Континент - Инфотекс xFirewall
Хостовая защита EPP/EDR/XDR	- Check Point SandBlast Agent - Cisco AMP - Microsoft ATP - Symantec ATP - Palo Alto Networks XDR - Sophos Endpoint - Bitdefender Enpoint - Avast Business Antivirus	- Kaspersky EDR - Kaspesrky KES - Positive XDR - Код Безопасности Secret Net Studio - BiZone EDR - Блокхост-Сеть 4 - SafeNode System Loader - Dr.Web Desktop Security Suite

	- Symantec Endpoint - Panda Endpoint - McAfee Endpoint	
Контроль привилегированных пользователей PAM	- CyberArk PAM - BalaBit PAM Privileged Access Management - Fudo PAM	- Zecurion PAM - Efros Access Control Server - Indeed Privileged Access Manager
Управление учетными данными, доступом и идентификацией IAM/IDM	- IBM Security Identity Manager - Oracle Identity Manager (OIM) - SailPoint IdentityIQ	- Ankey IDM - Avanpost IDM - Solar inRights
Защита веб-приложений	- F5 - Imperva	- PT Application Firewall - Код Безопасности WAF - SolidWall WAF
Системы анализа и корреляции событий SIEM	- Micro Focus ArcSight - IBM Qradar - FortiSIEM - McAfee SIEM	- PT MaxPatrol SIEM - Kaspersky KUMA - RuSIEM - Ankey SIEM - CL DATAPK
Сканер безопасности	- Tenable Nessus - Qualis	- PT MaxPatrol VM - CL DATAPK Audit

Поведенческий анализ сетевого трафика NDR/NTA/UEBA	- Cisco StealthWatch - Plixer Scrutinizer - Vectra AI - Awake Security Platform - LogRhythm NetworkXDR - RSA NetWitness Network - ExtraHop Reveal(x) - TrendMicro DDI	- PT Network Attack Discovery - Гарда Монитор - CL Thymus
Обнаружение вторжений IDS/IPS	- TrendMicro TippingPoint - Palo Alto Networks NGFW - Check Point Firewall - Fortinet FortiGate - Cisco FTD - Sophos XG Firewall - Juniper SRX	- VipNet IDS - Код безопасности Континент - Kaspersky KATA и KICS - PT Network Attack Discovery - Гарда Монитор
Мультифакторная аутентификация MFA	- ESET SA - Microsoft MFA - Okta - Google Authenticator	- Multifactor - Алладин Jacarta - Актив Рутокен
Защита от утечек по сети и на хостах	- Symantec - ForcePoint	- Infowatch - SearchInform

DLP	- McAfee	
Антиспам	- Fortinet FortiMail - Cisco IronPort	- Kaspersky Antispam - Dr.Web Mail Security Suite
Разработка безопасного кода SAST/DAST	- Fortify Static Code Analyzer - Checkmarx CxSAST - IBM App Scan Source	- Solar inCode - Infowatch Custom Code Scanner
Управление поверхностью атаки EASM	- Palo Alto Networks XPANSE	- Group-IB AssetZero
Защита контейнеризации CWPP	- Palo Alto Networks Prisma Cloud - Aqua - Sysdig	Нет
Безопасность в облаке CASB	- Netscope - Palo Alto Networks CASB - Symantec CloudSOC - CipherCloud - Cisco CloudLock - Oracle CloudServic - Microsoft Cloud App Security	Нет
Сетевая безопасность	- Palo Alto Networks Prisma Access	нет

SASE/ZTNA	- Skyhigh Networks - Netscope NewEdge - Cisco SASE - Check Point CloudGuard Connect - Citrix SASE - FortiSASE - Versa SASE - Vmware SASE - Zscaler SASE	

В статистике от компании Код Безопасности наглядно видны проблемы, с которыми сталкивается наш процесс импортозамещения.

Основная проблема, которая выделяется в этом опросе – это сами компании, которые по нескольким причинам не хотят переходить на отечественное ПО, разберем основные, в связи с которыми они не хотят делать переход. Первая проблема - это отсутствие финансовой поддержки со стороны государства. Вторая проблема – это скептицизм в отношении Российских решений и простое нежелание тратить деньги и время на переход на отечественные решения

В) Импортозамещение в сфере оборудования

В данной сфере процесс идёт не так быстро, хоть в России и есть свои процессоры, к примеру процессоры марки Эльбрус, которые сделаны на полностью Российской архитектуре и имеют неплохую производительность, но проблема в том, что они собирались на заводах компании TSMC, а они запретили производство в этом году из-за санкций. В итоге мы оказались в ситуации, когда у нас есть собственные неплохие разработки, но произвести их мы не можем, так как в России совершенно нет заводов по производству процессоров такого уровня, а строительство такого дело долгое и затратное. Из-за чего импортозамещение в этой области практические остановилось. К примеру, с такими же проблемами столкнулся производитель Российских процессоров Байкал. в первую очередь надо решить проблему отсутствия базы для производства нашего оборудования.

Г) Эксклюзивное интервью с архитектором проектов/ведущим инженером информационной безопасности компании Softline о том, как на них повлияли санкции и как они проводят импортозамещение

(все ниже сказанное является личным мнением и не является официальной позицией компании по данным вопросам)

Никита Титов, ведущий инженер\архитектор проектов в отделе ИБ компании Softline

1) -Считаете ли вы импортозамещение в сфере иб важным процессом?

-Безусловно да. В первую очередь, процесс импортозамещения затрагивает государственные структуры и объекты критической инфраструктуры, стабильное

функционирование которых, для государства является первостепенным в виду важности этих отраслей для нормального функционирования государства. Во-вторых, хотел бы отметить, что сертифицированные средства защиты информации (СЗИ) проходят дополнительную проверку соответствия определенным критериям в лабораториях, аккредитованных для этой деятельности, в частности исключается использование не задокументированных возможностей. В-третьих, хотелось бы отметить, что при использовании российских решений в сфере ИБ, минимизируется вероятность того, что данные СЗИ будут отключены от обновлений, тех поддержки или полностью будут неработоспособны ввиду ухудшения политической обстановки и/или санкций. И в-четвертых, развитие внутреннего рынка ИБ повышает технологическую независимость страны, развивает внутренние кадры и повышает экономические показатели государства.

2) - С какими трудностями столкнулась компания в связи с санкциями 22года?

-Проблем было много, особенно на первоначальных этапах, когда было не понятно, как будет развиваться ситуация в дальнейшем, останутся ли зарубежные вендоры на нашем рынке и на долго ли, как будут исполняться контракты, которые уже были заключены, как будет происходить отгрузка оборудования. Даже в условиях, когда можно было найти адекватную российскую замену, которая ничем не уступала зарубежным вендорам, вставал вопрос как можно приобрести товар, какие сроки ожидания отгрузки в особенности, если это аппаратные платформы, которые в большинстве своем имеют зарубежную компонентную базу.

3)- Проводит ли компания softline импортозамещение иностранных решений ? Какими темпами оно идёт? С какими трудностями компания сталкивается?

-Да конечно, как только стало понятно, что зарубежные вендоры уходят, мы не стали дожидаться их окончательного решения (многие вендора долгое время не принимали решения об окончательном уходе, наблюдая за развитием ситуации) и составили исчерпывающий список для импортозамещения по каждому классу СЗИ,

да и не только СЗИ, но и ИТ решений. По многим классам решений у нас и до санкций больше было проектов по российским вендорам ввиду того, что они ни только не уступают зарубежным, но некоторые из них и превосходят, например, EPP от Kaspersky, SIEM от Positive Technologies. На данный момент на рынке уже прошел шок ухода зарубежных вендоров и темпы импортозамещения могу заметить отличные. В начале фин года мы столкнулись с ожидаемой реакцией заказчиков на огромный запрос на пилоты, демонстрации и тому подобное для поиска аналогов среди российских вендоров. Также были проблемы непосредственно с размещением заказов у российских вендоров, которые не были к такому большому наплыву новых клиентов и тем боле в такой коротки промежуток времени. Но сейчас ситуация уже стабилизировалась.

4) - Считаете ли вы возможным полный переход на российские продукты в сфере иб?

-Полный переход? в ближайшие лет 5 я не вижу такой перспективы. И дело не в том, что я не верю в российских разработчиков, как показывает практика выхода на рынок новых решений, даже от самых крупных российских компаний, они сталкиваются с кучей ошибок, недоработок, некорректно работающего функционала и на качественную доработку продукта уходит не один год и это нормальная практика, все набивают свои шишки. В определенных категориях СЗИ мы можем уже сейчас с уверенностью сказать, что доля зарубежного ПО крайне мала, но окончательно оставить рынок только под российские решения не получится. На данный момент мы видим запросы от заказчиков на зарубежное ПО "дружественных" стран - Китай, Индия.

5) - Какие меры, по вашему мнению, помогут реализовать политику импортозамещения на российском рынке?

-Для более качественного перехода на российских вендоров необходимо повысить конкуренция на рынке. После ухода зарубежных вендоров, российские компании по сути остались без самых сильных конкурентов, что позволило им

поднять цены на 30-50%, что с учетом того, что не все эти решения обладают сопоставимым функционалом с ушедшими решениями, приводит к тому, что Заказчики пытаются искать варианты покупки в обход санкций или начинают смотреть в сторону зарубежных решений дружественных стран. Также многие решения не адаптированы к современным реалиям, после ухода зарубежных облачных провайдеров, многие компании начали переходить на российских провайдеров, но решений по защите информации, которые можно в них использовать или интегрировать с другими СЗИ on-prem практически равна нулю

Д) Перспективы импортозамещения в России

Рассмотрим перспективы России в импортозамещении в сфере информационной безопасности. В области импортозамещения программного обеспечения Россия уже сейчас имеет немалые успехи, как мы можем подчеркнуть из интервью, мы достаточно стойко перенесли уход иностранных компаний из данной сферы, конечно, имеются проблемные стороны, к примеру необходимо решить проблемы, связанные с отсутствием конкуренции, в связи с уходом западных компаний, некоторым скептецизмом в отношении отечественных решений, а также финансовыми сложностями, связанными с переходом на российские решения., но в целом импортозамещение в данной области идёт достаточно хорошо.

Гораздо сложнее ситуация с импортозамещением в сфере оборудования. В данной области у нас серьезные проблемы с производством самого оборудования, все заводы, которые могут производить наши процессоры отказали нам в дальнейшем производстве, в связи с этим перспективы очень туманные, так как строительство собственных производств будет длиться непозволительно долго, необходимо искать решения в дружественных нам странах.

Заключение:

В целом Россия достаточно успешно проводит политику импортозамещения в сфере информационной безопасности. У нас отличный темп импортозамещения в

области программного обеспечения, но имеются проблемы с области оборудования.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Tadviser Санкции против Huawei/текст – электронный/ url: https://www.tadviser.ru/a/460529 (10.09 Дата обращения)
2. Валерий Тимошенко/ Политика импортозамещения в России: от слов к делу/текст – электронный/ url: https://www.garant.ru/article/630000/
3. Дмитрий Кухтенков/ Импортозамещение и Закон № 44-ФЗ/ текст – электронный/ url: https://otc.ru/academy/articles/importozameschenie_44_fz
4. Tadviser/Импортозамещение информационных технологий в Китае/ текст – электронный/ url: https://www.tadviser.ru/a/493312
5. Tadviser/Информационная безопасность в США/текст-электронный/ url: https://www.tadviser.ru/a/630465
6. Геннадий Детинич/Positive Technologies сообщила о находке новой потенциальной «закладки» в чипах Intel/ текст – электронный/ url:https://3dnews.ru/984950/positive-technologies-soobshchila-o-nahodke-novoy-potentsialnoy-zakladki-v-chipah-intel
7. Роман Кильдюшкин/Черный код: в процессорах Intel нашли две критические уязвимости/ текст – электронный/ url: https://iz.ru/1141889/roman-kildiushkin/chernyi-kod-v-protcessorakh-intel-nashli-dve-kriticheskie-uiazvimosti
8. Юрий Абрамов/Импортозамещение в ИБ: ожидания и перспективы/ текст – электронный/ url: https://www.securitycode.ru/upload/iblock/482/Importozameshenie_v_IB.pdf
9. Пьянзин Сергей Александрович/Импортозамещение в сфере информационно-коммуникационных технологий: нормативная база, проблематика, прецеденты/ текст – электронный/ url: https://dit.urfu.ru/fileadmin/user_upload/site_49_5219/news/Pjanzin_S.A.pdf

10. Александр Ендальцев/ Импортозамещение на рынке информационной безопасности/текст-электронный/url: https://habr.com/ru/post/676664/

11. Правительство России/ Приказы №623,269,96,621,622,614,134,615 / Постановление №1236 / Федеральный закон №188/ текст- электронный/ url: https://digital.gov.ru/

Жарова А.К.,
д.ю.н., доцент,
Елина В.В.,
студентка МТУСИ, факультет ИТ

ОБЕСПЕЧЕНИЕ АТРИБУЦИИ КИБЕРАТАК

Проблема противодействия компьютерным атакам, является общей для всех государств,

все информационно развитые государства взаимозависимы от уязвимостей, ошибок, программных закладок которые возможны в информационных технологиях, а результатом компьютерной атаки может стать межгосударственный конфликт.

Интернет - основа взаимодействия различных информационных технологий, а также человека с устройствами и образует ИКТ-сферу,

ее невозможно разделить на территории, принадлежащие государствам, она подобна космосу, который принадлежит всем.

Проблема обеспечения информационной безопасности ИКТ-сферы является одной из наиболее сложных.

С одной стороны, главной силой обеспечения безопасности должны выступать суверенные государства, а не отдельные индивиды, но в ИКТ-сфере ситуация складывается иным образом. Технологическая составляющая ИКТ-сферы позволяет физическим и юридическим лицам оказывать существенное влияние на ИКТ-отношения. Например:

- деятельность ИТ-гигантов,

- хакеры, которые могут удаленно провести компьютерную атаку на информационные технологии.

Проблему защиты от компьютерной атаки составляет сложность определения источника нападения, которым может быть программное обеспечение,

начавшее распространять вредоносную информацию или проводить атаку на сервер критической информационной инфраструктуры.

Для поиска лица, ответственного за проведение кибератаки, необходимо определить разработчика программной технологии, ее тестировщика, а также ее пользователя.

вредоносные действия могут произойти по причине программных закладок в технологии, так и в силу наличия уязвимостей, которые свойственны всем аппаратно-программным технологиям.

В случае программных закладок в технологии подлежит доказыванию преднамеренность действий разработчика, создавшего свою технологию с возможностями ее несанкционированного использования третьими лицами.

В случае применения уязвимости, другой вопрос – подлежат ли эти действия наказанию в соответствии с административным или уголовным законом?

Сложность выявления источника, лица, территории проведения и противодействия компьютерным атакам демонстрируют проблемы атрибуции компьютерных атак.

Атрибуция компьютерной атаки состоит из двух аспектов: технического и правового, связанных одной целью – собирание доказательств проведения компьютерной атаки и причастного лица. Исследования подтверждают, что провести атрибуцию компьютерной атаки очень сложно, многое зависит от примененных для проведения кибероперации технологий, а также от технологий и средств, потраченных на определение источника компьютерной атаки и лица ее реализовавшее.

Проблему атрибуции компьютерной атаки невозможно решить без внимания к вопросам кибербезопасности еще на стадии разработки, поскольку на последующих стадиях, например, на стадии применения информационных технологий исправление уязвимостей и нахождение программных закладок не всегда возможно.

Так, устройства можно скомпрометировать еще на стадии разработки, создать уязвимости или программные закладки.

Таким образом, критически важно знать поставщиков, разработчиков или производителей, а также тех, кто испытывает и сертифицирует технологию.

Такие вопросы должны находиться под контролем органов государственной власти.

Для обеспечения информационной безопасности государства видят один путь - это создание условий подчинения своему закону всех лиц, которые используют информационные технологии на его территории и их разрабатывают.

Таким образом, одним из методов обеспечения информационной безопасности и принуждения к выполнению требований национального законодательства является привязка информационных технологий к территории своего государства.

Поскольку невозможно снизить уровень взаимосвязанности современных обществ, лучшим вариантом является усовершенствование механизмов сдерживания и способов защиты

Необходимо обсуждать вопросы о применимости системы норм и принципов в целях обеспечения информационной безопасности, а также выявления ответственных лиц в связи с произошедшими компьютерными атаками и киберинцидентами.

Кашин Ю.О.,
МосУ МВД России им. В.Я. Кикотя, безопасность информационных
ехнологий
в правоохранительной сфере, 4 курс
yurikashin@mail.ru
Рязанова А.М.,
МосУ МВД России им. В.Я. Кикотя Безопасность информационных
ехнологий
в правоохранительной сфере, 4 курс
Булгаков В.В.,
ГБОУ «Школа Свиблово» г. Москвы, ученик 11 класса
Научный руководитель:
Булгакова Е.В.,
доцент кафедры информационной безопасности
МосУ МВД России им. В.Я Кикотя

СОВРЕМЕННЫЕ СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ В ОБЛАЧНЫХ ХРАНИЛИЩАХ ДАННЫХ

Облачные технологии являются большим прорывом в мире IT. Технология предоставляет огромный спектр различных преимуществ, начиная от управления данными и их хранением, заканчивая автоматизацией всего процесса на предприятии или компании. В настоящее время у IT-специалистов возникают вопросы о том, как обеспечивается безопасность данных в облачных вычислениях. Поэтому сегодня задача обеспечить безопасность данных и защиту конфиденциальности являются актуальной. Решение этих задач является основным факторам для дальнейшего развития технологий облачных вычислений во всех сферах ее применения.

В настоящее время выделяются следующие **виды проблем**, возникающие при хранении и обработке данных в облачных сервисах:

Репликация данных. Снимки и резервные копии данных в организациях делаются постоянно, сохраняясь в облаке. Но никто не может дать четкого ответа, где эти данные были сохранены и кто их может просматривать и получать к ним доступ. Владелец данных не может в таком случае идентифицировать и контролировать несанкционированное копирование своих данных.

Небезопасные API. Интерфейс программирования приложений позволяет пользователям настраивать свои методы облачных вычислений. API-интерфейсы могут представлять угрозу для облачной безопасности из-за их «природы». API предоставляют разработчикам инструменты для создания решений по интеграции своих приложений с другим программным обеспечением. Уязвимость API и заключается в этом взаимодействии, которое происходит между приложениями. Хоть оно и помогает разработчикам и предприятиям, но вместе с этим возникают серьезные проблемы с безопасностью.

Внутренние угрозы. Нельзя списывать данную угрозу со счетов. Возможно, владельцы считают, что данные, находящиеся в зоне контроля – в безопасности. Но это одна из самых больших проблем – недобросоветсные сотрудники, с которыми могут столкнуться разработчики и компании. Сотрудники организации могут использовать свой доступ к облачным сервисам для неправомерного использования или доступа к информации, связанной с финансами, персональными данными и т.д.

Стандарты защиты облачной информации – отечественные и зарубежные.

В нашей стране основные положения по обеспечению безопасности данных в облачных хранилищах содержатся в ГОСТ Р ИСО/МЭК 27018-2020, который в свою очередь идентичен иностранному ISO/IEC 27018:2019 "Information technology - Security techniques - Code of practice for protection of personally identifiable information (Pll) in public clouds acting as Pll processors" В данном документе

содержатся основные понятия, рекомендации и правила обращения с оборудованием, используемым для облачных вычислений, правил обращения с информацией а так же ссылки на многие другие смежные документы ИСО/МЭК, регламентирующие защиту информации.

Утечка данных у Amazon.

За прошедший время произошло большое количество утечек, следствием которых явились незащищенные хранилища Amazon S3. В результате было похищено огромное количество данных о различных организациях. По словам исследователей безопасности, в очередной раз обнаруживших три открытых хранилища AWS, платформа July System используется несколькими известными компаниями, включая CNN, ESPN, Intel, Toys “R” Us, CBS, Fox и NBC Universal Данные содержат учетные записи безопасности для приложений iPhone/Android и репозитория, которые потенциально могут позволить кому-либо получить доступ к персональным данным клиента и трекинга, а также внутренние сборки и средства разработки для различных клиентов, включая NFL, CBS, Amex, NBA, FOX, PGA и другие. Все три хранилища являются частью одной экосистемы, называемой EMSP. EMSP — это платформа Enterprise Mobility Services Platform, которая может получать ценную информацию о клиентах и персонализировать мобильных пользователей, используя Wi-Fi-сеть. В базах данных также были представлены файлы с именами и брендами, такими как Katy Perry, NFL, NBA. В одной из папок содержались более 1000 имен пользователей и паролей менеджеров Unilever в Индии. Реальная проблема заключаются в том, что обнаруженное является частью гораздо более крупной инфраструктуры и утекшие пароли могли быть использованы киберпреступниками для доступа к ее защищенным областям.

Почему защита данных в облаке необходима.

Защита облачных данных и другие вопросы конфиденциальности рассматриваются как существенные риски при хранении личной информации в облаке. Опасности или риски, связанные с хранением данных в облаке, включают:

• Несанкционированный доступ

• Убытки или ущерб, причиненные поставщиком услуг и их работниками

• Действия, направленные против поставщика услуг - взлом или отправка вредоносных программ и троянов

• Слабые методы обеспечения безопасности, связанные с защитой данных

• Нарушение регулятивного контроля

Прежде чем выбирать службу облачных вычислений, нужно провести анализ рисков, чтобы оценить любое потенциальное влияние на организацию. Поскольку значительная часть приложений и данных размещается в инфраструктуре сторонних производителей, существует несколько типов рисков. Например:

• Неспособность отслеживать, где хранятся приложения и данные.

• Отсутствие понимания того, как поставщик облачных услуг хранит и защищает данные.

• Пренебрежение признанием того, что облачная безопасность является общей ответственностью. Как правило, большинство облачных провайдеров имеют самую современную систему безопасности; однако она может быть ограничена.

• Игнорирование того, что облачные провайдеры имеют разные возможности, и неспособность устранить несоответствия в защите облачных данных путем разработки собственной политики безопасности.

Организациям также приходится решать ряд других проблем в области безопасности, таких как:

• Нарушения безопасности

• Неправомерное использование и кража данных

• Системные уязвимости и заражения вредоносными программами

Следовательно, несмотря на множество преимуществ облачных вычислений, существуют и подводные камни, которые необходимо устранить, чтобы обеспечить безопасность и защиту конфиденциальных данных.

Как защитить свои данные?

Не хранить конфиденциальные данные. Технологии меняются. Бизнес также меняется в соответствии с технологией. Сегодня данные играют важную роль в бизнесе. Таким образом, конфиденциальность данных является одним из основных аспектов любого бизнеса. Но если что-то есть в Интернете, трудно поверить, что это безопасно. Поэтому следует избегать хранения наиболее важных файлов или информации в облаке. Необходимо в облачной платформе хранить только те файлы, к которым вы часто обращаетесь, и избегать размещения информации, связанной с финансовыми данными, данными о конкурентах, данными о клиентах, контактными данными, такими как номер телефона / адрес и т.д.

Шифрование данных. Один из лучших способов защитить данные при использовании облачного хранилища - это шифрование данных. Это лучшая форма безопасности, поскольку перед доступом к данным требуется расшифровка. Это также защитит данные от поставщиков услуг и пользователей. Чтобы сделать их более защищенными, следует обеспечить облачное шифрование на этапах загрузки и выгрузки.

Зашифрованный облачный сервис. Существует несколько облачных сервисов, которые обеспечивают локальное шифрование и дешифрование файлов и информации внутри них, кроме хранения и резервного копирования. Это означает, что сервис заботится как о шифровании файлов, так и о их безопасном хранении в облаке. Это гарантирует, что никто, включая поставщика услуг или администраторов, не сможет получить доступ к вашим файлам и данным. На рынке доступно множество бесплатных, а также пробных версий.

Использование пароля. Первое, что можно сделать, это ввести надежный пароль, который может выдержать взлом. Очень важно часто менять свой пароль и никогда не использовать один и тот же пароль для всех учетных записей или папок. Можно выбрать 2-шаговую проверку для входа в систему, если облачный сервис предлагает такую возможность. Google Drive использует 2-фазный вариант входа в систему, состоящий из пароля и кода, отправленных на зарегистрированный номер. Эта дополнительная защита сделает данные намного безопаснее.

Антивирус является обязательным. Иногда самым слабым звеном оказывается компьютер или устройство, которые используется для доступа к облачным данным. Необходимо обеспечить надлежащую защиту системы или устройства. Если подвергать компьютер ошибкам и вирусам, хакеры могут легко получить доступ к системе. Необходимо выбрать эффективную и надежную антивирусную систему для системы, которая защитит все файлы и информацию внутри нее. Если ваша система не защищена должным образом, и если система не зашифрована и не защищена от ошибок, хакеры могут получить доступ к информации.

Ограничение доступа. Предоставлять доступ следует только тем пользователям, которые действительно нуждаются в нем. Внутренние пользователи и сторонние поставщики должны получать доступ только к тем файлам, которые необходимы им для работы. При необходимости нужно использовать ключи шифрования. Также необходимо регулярно проверять пользователей и поставщиков, и добавлять / удалять пользователей в соответствии с требованиями.

Непрерывное обновление системы. Безопасность облачных *данных* повышается благодаря регулярному исправлению и обновлению систем и прикладного программного обеспечения в облачной платформе. Для поддержания высокого уровня безопасности и поддержки новых версий, требуются новые исправления, обновления и пакеты обновления для операционной системы. Здесь

важно определять тенденции рынка и новые версии программного обеспечения, а также сообщать о пробелах в безопасности, которые могут возникнуть в установленных системах и приложениях.

Многонациональная структура конфиденциальности и безопасности. Чтобы обеспечить каждому бизнесу и стране все преимущества облачных вычислений, разные страны должны сотрудничать в разработке многонациональной структуры конфиденциальности и безопасности данных в облаке. По мере развития облачных вычислений и потоков данных из одной страны в другую. Например, данные были созданы в Индии с использованием программного обеспечения, размещенного в Великобритании, и хранятся в США у пользователей из Австралии. Облачный провайдер должен координировать весь этот процесс, чтобы обеспечить бесперебойную и безопасную передачу данных.

Правила трансграничной передачи данных. Для повышения эффективности и безопасности облачных решений, и получения быстрых результатов поставщики облачных услуг должны иметь возможность управлять центрами обработки данных в нескольких местах и свободно передавать данные между ними. Плавный поток данных позволяет облачным провайдерам оптимизировать свои услуги и предлагать лучшие бизнес-решения. Однако ограничения на трансграничную передачу данных могут создать неопределенность, если не соблюдаются правила или правовые рамки.

Чтобы защитить данные в облачной платформе, необходимо помнить обо всех вышеперечисленных вещах.

В заключении следует сказать, что облачный рынок имеет множество поставщиков, каждый из которых предлагает широкий спектр услуг. Это позволяет предприятиям и организациям оценивать несколько облачных провайдеров, чтобы найти тот, который наилучшим образом соответствует вашим потребностям в области безопасности, конфиденциальности и защиты данных.

Таким образом, облачные вычисления - одна из наиболее перспективных технологий для следующего поколения ИТ-приложений. Основной проблемой ускоренного роста облачных сервисов являются вопросы безопасности и конфиденциальности данных. Главной целью любой компании является сокращение объема хранения данных и связанных с этих затрат. Поскольку мы все знаем, что данные играют большую роль в принятии бизнес-решений, ни одна компания не будет размещать все свои бизнес-данные в облаке, если они не доверяют им полностью. Существует множество методов, которые были внедрены ИТ-исследователями для защиты данных и достижения наивысшего уровня безопасности данных. Тем не менее, все еще существуют определенные пробелы, которые необходимо заполнить, сделав эти методы более эффективными. Требуется больше знаний в области облачных вычислений, чтобы сделать их приемлемыми.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Утечка данных через незащищенное хранилище Amazon // SecurityLab URL: https://www.securitylab.ru/blog/personal/bezmaly/343140.php (дата обращения: 17.09.2022).

2. Ванина М.Ф., Ерохин А.Г., Фролова Е.А Применение облачных технологий в компаниях малого и среднего бизнеса // Век качества. – 2015

3. Лучшие практики по безопасности хранилищ данных // SecurityLab URL: https://www.securitylab.ru/analytics/502751.php (дата обращения: 15.09.2022).

4. Средства защиты данных // Библиофонд URL: https://www.bibliofond.ru/view.aspx?id=66834 (дата обращения: 14.09.2022).

5. Облачные вычисления // Хабр URL: https://habr.com/ru/post/111274/ (дата обращения: 16.09.2022).

6. Что такое безопасность облака? // Kaspersky URL: https://www.kaspersky.ru/resource-center/definitions/what-is-cloud-security (дата обращения: 18.09.2022).

7. Серикулы О. Информационная безопасность облачных вычислений // Вестник магистратуры. - 2019. - №6-5(93). - С. 17-23.

Корюкин Д.Д.,
Курганский государственный университет,
Информационная безопасность автоматизированных систем, 4 курс,
koryukin.danil@list.ru

ВИРТУАЛЬНАЯ ЧАСТНАЯ СЕТЬ ЕЕ БЕЗОПАСНОСТЬ И ЗАКОННОСТЬ

В современном мире во множестве стран существует тенденция увеличения защищенности различных объектов и субъектов, связанных с информационной сферой. Для успешной борьбы с угрозами необходимо обезопасить как конечные узлы сети, так и среду, по которой передаются данные [5]. Именно для этого можно использовать такой инструмент как VPN.

Виртуальные частные сети или как привычнее слышать сокращение VPN от английского наименования Virtual Private Network это совокупность технологий, которые обеспечивают развертывание одного или нескольких частных сетевых соединений над внешней сетью [3].

Данная технология зародилась в конце 20 века [1], но активное использование обрело позднее, это связано с увеличением количества субъектов, которым необходимо безопасно обмениваться информацией вне локальной сети или в сетях, которые физически расположены на большом расстоянии, еще из-за роста числа хакеров, которые стремятся заполучить конфиденциальную информацию, а также благодаря ужесточению цензуры множеством стран в сети интернет.

Вышеперечисленные проблемы подтолкнули пользователей использовать технологию VPN из-за того, что она обеспечивает шифрование информации, а еще с ее помощью возможна реализация множества функций [8]:

1. она помогает осуществить безопасность корпоративной информации, которая используется в делах государства или какой-либо корпорации;

2. обеспечивает конфиденциальность и защищенность данных в общедоступной сети;

3. при использовании интернет-телефонии, подключившись к публичной сети, обеспечивается конфиденциальность разговора;

4. реализуется подключение сотрудников организации, которые работают удаленно.

Глобально не обращая внимания на различные протоколы, можно обозначить два типа VPN сервисов по способу их соединения: «site-to-site» и «remote access» [9].

В первом случае реализация данного VPN-соединения достигается при помощи пограничных маршрутизаторов, когда две или более сети объединяются при помощи маршрутизаторов, создавая между собой VPN-туннель. Именно VPN-туннель мы и называем, в данном случаем, VPN. Данный туннель или туннели обеспечивает конфиденциальность и безопасность во внешней сети. Здесь важно отметить, что субъектами, которые обмениваются информацией, являются целые сети, то есть объединения двух или более конечных узлов.

Реализация типа соединения «remote access» достигается схожим образом, как в соединении «site-to-site», но в нем обмениваются информацией не целые сети, а конечные узлы. Так в соединении «remote access» строится VPN-тоннель между конечным устройством и VPN-сервером. При помощи данного подключения реальный IP-адрес устройства пользователя будет заменен на IP-адрес, который будет назначен VPN-сервером и именно под ним пользователь будет авторизован во внешней сети. Именно данный тип соединения чаще всего используется, так как намного больше пользователей, которые единолично хотят использовать технологию. Важно отметить, что для «remote access» соединения необходим клиент в виде приложения или расширения в веб браузере, как в случае соединения «site-to-site» реализация туннеля происходит на уровне маршрутизатора, если обратиться к сетевой модели OSI, полное название «The Open Systems Interconnection model», в переводе с английского модель взаимодействия открытых систем, то можно сказать, что данное соединение реализуется на третьем, то есть

сетевом уровне. Из-за популяризации и недопонимания технологии начали появляться обсуждения безопасности и законности ее использования в Российской Федерации.

Касаемо безопасности использования виртуальных частных сетей необходимо отметить, что VPN-сервисы обеспечивают конфиденциальность пользователя во внешней сети, но в то же время могут собирать и сохранять ту же информацию, поэтому становятся целью для злоумышленников, это касается VPN-сервисов, использующих тип соединения «remote access». Так, весной 2021 года на сомнительных форумах была выставлена на продажу информация о 21 млн пользователей бесплатных VPN-сервисов для Android, а в ноябре в открытый доступ просочились данные о 45,5 млн пользователей мобильных VPN-сервисов. Базы данных содержали основную информацию о мобильных устройствах, адресах электронной почты, паролях, и различных платежах [4]. Но данная ситуация не распространятся на, абсолютно, все подобные сервисы и такая проблема могла возникнуть и с другими системами, которые используют пользователи, будь то социальные сети или онлайн банки. Также необходимо отметить, что VPN-серверы являются не только целью злоумышленников, но и их инструментом для реализации кибер-атаки [2]. Как минимум с их помощью они скрывают свое физическое местоположение, а также защищенный обмен информацией между собой. Чтобы избежать утечки собственных данных необходимо пользоваться только проверенными и популярными VPN и другими сервисами, а также не злоупотреблять обменом важными данными при помощи VPN, если в этом нет необходимости, но это полностью не обеспечивает безопасность [7].

Относительно законности VPN-сервисов можно сказать, что законодательство РФ, в частности федеральный закон об информации, информационных технологиях и о защите информации не запрещает использование технологии VPN, но обязывает своих владельцев ограничивать доступ к заблокированным интернет-ресурсам в стране [10], в противном случае данные

сервисы рискуют попасть под блокировку. Роскомнадзор в середине марта 2022 года ограничил работу около 20 сервисов, которые нарушали законодательство Российской Федерации. Но требуется обратить внимание, что пользователи подобных сервисов не рискуют преступить закон, только если не используют виртуальные частные сети, как инструмент реализации противозаконных действий [6]. То есть люди могут посещать различные заблокированные объекты сети интернет, используя VPN, но в данном случае необходимо не забывать о возможной утечке данных.

Главной целью виртуальных частных сетей является обеспечение безопасности и конфиденциальности как объектов, так и субъектов сети, поэтому, при необходимости, ее разумно использовать в рамках, разрешенных законом Российской Федерации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. VPN [Электронный ресурс] URL: https://ru.wikipedia.org/wiki/VPN (дата обращения: 14.09.2022).
2. VPN: ещё раз просто о сложном [Электронный ресурс] URL: https://habr.com/ru/post/534250/ (дата обращения: 14.09.2022).
3. Виртуальная частная сеть (VPN) [Электронный ресурс] URL: https://www.ibm.com/docs/ru/i/7.2?topic=security-virtual-private-networking (дата обращения: 16.09.2022).
4. Данные 21 млн пользователей бесплатных VPN-сервисов для Android выставили на продажу в сети [Электронный ресурс] URL: https://www.forbes.ru/newsroom/tehnologii/422227-dannye-21-mln-polzovateley-besplatnyh-vpn-servisov-dlya-android-vystavili (дата обращения: 16.09.2022).
5. Мельников Д. А. Информационная безопасность открытых систем : учеб. пособие / М. : ФЛИНТ, 2014. – 31 с.

6. Можно ли пользоваться VPN в России? [Электронный ресурс] URL: https://www.interfax-russia.ru/kaleidoscope/zakonno-li-ispolzovanie-vpn-v-rossii#:~:text=%D0%97%D0%B0%D0%BA%D0%BE%D0%BD%20%D0%BD%D0%B5%20%D0%B7%D0%B0%D0%BF%D1%80%D0%B5%D1%89%D0%B0%D0%B5%D1%82%20%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D1%83%20VPN,%D0%B3%D0%BE%D1%81%D1%83%D0%B4%D0%B0%D1%80%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D0%BE%D0%B9%20%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9%20%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B5%20(%D0%A4%D0%93%D0%98%D0%A1) (дата обращения: 16.09.2022).

7. Николахин А.Ю. Использование технологии vpn для обеспечения информационной безопасности [Электронный ресурс] URL: https://cyberleninka.ru/article/n/ispolzovanie-tehnologii-vpn-dlya-obespecheniya-informatsionnoy-bezopasnosti (дата обращения: 16.09.2022).

8. Разрешает ли закон использовать VPN? Полный обзор 2022 [Электронный ресурс] URL: https://ru.vpnmentor.com/blog/%D0%B7%D0%B0%D0%BA%D0%BE%D0%BD%D0%BD%D0%BE-%D0%BB%D0%B8-%D0%B8%D1%81%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5-vpn/ (дата обращения: 17.09.2022).

9. Стивен Б. Виртуальные частные сети : учеб. пособие / под ред. Д.О. Труфанова – М. : Лори, 2001. – 135 с.

10. Федеральный закон "Об информации, информационных технологиях и о защите информации" [Электронный ресурс] : от 27.07.2006 N 149-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

Максимов О. В.,
Курганский государственный университет,
Информационная безопасность автоматизированных систем, 4 курс,
smegovic@gmail.com
Человечкова А. В.,
Курганский государственный университет, старший преподаватель,
chelovechkova_2011@mail.ru

ПРОБЛЕМЫ БЕЗОПАСНОСТИ «УМНОГО ГОРОДА»

С развитием технологий «умных городов» вопрос информационной безопасности становится все более актуальным. Система «умного города» работает с большим количеством данных, в том числе и конфиденциальных, защите которых должно уделяться отдельное внимание. Информация гражданина, кадры с камер видеонаблюдения, документы или персональные данные, должны быть защищены от несанкционированного доступа.

Для определения способов защиты данных в системе «умного города» необходимо сначала определить, что представляет «умный город», и провести анализ его информационных компонентов, обрабатывающих данные о гражданах и о ситуации в городе.

Умный город — это градостроительная концепция интегрирования множества информационных и коммуникационных технологий (ИКТ), в том числе систем Интернета вещей (IoT) для управления городской инфраструктурой: системами ЖКХ, транспортом, образованием, здравоохранением, безопасностью и т.д. Целью создания «умного города» является улучшение качества жизни жителей с помощью технологии городской информатики для повышения эффективности обслуживания и удовлетворения их нужд [6].

Система видеонаблюдения является одним из основных компонентов «умного города» [6]. Городская система видеонаблюдения — это государственная

информационная система, предназначенная для сбора, обработки и хранения видеозаписей с камер, установленных в городе, используемая для повышения качества жизни населения и уровня обеспечения безопасности [1]. Для системы видеонаблюдения используются IP-камеры. Они являются самодостаточным средством наблюдения, управляются через веб-интерфейс и самостоятельно передают видео по сети. Сетевая камера представляет собой микрокомпьютер на базе ОС Linux [9]. Для получения доступа к устройству необходимо знать, кроме самого IP-адреса, имя пользователя и пароль. Проблема заключается в том, что данные аутентификации не всегда устанавливаются и остаются по умолчанию. Также прошивка камеры не всегда позволяет конфигурировать параметры безопасности. Таким образом, к IP-камере может подключиться любой человек и, подобрав имя пользователя и пароль, получить визуальный доступ к контролируемому камерой объекту. Для защиты камер системы городского видеонаблюдения необходимо изменять данные доступа по умолчанию, регулярно обновлять пароль пользователя и, при необходимости, изменить прошивку IP-камеры, для настройки IP-адресов, которые могут получить доступ к устройству.

Неотъемлемой частью "умного города" является система "умных светофоров". Она регулирует автомобильный поток и разгружает улицы города от пробок, меняя продолжительность зеленого сигнала в зависимости от ситуации на дороге. Также существуют автомобили, которые считывают информацию со светофоров на перекрестке, и меняют свое поведение. Светофоры перекрестков в данной системе передают информацию между собой посредством радиосвязи. Проблема заключается в том, что пакеты, передаваемые по радиосвязи, далеко не всегда шифруются, и передаются в явном виде. Для перехвата данных достаточно настроить радиоприемник на необходимую частоту. Кроме просмотра информации, злоумышленник может сам отправлять пакеты и тем самым нарушить корректное передвижение транспорта на перекрестках, изменив работу светофоров. Дело ещё в том, что данная проблема носит системный характер, и отсутствие защищенной

связи скорее является нормой, чем исключением [4]. Для защиты соединения в системе "умных светофоров", если светофор не шифрует данные, необходимо изменить модуль передачи данных в светофоре, добавив в него программное или аппаратное шифрование. Данная мера не защитит передаваемые пакеты между светофорами от перехвата. Шифрование не позволит злоумышленнику понять содержимое пакетов, и таким образом предотвратит отправку корректных пакетов с ложной информацией.

Движение транспорта в "умном городе" зависит не только от корректной работы светофоров на перекрестках, но и от системы спутниковой навигации (GPS / ГЛОНАСС), которая внедрена в сам транспорт или в мобильное устройство водителя. Спутниковая навигация позволяет определять координаты устройства, а сервисы, использующие навигацию, могут прокладывать кротчайшие пути до места назначения, упрощая тем самым жизнь не только водителям транспортных средств, но и пешеходам. Спутниковая система навигации отвечает не только за координаты, но и за время, которое используют приложения. Для определения уязвимости навигационных систем необходимо понимать их принцип работы. Сигнал от спутника до целевого устройства преодолевает огромные расстояния, и на момент достижения цели имеет относительно слабую мощность. Для подделки сигнала достаточно устройства, которое генерирует подобный сигнал несколько большей мощности и глушит сигналы с действительных спутников. Ещё одной проблемой является большое количество помех на пути сигнала от спутника. Чтобы передать корректные данные, один информационный бит заменяется на большую последовательность бит с корреляционными свойствами. Кроме того, скорость передачи данных крайне небольшая – 50 бит в секунду [5]. Это всё приводит к тому, что передавать аутентификационные данные в виде дополнительных бит очень тяжело из-за низкой пропускной способности. Вышеперечисленные проблемы позволяют реализовывать GPS-спуфинг – подмену исходного местоположения GPS-устройства. Для реализации необходимо

использовать радиопередатчик, который создает помехи для реальных спутников и генерирует сигнал несколько мощнее действительного сигнала [10]. Подмена местоположения позволяет "телепортировать" GPS-устройства в совершенно другую точку планеты. В рамках города достаточно перенести транспорт в другое место города, чтобы сбить его систему навигации. В городе это может парализовать движение транспорта по улицам, создав огромные пробки. Подмена местоположения может использоваться и для атак на грузовые компании. Грузовые компании отслеживают положение своего транспорта. Замена геолокации транспорта позволяет угнать средство, незаметно для грузовой организации. Так как реальный сигнал от спутников имеет небольшую мощность и пакеты, передаваемые через данный канал связи, не имеют аутентификационных данных, как таковой защиты от GPS-спуфинга в данный момент не существует [5].

Как показывает практика, составляющие элементы "умного города" имеют уязвимости, о которых не задумываются специалисты во время установки оборудования. Реализация существующих угроз безопасности может привести к тяжелым последствиям, парализовать жизнь "умного города". Приобретение более качественного оборудования или модификация существующих устройств с уязвимостями может решить обнаруженные проблемы безопасности. Но, к сожалению, в настоящее время невозможно обезопасить "умный город" от всех проблем безопасности – GPS-спуфинг тому доказательство.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Городская система видеонаблюдения. URL: https://video.dit.mos.ru/ (дата обращения: 14.09.2022).

2. Как работают умные светофоры: преимущества и недостатки технологии. URL: https://trasscom.ru/blog/umnye-svetofory/ (дата обращения: 14.09.2022).

3. Качанов С.А. О месте аппаратно-программного комплекса"безопасный город" в концепции "умный город" / С.А. Качанов, А.П. Попов // Технологии гражданской

безопасности. — 2019. — №3. — С. 4-9.

4. Можно ли взломать умный город? - Умный город/ЖКХ. URL: https://smartcitytalk.ru/mozhno-li-vzlomat-umnyj-gorod/ (дата обращения: 14.09.2022).

5. Спуфинг подкрался незаметно, хоть виден был издалека / Хабр. URL: https://habr.com/ru/post/650741/ (дата обращения: 15.09.2022).

6. Умные города (Smart cities). URL: https://www.tadviser.ru/index.php/Статья:Умные_города_(Smart_cities) (дата обращения: 14.09.2022).

7. Умный город – что это, как и где применяется. URL: https:// center2m.ru/smart-city-about (дата обращения: 14.03.2022).

8. Умный город и безопасность — ФСА. URL: https://fsa3d.com/ 2020/03/19/smart-city-and-safety-19/ (дата обращения: 13.03.2022).

9. Уязвимости камер видеонаблюдения — Teletype. URL: https://teletype.in/@hacker_place/GYRvbyF-hhk (дата обращения: 14.09.2022).

10. Что такое GPS-спуфинг? Как работает и для чего используется? URL: https://bezopasnik.info/что-такое-gps-спуфинг-как-работает-и-для-ч/ (дата обращения: 15.09.2022).

Мясищева Н.Р.,
студент группы ЗРС2001 МТУСИ,
myasischevenr@gmail.com
Николаев В.В.,
МТУСИ ассистент кафедры БТК,
fredfred9033@yandex.ru

РУТКИТЫ - РАЗВИТИЕ И СПОСОБЫ ИХ ОБНАРУЖЕНИЯ.

Развитие интернета упрощает человеку жизнь, обеспечивая возможность обмениваться знаниями, заключать электронные договоры и оплачивать покупки, не вставая с кровати. Но подобного рода информация нуждается в защите, и чем она лучше, тем незаметнее и хитрее вирус, созданный, чтобы ее взломать.

Согласно словарю Фридланда, руткиты — это вредоносное программное обеспечение (ВПО), внедряющееся в приложения, прошивки, ядра операционных систем или гипервизоры, обеспечивая удаленный административный доступ к компьютеру и позволяющий скрыть свое присутствие [1]. Вместе с распространением различных сканеров для обнаружения вирусов, атаки становятся все более сложными и, к сожалению, открытые ресурсы и быстрый обмен информацией дает возможность злоумышленникам тщательно планировать преступления и совершать атаки на другие устройства невероятно быстро а, главное, незаметно.

Процесс создания руткита требует достаточно большого опыта в использовании разных ПО, знаний и усилий, за счет чего этот вид атак не является популярным. Но каждый случай обнаружения связан с громкими преступлениями.

Так, например, 9 июля 2010 года специалисты белорусской антивирусной компании «ВирусБлокада» нашли следы применения руткита Stuxnet, направленного на ядерные объекты Ирана [2]. Он заставлял компьютеры изменять частоту вращения центрифуг, что приводило к их разрушению. При этом

Модифицированный модуль, при попытке чтения изменения блоков программы, отображал их в исходном виде, что позволяло скрыть факт модификации. В результате этих действий ядерная программа Ирана была отброшена на два года назад, а исследователи этого руткита до сих пор спорят о времени начала его действия.

В ходе расследования этого преступления удалось установить, что основная функция ВПО – распространение и автономная работа в замкнутой системе с последующим саботажем работы системы управления производственными процессами. Более того, для реализации этих целей необходимо иметь идентичную объекту нападения аппаратно-программную систему, несколько модулей, написанных с использованием различных сред разработки и языков программирования и значительное финансирование. Это не свойственно «традиционным» киберпреступникам, которые обычно преследуют цели «монетизации» прибыли и, как правило, используют ВПО, разработанное программистами-одиночками [2].

Исследование, проведенное Positive Technologies в 2020 году [3], утверждает, что за последние 10 лет лишь в 31% случаев руткиты использовались с целью получения денежной выгоды. В более чем 70% случаев атаки были направлены на внедрение в инфраструктуру и получение информации.

Типы руткитов

На рисунке 1 представлены виды руткитов.

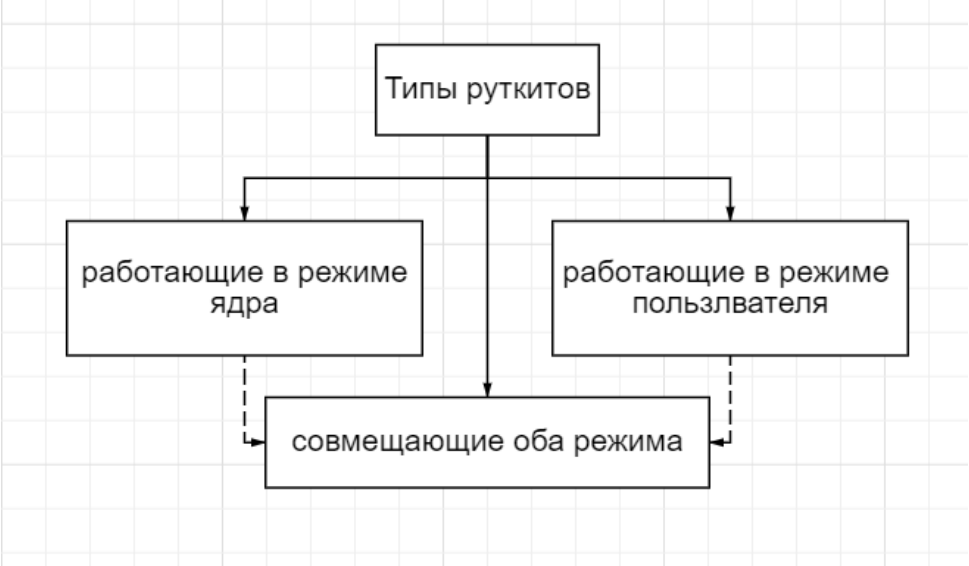


Рис.4 Типы руткитов

Руткиты, работающие в режиме пользователя, имеют привилегии приложений и чаще всего используются в массовых атаках. Они перехватывают и изменяют поведение исполняемых файлов. Например, подобный вредонос может внедриться в DLL вашего принтера, что позволит ему действовать, ведь вы уже разрешили вносить изменения вашему «безопасному» девайсу.

Руткиты, работающие в режиме ядра обычно разрабатывают в виде драйверов устройств или загружаемых модулей и имеют привилегии, схожие с операционной системой [4]. Такие руткиты сложнее в создании, так как могут повлиять на стабильность системы, что противоречит их основной задаче – оставаться незамеченными. Пример подобного руткита был приведен выше.

Совсем недавно в поле зрения исследователей появлялись руткиты, совмещающие в себе оба режима работы, например, DirtyMoe. Данный руткит с 2017 года пользуется скомпрометированными ПО с целью майнинга криптовалюты и запуска DDos-атак.

Несмотря на сложность разработки каждый год появляются все новые, гремящие на весь мир, руткиты. Это говорит о том, что на такой вид атак имеется

спрос и есть организации, готовые профинансировать нужные им ВПО [5]. Главными тенденциями в развитии руткитов стали активный переход на пользовательский режим, в силу относительной простоты разработки, и усиления функции сокрытия активности.

Как распространяются руткиты

Согласно классификации MITRE ATT&CK [6], руткиты распространяются на целевые устройства следующими методами:

1) В 69% случаев это происходит с помощью фишинга или другого типа атак с применением социальной инженерии. Цели атак загружают и устанавливают ВПО, скрытые внутри других приложений или программ, что дает злоумышленникам контроль над большей частью операционной системы.

2) 62% приходятся на эксплуатацию уязвимостей для принудительной установки руткита на компьютер в публично доступных приложениях.

3) ВВО можно также распространить через съемные носители, но это не самый массовый способ. На него приходится всего 15%.

4) ВПО также может быть связан с зараженными файлами PDF, пиратскими носителями или приложениями из подозрительных сторонних магазинов [7].

Основными целями атак с помощью руткитов являются государственные учреждения (44%), научно-исследовательские институты (38%), телекоммуникационные компании (25%) и частные лица (56%). Самой уязвимой системой для подобных преступлений является Windows (69%). Несмотря на то, что руткиты изначально были придуманы для Unix ОС, на нее приходится всего 31% случаев нападения. На системы Android, macOS и IOS же приходится по 6% [3].

Способы обнаружения руткитов и защиты от них

Так как руткиты появились уже около 30 лет назад, способы их обнаружения не заставили себя долго ждать. Основными концепциями защиты от ВПО были ограничение доступа или создание демилитаризованной зоны, так называемой, песочницы [8].

Первый вариант основан на проверке электронных подписей, целостности системы и установке специальных сканеров, в реестр которых записаны руткиты старых моделей. К сожалению, эта концепция имеет ряд минусов, в числе которых низкая вероятность обнаружить новый, ранее не известный руткит и большая нагрузка на ОС устройства. Такой вариант подходит только для закрытых систем, и подразумевает построение нескольких этапов защиты и тщательной проверки устройства, даже этапе создания.

Второй же вариант предполагает свободное общение прокси-сервера с внешними для защищаемой сети информационными системами и наличие максимально упрощенного интерфейса между этим сервером и компьютерами в защищаемой локальной сети. Предполагается, что ВПО, попав в песочницу, может нанести вред только в пределах песочницы, а более простой интерфейс с внутренним компьютером остановит дальнейшее проникновение ВПО в защищаемую локальную сеть [8]. Этот способ гораздо эффективнее ограничения доступа, но все еще не гарантирует своевременное обнаружение руткита. Однако, продуктах ранее упоминаемой компании Positive Technologies имеются песочницы с технологией проактивного и скрытого детектирования [3], которые позволяют обнаружить ВПО даже после того, как система заражена. К сожалению, в таком случае помогает только полная переустановка системы.

Также, в обнаружении уже установленных руткитов помогут специальные утилиты, средства обнаружения активности на конечных узлах и проверка сетевого трафика на предмет аномалий [9]. Но, во-первых, как уже было сказано ранее, это не самый эффективный способ защиты, так как ваши данные уже скомпрометированы. А, во-вторых, некоторое утилиты оставляют уязвимости,

благодаря которым позволяют устанавливать руткиты. Так, 18 мая 2020, исследователю Биллу Демиркапи удалось скомпрометировать утилиту RootkitBuster компании Trend Micro и, с ее помощью, установить собственный руткит на устройство [10]. Примечательно, что исполняемые файлы этого сканера были распакованы еще до того, как пользователь согласился с условиями пользования, что позволило Биллу, с юридической точки зрения, вносить изменения в только что установленную программу.

На примере случая с руткитом Stuxnet видно, что подобные ВПО потенциально могут спровоцировать катастрофу или террористический акт, поэтому особенно важно исследовать новые способы защиты. Для частных лиц же достаточно регулярно проверять и устанавливать обновления безопасности, проверять цифровые подписи и обновлять базы антивирусных средств [7].

Подводя итоги, можно сказать, что атака с использованием руткита – очень опасная и трудно обнаруживаемая атака, которая может скомпрометировать даже самые защищенные организации. Несмотря на трудности при создании, преступники находят новые способы разработки и распространения вирусов, что сказывается на безопасности как госучреждений, так и рядовых пользователей. Но создатели антивирусных средств развивают свои продукты, надо только следить и вовремя обновлять библиотеки известных руткитов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Фридланд А.Я. Информатика и компьютерные технологии: Основные термины: Толков. Слов.: Более 1000 базовых понятий и терминов. - 3-е изд. испр. и доп./ А.Я. Фридланд, Л.С. Ханамирова, И.А. Фридланд. - М.: ООО «Издательство Астрель», 2003. - 272 с.

2. И снова о Stuxnet // Хабр URL: https://habr.com/ru/post/159053/ (дата обращения: 19.09.2022).

3. Руткиты: эволюция и способы обнаружения // Positive Technologies URL: https://www.ptsecurity.com/ru-ru/research/analytics/rootkits-evolution-and-detection-methods/ (дата обращения: 19.09.2022).

4. Кирилова К.С., Цветков А.Ю., Волкогонов В.Н. ПРОБЛЕМА ОБЕЗВРЕЖИВАНИЯ РУТКИТОВ УРОВНЯ ЯДРА В СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ // I-methods. - 2020. - №том 12 №3. - С. 1-9.

5. Барабанов А.В., Гришин М.И., Кубарев А.В. Моделирование угроз безопасности информации, связанных с функционированием скрытых в вредоносных компьютерных программ // Вопросы кибербезопасности. - 2014. - №4. - С. 41-48.

6. MITRE ATT&CK // MITRE ATT&CK URL: https://attack.mitre.org/matrices/enterprise/containers/ (дата обращения: 19.09.2022).

7. Что такое руткит – определение и описание // kaspersky URL: https://www.kaspersky.ru/resource-center/definitions/what-is-rootkit (дата обращения: 19.09.2022).

8. Грушо А.А., Грушо Н.А., Тимонина Е.Е. Методы защиты информации от атак с помощью скрытых каналов и враждебных программно-аппаратных агентов в распределенных системах // История и архивы. - 2009. - С. 33-45.

9. Авезова Я.Э., Фадин А.А. Вопросы обеспечения доверенной загрузки в физических и виртуальных средах // Вопросы кибербезопасности. - 2016. - №1. - С. 24-30.

10. Опасный тренд. Как утилита Trend Micro для борьбы с руткитами позволила устанавливать руткиты // xaker URL: https://xakep.ru/2020/05/19/trendmicro-rootkit/ (дата обращения: 19.09.2022).

Сухоносов Ф.А.,
доцент кафедры Информационная безопасность,
Ратушняк А.Н.,
доцент кафедры Информационная безопасность,
Шабельник Д.И.,
студент кафедры Информационная безопасность

РАЗРАБОТКА ПРЕДЛОЖЕНИЙ ПО СОВЕРШЕНСТВОВАНИЮ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОКОММУНИКАЦИОННОЙ СЕТИ ЮРГПУ (НПИ)

Корпоративная вычислительная сеть ЮРГПУ(НПИ) (NPINet) представляет собой систему для доступа в сеть Интернет и к ресурсам «ЮРГПУ(НПИ)» для обеспечения учебного процесса. Наиболее крупными сегментами NPINet являются: библиотечный корпус, главный корпус, робототехнический корпус, лабораторный корпус, химический корпус и горный корпус. Основу пользователей данного сегмента составляют студенты и преподаватели ЮРГПУ(НПИ), пользующиеся персональными компьютерами и иным оконечным оборудованием. Такое оборудование, устаревая в среднем за 5–6 лет, требует модернизации или замены.

Подразделения ЮРГПУ(НПИ) имеют сетевые серверы, предназначенные для использования внутри подразделения. Сетевая служба NPINet является центром административного контроля и управления сетью NPINet. В ее функции входит:

- установка, наладка, эксплуатация, ремонт и сопровождение программно–аппаратных средств общего пользования NPINet;

\- контроль за состоянием технических средств центрального и выносных узлов сети NPINet;

- управление маршрутизацией внутри сети NPINet ;

- обеспечение функционирования основных сетевых сервисов (DNS, email, и др.);

- обеспечение взаимодействия с другими сетями передачи данных;

- регистрация и перерегистрация всех пользователей NPINet, сетевых элементов и сервисов;

- обеспечение безопасности работы сети;

Текущая конфигурация сети имеет следующие существенные недостатки:

1. С 1 января 2025 года органам власти и МСУ, госкомпаниям, стратегическим предприятиям и системообразующим организациям будет запрещено использовать западные средства защиты информации (Указ Президента РФ от 1 мая 2022 г. № 250 “О дополнительных мерах по обеспечению информационной безопасности Российской Федерации”), из которых состоит весь сегмент ЮРГПУ (НПИ). Требуется замена импортного оборудования в соответствии с руководящими документами ФСЭТК.

2. Постановление Правительства РФ от 16 ноября 2015 г. N 1236 "Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд", требует замены программного обеспечения.

3. В связи уходом компании Cisco с рынка, все сегменты NPINet, потеряли свою актуальность.

В связи с перечисленными недостатками текущей конфигурации сети возникает необходимость в проведении анализа объекта исследования, разработке технических предложений по совершенствованию новой сети NPINet. Предложены и реализованы следующие технические решения:

- Замена маршрутизирующих устройств и коммутаторов.
- Внедрение межсетевого экрана, с целью установки средств защиты информации в соответствии с руководящими документами ФСЭТК.
- Внедрение ViPNet IDS NS.

- Построение новой сети NPINet.
- Установка средств защиты информации в соответствии с руководящими документами ФСЭТК.
- Замена маршрутизирующих устройств.

ESR-1500 FSTEC предназначен для использования в корпоративных сетях связи. Устройство сертифицировано Федеральной службой по техническому и экспортному контролю (ФСТЭК), что позволяет использовать ESR-1500 FSTEC в качестве межсетевых экранов типа “А” пятого класса защиты в государственных организациях, ведомственных структурах, в информационных системах персональных данных и других организациях с повышенными требованиями к передаче конфиденциальных данных.

В соответствии с требованиями ФСТЭК к межсетевым экранам устройства ESR FSTEC обеспечивают следующий функционал:

1. Контроль и фильтрация трафика;
2. Аутентификация пользователей;
3. Сбор и хранение статистики событий;
4. Взаимодействие с другими средствами защиты информации.

MES7048 - это высокопроизводительные устройства, оснащенные интерфейсами 10GBASE-R и 100GBASE-SR4/LR4 и предназначенные для использования в операторских сетях в качестве устройств агрегации и в центрах обработки данных (ЦОД) в качестве Top-ofRack или End-of-Row коммутаторов.

MES2448B - Коммутаторы осуществляют подключение конечных пользователей к сетям крупных предприятий, предприятий малого и среднего бизнеса, а также к сетям операторов связи с помощью интерфейсов 1G/10G. Функциональные возможности коммутаторов обеспечивают поддержку виртуальных локальных сетей, многоадресных групп рассылки и расширенные функции безопасности.

MES3324F - коммутатор агрегации, предназначен для использования в операторских сетях в качестве коммутатора уровня агрегации района или транспортного коммутатора. Устройство имеет значительный запас по производительности благодаря универсальным интерфейсам, работающим на скорости 10 Гбит/с или 1 Гбит/с. Коммутаторы также имеют 4 интерфейса 10 Гбит/с (SFP+).

ViPNet IDS NS является средством обнаружения сетевых атак и вредоносного программного обеспечения в файлах, передаваемых в сетевом трафике.

ViPNet IDS NS предназначен для интеграции в компьютерные сети с целью повышения уровня защищенности информационных систем, центров обработки данных, рабочих станций пользователей, серверов и коммуникационного оборудования.

ViPNet IDS NS в исполнениях ViPNet IDS NS100/1000/2000 представляет собой программно-аппаратные средства на базе x86-64-совместимой аппаратной платформы и программного обеспечения ViPNet IDS NS.

Имеет сертификацию ФСБ России: сертифицирован как средство обнаружения сетевых атак (вторжений) в составе ViPNet IDS 3 на соответствие требованиям к СОА класса В. А также сертификацию ФСЭК: сертифицирован как система обнаружения вторжений на соответствие требованиям: «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2011), «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения доверия безопасности информационных технологий» (ФСТЭК России, 2020) по 4 уровню доверия.

Способы подключения в сети.

Под подключением ViPNet IDS NS в сети предполагаются:

- Внедрение в защищаемую сеть устройства дублирования трафика и его подключение к интерфейсу захвата трафика ViPNet IDS NS.

- Подключение управляющего интерфейса ViPNet IDS NS в локальную сеть организации.
- Управляющий интерфейс, подключается к сетевому оборудованию сегмента защищаемой сети.
- Обмен данными по сети со следующими внешними системами:
  - Системы анализа и мониторинга информации о событиях (ViPNet TIAS, SIEM и т.д.);
  - Система централизованного управления и мониторинга ViPNet IDS MC;
  - Системы мониторинга состояния узлов (SNMP-менеджеры, NetFlow-коллекторы). NTP-серверы.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Гафнер В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. — Рн/Д: Феникс, 2017. — 324 с.;
2. Родичев Ю. А. Информационная безопасность. Национальные стандарты Российской Федерации / Ю. А. Родичев — «Питер», 2019 — (Учебник для вузов (Питер)) ISBN978-5-4461-1275-3. - 304 с.;
3. Шаньгин В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. — М.: ДМК, 2017. — 702 с.;
4. Ярочкин В.И. Информационная безопасность: Учебник для вузов / В.И. Ярочкин. — М.: Акад. Проект, 2018. — 544 с.;
5. Методика определения актуальных угроз (АУ) безопасности ПДн при их обработке в ИСПДн, которая утверждена заместителем директора ФСТЭК (14.02.2008 г.);
6. Методические рекомендации по обеспечению с использованием криптографических средств безопасности ПДн при их обработке ИСПДн с

использованием средств автоматизации, которые утверждены Приказом руководства восьмого Центра ФСБ РФ № 149/5-144 (21.08.2008).

7. Постановление Правительства РФ от 16 ноября 2015 г. N 1236 "Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд";

8. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: Приказ ФСТЭК России № 17 от 11 февраля 2013. - 2013;

9. Шаньгин В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. — М.: ДМК, 2017. — 702 с.;

10. РЕГЛАМЕНТ СЕТИ в ЮРГПУ (НПИ) имени М.И. Платова Новочеркасск, [Электронный ресурс]// ЮРГПУ (НПИ) имени М.И. Платова. – https:www. npi-tu.ru/assets/files/docs/cnit/Reglament_seti/doc.

Топчиев Г.В.
ЮРГПУ(НПИ), студент
bunny666666@mail.ru

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В РАМКАХ ИМПОРТОЗАМЕЩЕНИЯ

Аннотация

Цель работы заключается в изучении и анализе Российского ПО а также офисных приложений , в связи с актуальностью замены иностранного ПО в рамках санкций в сторону Российской Федерации, для полного обеспечения независимости нашей страны в плане информационных технологий.

В ходе работы показано, как проводить анализ ПО и на какие вещи нужно ориентироваться в первую очередь; определены зарубежные продукты, используемые в организациях на территории Российской Федерации, которые подлежат замене отечественными аналогами (система управления базами данных Oracle, операционные системы Windows и VMware, офисное приложение Microsoft Office, почтовая система Outlook) ; как достигнуть полной независимости от иностранного ПО и почему это так важно. В результате работы, определены ПО, приложения и программы наиболее подходящие для замещения используемых зарубежных на данный момент.

Итогом работы является комплекс ПО, приложения и программы наиболее подходящие для замещения используемых зарубежных на данный момент.

В связи современной международной обстановкой , идет борьба государств за лидирующие позиции в сфере информационных технологий. Надо понимать, что лидирующие позиции будут занимать только те страны, которые выбирают технологии будущего.

Так в Российской Федерации модернизация и совершенствование происходит

на основе внедрения новых перспективных Информационно-коммутационных технологий (ИКТ).

Существенным фактором на развитие ИКТ в России, является введение санкций против нее со стороны западных стран . С учетом такой позиции на западе по отношению к Российской Федерации , Указом Президента от 30.03.2022 № 166 , установлен запрет на закупку Юридическими лицами иностранного ПО и программ в целях его использования на объектах критической информационной инфраструктуры с 31 марта 2022 года. А так же с 1 января 2025 года, запрещается органам государственной власти использовать иностранное ПО.

Кроме этого, необходимо понимать, что угрозы негативного воздействия со стороны стран-конкурентов на информационную инфраструктуру , как всегда актуальны , посредством внедрения вредоносных программ в компьютерную технику или ПО, поставляемых на территорию Российской Федерации.

Анализ и определение зарубежного ПО и программ используемых в юридических, а так же и в государственных учреждениях показывает нам, что для полной независимости, а так же исключения возможных угроз или атак со стороны запад – замещения данного ПО и программ необходимо и максимально актуально.

В настоящее время существует определенный список ПО и программ используемых не только в отдельных юридических организациях и органах государственной власти. Но и обычными гражданами Российской Федерации, что так же может негативно сказаться на угрозу от западных стран по отношению к России.

Данный список состоит из следующих ПО и программ :

1. Система управления базами данных Oracle
2. Операционные системы Windows и VMware
3. Офисное приложение Microsoft Office
4. Почтовая система Outlook
5. Программная система коммуникаций Zoom

Оценка Системы управления базами данных

Система управления базами данных (СУБД) – является очень важной частью в информационной инфраструктуре. Естественно первостепенно нужно обратить на нее внимание. Поэтому при выборе заместителя иностранного ПО, можно смело остановиться на отечественной Системе управления базами данных – PostgresPro. В свою очередь она имеет большой спектр возможностей. а так же входит в Единый реестр и имеет сертификат ФСТЭК.

Данная СУБД разработана на платформе наиболее востребованной PostgresSQL. К тому же проверена крупными предприятиями , такими как : Федеральная налоговая служба (ФНС) , Министерство Финансов (МинФин) , Газпромнефть , Федеральная Таможенная Служба (ФТС) и др.

Однако, существуют некоторые недостатки в этой системе , которые пока что препятствуют резкому массовому внедрению в большие структурные юридические организации , а так же государственные учреждения, такие как :

1. Возможный недостаток уровня отказоустойчивости и производительности на существующих у организаций или государственных учреждений объемах баз данных , с учетом необходимости скорости обработки транзакций.

2. Администрирование и управление Система управления базами данных PostgresPro требует высококвалифицированных специалистов для безопасного использования и своевременных устранений неполадок, что влечет либо замену кадров, либо переобучение уже работающих сотрудников.

Оценка операционных систем

Следующим немаловажным пунктом в области в имортозамещения является замена Операционной системы компании Microsoft на отечественные операционные системы. По результатам анализа, можно выделить 2 основные ОС для массового внедрения - РедОС и Альт.

Данные ОС обладают сертификатом ФСТЭК России, что подтверждает его соответствие требованиям информационной безопасности и допускает его применение в государственных информационных системах.

Анализ данных ОС проводился на основе технических требований к Операционной системе и ее различных характеристик, условиям функционирования и обеспечение информационной безопасности, в том числе :

- Рекомендованные системные требования к АРМ (автоматизированному рабочему месту), таких как : Объем оперативной памяти, частота процессора , объем свободного места на диске.

- Сертификация (имеют ли данные ОС действующие сертификаты по актуальное время)

- Наличие возможности удаленного подключения к другим средствам и системам (Виртуальных рабочих столов, и подключение к удаленному рабочему столу)

- Совместимость с офисным пакетом программ, присутствующих в Реестре

- Поддержка сетевых протоколов

- Разрядность системы и поддержка процессоров с 64-ех битной архитектурой

Оценка офисного приложения для работы с документами

Не считая систем управления базами данных и операционные системы, для большинства пользователей существуют еще и офисные программы, с которыми нужно постоянно взаимодействовать и применять в рабочее время. Одной из таких программ является встроенный продукт компании Microsoft – Office (для работы с текстовыми файлами и документами). Так же в группу основных программ для работы с документами входят Excel (для работы с таблицами), и PowerPoint (для работы с презентациями).

На замену данным офисным приложением лучшим кандидатом является пакет программ от МойОфис. В свою очередь, отечественный аналог имеет все те же возможности по эксплуатированию документов, как и в текстовом формате, так

и в работе с таблицами и презентациями.

Самым главным пунктом при выборе данного пакета программ, естественно является его удобство и возможность применения. Но так же нельзя забывать и о том, что МойОфис имеет актуальные действующие сертификаты ФСТЭК России №4119 , №3688 , № 3877.

Исходя из этого, можно с полной уверенностью сказать, что настольные версии ПО МойОфис – это безопасное Программное обеспечение в условиях современных киберугроз.

Оценка Почтовой системы

Основной функционал почтовой системы - обмен электронной почтой и мгновенными сообщениями. Зарубежный сервис встроенный в Операционную систему Microsoft – Outlook обладает именно этими возможностями. Но отечественный представитель почтовой системы с наиболее мощной структурой - CommuniGate Pro является хорошим аналогом для Outlook.

Основной функционал CommuniGate Pro: обмен электронной почтой, мгновенными сообщениями, управление календарем, контактами, задачами, заметками, возможность голосовых и видео коммуникаций, полноценный контакт-центр, хранение и совместная работа с корпоративным контентом, возможность доступа посредством веб-интерфейса, так и с помощью популярных клиентов, наличие единой панели управления администратора.

Самое главное, у CommuniGate Pro есть свой функционал по управлению идентификацией, аунтификацией :

- Аутентификации (в т.ч. двухфакторная) пользователей; поддержка работы служб RADIUS;
- LDAP-сервер и LDAP- доступ в справочник, хранящий информацию о пользователях;
- Механизм внешней аутентификации, в т. ч. готовые утилиты

синхронизации с Active Directory;

• Средства шифрования, безопасная почта, встроенные средства для работы с S/MIME;

• SSL/TLS - безопасный обмен данными для основных протоколов;

Заключение

В ходе проделанной работы, можно смело утверждать, что большинство ПО и программ западного происхождения можно массово начать заменять уже сейчас. Конечно, с большими и сложными системами , как СУБД еще нужно провести много тестирований, чтобы внедрять такие системы без потерь денежных и временных ресурсов. Однако, отечественные производители ПО и программ ничем не уступают по общему функционалу компьютерных технологий и программ , используемых ежедневно

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. http://publication.pravo.gov.ru/Document/View/0001202203300001.

2. Белов Е.Б., Лось В.П. и др. Основы информационной безопасности. Учебное пособие для вузов. – М.: Горячая линия - Телеком, 2006. – 544 с.

3. Гатчин Ю.А., Климова Е.В. Ожиганов А.А. Основы информацион- ной безопасности компьютерных систем и защиты государственной тайны: учебное пособие. - СПб: СПбГУ ИТМО, 2001. - 60 с.

4. Гатчин Ю.А., Климова Е.В. Основы информационной безопасно- сти: учебное пособие. – СПб: СПбГУ ИТМО, 2009. – 84 с.

5. ГОСТ Р 51624-00 Защита информации. Автоматизированные си- стемы в защищенном исполнении. Общие требования.

6. ГОСТ Р 51275-99 Защита информации. Объект информатизации, факторы, воздействующие на информацию. Общие положения.

7. ГОСТ Р ИСО 7498–2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть1. Архитектура ЗИ.

8. Грибунин В.Г., Чудовский В.В. КСЗИ на предприятии. – М.: Ака- демия, 2009. – 416 с.
9. https://myoffice.ru/certificates/
10. https://www.communigate.ru/main/customers/
11. https://redos.red-soft.ru/
12. https://www.basealt.ru/

Чубан А. С.
ЮРГПУ (НПИ) им. М. И. Платова, 10.05.02-ЗИСа-017, 5 курс,
ann.solovyova2014@gmail.com
Научный руководитель:
Ратушняк А. И.,
ЮРГПУ (НПИ) им. М. И. Платова, доцент кафедры ИБ, к.в.н. доцент
a.ratushnyak@npi-tu.ru

РИСК-АНАЛИЗ ИССЛЕДУЕМЫХ СИСТЕМ, В ОТНОШЕНИИ КОТОРЫХ РЕАЛИЗУЕТСЯ МОДЕЛЬ УГРОЗ ИБ

Зачем нужно исследовать риски в сфере информационной безопасности (ИБ) и что это может дать при разработке системы обеспечения ИБ для информационной системы (ИС)?

Риск информационной безопасности — это вероятность возникновения негативного события, которое нанесет ущерб организации или физическому лицу. Применительно к сфере информационной безопасности (ИБ) выделяют следующие последствия:

1. Утечка конфиденциальных данных в организации
2. Внешние атаки на информационные системы компании
3. Действия неблагонадежных сотрудников (человеческий фактор)
4. Доступ к потенциально опасным объектам во внешней сети
5. Получение информации при помощи технических средств
6. Вредоносное ПО (трояны, бэкдоры, блокировщики, шифраторы и т. д.)
7. Использование нелицензионных программных решений, зачастую содержащие не декларируемые возможности

Утечка данных в большинстве случаев связана с непониманием сотрудников возможных последствий при нарушении правил ИБ. Пример: рассылка коммерческой информации через незащищенный канал связи. Сетевые атаки, как

правило, проводятся с целью воровства коммерческой тайны, шпионажа за конкурентами, вывода из строя критически важных для жертвы ресурсов и пр.

Человеческий фактор включает в себя не только ошибки сотрудников, но и умышленные действия, которые приводят к распространению конфиденциальной информации.

К опасным объектам относятся сайты, содержащие фишинговые скрипты, зловредное ПО или другие средства, которые нарушают информационную безопасность физического или юридического лица. К примеру, сотрудник зашел на веб-ресурс, созданный мошенниками, и оставил аутентификационные данные, которые в дальнейшем будут использоваться для шантажа.

Риском в сфере ИБ будем называть потенциальную возможность понести убытки из-за нарушения безопасности информационной системы (ИС). Зачастую понятие риска смешивают с понятием угрозы.

зачем нужно исследовать риски в сфере ИБ и что это может дать при разработке системы обеспечения ИБ для ИС. Для любого проекта, требующего финансовых затрат на его реализацию, весьма желательно уже на начальной стадии определить, что мы будем считать признаком завершения работы и как будем оценивать результаты проекта. Для задач, связанных с обеспечением ИБ это более чем актуально.

Для ответа на данный вопрос в процессе создания системы ИБ можно использовать два подхода.

Первый из них основан на проверке соответствия уровня защищенности ИС требованиям одного из стандартов в области информационной безопасности. Это может быть *класс* защищенности в соответствии с требованиями руководящих документов Гостехкомиссии РФ (сейчас это ФСТЭК России), *профиль защиты*, разработанный в соответствии со стандартом ISO-15408, или какой-либо другой набор требований. Тогда критерий достижения цели в области безопасности - это выполнение заданного набора требований. *Критерий эффективности* -

минимальные суммарные *затраты* на выполнение поставленных функциональных требований: $\sum C_i \rightarrow min,$ где c_i - *затраты* на i -е средство защиты.

Основной недостаток данного подхода заключается в том, что в случае, когда требуемый уровень защищенности жестко не задан (например, через законодательные требования) определить "наиболее эффективный" уровень защищенности ИС достаточно сложно.

Второй подход к построению системы обеспечения ИБ связан с оценкой и управлением рисками. Изначально он произошел из принципа "разумной достаточности" примененного к сфере обеспечения ИБ. Этот принцип может быть описан следующим набором утверждений:

- абсолютно непреодолимой защиты создать невозможно;
- необходимо соблюдать баланс между затратами на защиту и получаемым эффектом, в т.ч. и экономическим, заключающимся в снижении потерь от нарушений безопасности;
- стоимость средств защиты не должна превышать стоимости защищаемой информации (или других ресурсов - аппаратных, программных);
- затраты нарушителя на несанкционированный доступ (НСД) к информации должны превышать тот эффект, который он получит, осуществив подобный доступ.

Но вернемся к рискам. В данном случае, рассматривая ИС в ее исходном состоянии, мы оцениваем размер ожидаемых потерь от инцидентов, связанных с информационной безопасностью (как правило, берется определенный период времени, например - год). После этого, делается оценка того, как предлагаемые средства и меры обеспечения безопасности влияют на снижение рисков, и сколько они стоят. Если представить некоторую идеальную ситуацию, то идею подхода отображает приведенный ниже график на рис.1[1].

Рис. 1.- Идеализированный график соотношения "затраты на защиту - ожидаемые потери".

Современные методики и технологии управления информационными рисками позволяют оценить существующий уровень остаточных информационных рисков. Это особенно важно в тех случаях, когда к информационной системе предъявляются повышенные требования в области защиты информации. Существенно, что качественно выполненный анализ информационных рисков позволяет провести сравнительный анализ «эффективность/стоимость» различных вариантов защиты, выбрать адекватные контрмеры и средства контроля, оценить уровень остаточных рисков[4].

Кроме того, инструментальные средства анализа рисков, основанные на современных базах знаний и процедурах логического вывода, позволяют построить структурные и объектно-ориентированные модели информационных активов компании, модели угроз и модели рисков, связанных с отдельными информационными и бизнестранзакциям. Следовательно, выявлять такие информационные активы компании, риск нарушения защищенности которых является критическим, то есть неприемлемым.

Такие инструментальные средства предоставляют возможность построить различные модели защиты информационных активов компании, сравнивать между собой по критерию "эффективность/стоимость" различные варианты комплексов

мер защиты и контроля, а также вести мониторинг выполнения требований по организации режима информационной безопасности отечественной компании.

Организациям необходимо задокументировать все стадии оценки риска, периодичность и способы её проведения, список ответственных за выполнение оценки, процедуры отчётности о результатах, способы обработки риска, которые будут использоваться, метод организации мониторинга риска и прочее. Часто подобные документы называют методикой управления риском. Поскольку риски для ИБ и ИТ в Положении рекомендуется оценивать качественно, а не количественно, нужен соответствующий план качественной оценки. В нём могут быть отражены области оценки (список бизнес-процессов, в отношении которых проводится оценка риска), периоды и ответственные за проведение оценки сотрудники. Мы рекомендуем делать такой план приложением к методике управления рисками. Положение обязывает описать все элементы системы управления риском во внутренних документах организации. Рекомендуется разработать единое руководство, в котором будет описано, как именно у вас реализован тот или иной элемент системы управления риском: своеобразный «навигатор» по ней. Такой подход зарекомендовал себя при построении систем управления ИТ-услугами и систем управления ИБ. Это позволяет избежать накопления лишней документации в вашей организации, помогает сотрудникам понять, как устроена и функционирует система, упрощает жизнь проверяющим. Порядок ведения базы событий риска должен включать требования к форме и содержанию вводимой информации, описывать процедуры внесения данных подразделениями, определять то, каким образом в процессе будут участвовать дочерние организации. Вдобавок необходимо описать, кто и каким образом собирает информацию о событиях риска, кто определяет потери, если эти события случатся.

Служба информационной безопасности формирует специализированные отчёты по рискам для ИБ, которые затем направляет на рассмотрение коллегиальному

исполнительному органу. Эксперт кредитной организации отвечает за расчёт потерь от реализации событий рисков, а внешний эксперт выполняет оценку того, насколько эффективно функционирует система управления риском. В задачи службы внутреннего аудита входит ежегодная оценка эффективности работы коллегиального органа управления операционными рисками. Поскольку риски для ИБ напрямую влияют на функционирование информационных систем, отвечающие за эти системы подразделения должны не реже раза в год анализировать требования к ним с учётом планов развития и отчётов службы ИБ. Эта работа ложится на плечи ИТ.

Таким образом с помощью внедрения и реализации решений организация получит уверенность в безопасности конфиденциальной информации, а так же системное понимание информационных потоков организации, снижение бизнес-рисков.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Руководство: НОУ «ИНТУИТ» 2003-2022 URL: https://intuit.ru/studies/courses/962/387/lecture/8990?ysclid=l84gz1ovyn269017497

2. Руководство:1995-2022 Компания «Инфосистемы Джет» URL: https://www.jetinfo.ru/analiz-riskov-upravlenie-riskami/

3. ФСТЭК России, 2022: ГОСТ Р ИСО/МЭК 27005-2010 // Приказ руководителя Росстандарта N 632-СТ от 30.11.201.

4. Руководство: Студенческий научный форум - 2012 URL: https://scienceforum.ru/2012/article/2012002437

5. Руководство: 2006–2022, Habr URL: https://habr.com/ru/post/279219/

6. Руководство: Методика определения угроз безопасности информации в информационных системах. Методический документ утвержден ФСТЭК России 2015 г. URL: https://fstec.ru/component/attachments/download/812

7. Руководство: Стрельцов А.А. Содержание понятия «обеспечение информационной безопасности» // Информационное общество №4. С.12 2015

8. Руководство: Выписка из Основных направлений научных исследований в области обеспечения информационной безопасности Российской Федерации. URL: http://www.scrf.gov.ru/security/information/document155/

9. Руководство: Галатенко В.А. Основы информационной безопасности. М., 2016. 264 с. URL: http://en.bookfi.net/book/584428

10. Руководство: 2022, ООО «ИЗДАТЕЛЬСТВО СК ПРЕСС» URL: https://www.itweek.ru/infrastructure/article/detail.php?ID=59394

Стецко Д.Б.,
студент учебной группы ЗРС2201,
Крылов Г.О.,
МТУСИ, профессор, д.ф-м.н.

КРИПТОДЖЕКИНГ И СПОСОБЫ ПРОТИВОДЕЙСТВИЯ ЗАРАЖЕНИЮ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА

Введение

Криптоджекинг – киберпреступление, при котором злоумышленник получает несанкционированный доступ к системе и использует ресурсы устройства с целью добычи криптовалюты. Основная опасность данного типа киберпреступлений заключается в том, что зачастую пострадавшие не знают о том, что их устройство заражено, так как весь процесс проходит в фоновом режиме.

Похищая вычислительные мощности зараженных устройств, хакеры без существенных рисков и затрат могут конкурировать с законопослушными майнерами.

Ущерб, который наносит криптоджекинг сильно недооценен, на данный момент только часть действительно опасных майнеров распознаются системами защиты, как вредоносное ПО, в связи с тем, что сами по себе майнеры – легальные приложения. Кроме того, код часто настолько индивидуализирован и безобиден, что сканеры и антивирусы не могут обнаружить угрозу.

Актуальность данной проблемы очевидна. С каждым годом количество жертв криптоджекинга увеличивается. Так, согласно исследованию компании SonicWall, работающей в сфере информационной безопасности, угроза скрытого майнинга в первой половине 2022 года достигла рекордного уровня: число выявленных атак выросло до 66,7 млн, что на 30% больше, чем за первые шесть месяцев 2021 года.

Глава 1. История появления майнеров-троянцев и принцип их работы.

1.1 История появления криптоджекинга

Явление скрытого майнинга обрело массовость в 2016-2017 годах. Несмотря на это, еще в 2011 году Symantec – компания из Калифорнии, специализирующаяся на разработке ПО в области ИБ, впервые выявила новую угрозу — cryptojacking. В конце этого же года Kaspersky Lab выявляет первый троянец, предназначенный для скрытого майнинга. Затем в 2013 году с помощью уязвимости в Skype хакеры заразили огромное количество устройств майнер-ботом. Инфоповодом послужило и намеренное внедрение разработчиками в свой продукт µTorrent вредоносного ПО EpicScale.

В 2017 году криптоджекинг признан главной угрозой криптоотрасли. Так, группа Adguard сообщила об обнаружении свыше 33 тысяч сайтов со скриптами криптомайнинга. В феврале 2018 года Badpackets рассказали, что скрытым майнингом занимаются 34474 сайта, применяя для этого Coinhive – самый популярный майнер на JavaScript. Летом того же года Check Point Software Technologies сообщила, что четыре из десяти найденных вредоносов представляют собой крипто-майнеры, в том числе Coinhive и Cryptoloot.

В этом же году исследователи обнаружили ботнет Smominru cryptomining, заразившего более 500 тысяч машин в России, Индии и Тайване. Ботнет был нацелен на добычу криптовалюты Monero и предназначался для серверов Windows.

1.2 Основные принципы работы майнера и влияние ПО на устройство.

Для того, чтобы получать коины, компьютер должен задействовать все имеющиеся вычислительные мощности, поэтому зараженный ПК может использовать не только процессор, но и видеокарту, а также накопители. Даже непродолжительная работа устройства в подобном режиме может привести к перегреву компьютера или выходу комплектующих из строя.

Если для рядового пользователя проблемы с производительностью в большинстве случаев не понесут за собой какого-либо существенного ущерба, то для крупных компаний это может привести к большим проблемам.

От продажи одного скрытого майнера хакеры могут получить от $50 до $1000, в то время, как доход от криптоджекинга зависит от количества и производительности зараженных устройств. Так, для заработка около $100 в месяц, злоумышленнику достаточно заразить около 1000 ПК среднего ценового сегмента, но если майнеру удается попасть в мощный игровой ПК, то доход может увеличиться в несколько раз.

Помимо самого майнера, вредоносная программа может содержать дополнительные сервисы, которые помогают закрепиться в системе и обеспечивают автозапуск и позволяют незаметно работать в фоновом режиме.

Такие сервисы могут:

- Деактивировать антивирусное ПО;
- Отслеживать запуск требовательного ПО или диспетчера задач;
- Проверять наличие майнера на носителе с целью его переустановки в случае деинсталляции.

1.3 Способы заражения и виды криптоджекинга

Наиболее простой способ заражения системы майнером – замаскировать зловред под бесплатное ПО. Проникнув в ОС, вирус устанавливает клиент, позволяющий подключится к майнинг-пулу для последующей добычи криптовалюты.

Есть распространенное заблуждение, что криптоджекинг ворует лишь электроэнергию и вычислительные мощности процессора. Тем не менее, имели место быть сценарии, при которых помимо установки майнера, запускаемый троян похищает персональные данные пользователя

В отличие от большинства других типов вредоносов, криптоджекинг практически не наносит вред компьютерам или данным жертв. Речь идет о краже ресурсов процессора. Однако в последнее время всё чаще используются гибридные сценарии, когда, помимо установки майнера, запускаемый троян похищает личные данные, пароли и т.д.

Вредоносное ПО может попасть на устройство жертвы посредством фишинговой атаки: хакер отправляет электронное письмо, в котором присутствует зараженный файл или ссылка, привлекающие пользователя, которые при запуске устанавливают криптомайнер.

Есть два основных вида криптоджекинга:

- На устройствах — зловред интегрирован непосредственно в систему под видом безвредного ПО. Это не мешает ему действовать как троян и использовать ресурсы ПК;
- В браузерах — майнинг-скрипт интегрирован в код веб-страницы или в рекламное объявление: посещая подобный сайт, пользователь непроизвольно запускает вредонос, который будет работать до тех пор, пока открыта вкладка.

Криптоджекинг в браузере является самым распространенным видом незаконного майнинга. Самая популярная программа Coinhive была обнаружена в сентябре 2017 года, и уже к декабрю стала топ-1 вредоносом этого типа. По состоянию на осень 2018 года скрипт использовался в 19% случаев, согласно отчета Check Point Software Technologies. Данный JavaScript может быть встроен в любой сайт: разработчики майнеров и владельцы веб-страниц делят прибыль в соотношении 30%/70% соответственно.

1.4 Частные случаи криптоатак

- **PowerGhost** – в отчете CyberThreatAlliance описывается PowerGhost – вредоносное ПО, использующее приемы фишинга для заражения

устройства. Способна воровать персональные данные и отключать антивирусное ПО, а также другие криптомайнеры, установленные в данной системе. Мог отслеживать положение курсора, а также приостанавливать процессы, что делает PowerGhost одним из самых скрытных ПО для криптоджекинга.

- **BadShell** – в материале Comodo Cybersecurity упоминается вирус, способный управлять процессами Windows: программа может внедриться в активную задачу, включая диспетчер задач, для противодействия защите системы.
- **Facexworm** – вредоносное расширение для Chrome, заражающее ПК при помощи уязвимости в Facebook Messenger. Замечено Лабораторией Касперского в 2017 году. Изначально Facexworm позиционировалсь как ПО для рекламы, однако позже стало известно о функциях, предназначенных для криптобирж, способных устанавливать майнеры без уведомления пользователя. Может перехватывать учетные данные для распространения на других сайтах.
- **WinstarNssmMiner** – майнер, обнаруженный 360 Total Security. Способен заменять атрибуты процесса svchost.exe на CriticalProcess. Это приводит к тому, что, при попытке удаления вируса, система выдает синий экран смерти.
- **CoinMiner** — проверяет наличие процесса AMDDriver64 в системах Windows. Имеет списки $malwares и $malwares2, в которых находятся названия процессов популярных криптомайнеров, что позволяет программе удалять конкурирующее ПО.
- **Криптомайнеры на GitHub** – злоумышленники копируют популярные проекты на GitHub и распространяют вредоносный клон на сайте, побуждая посетителей установить майнер под видом безвредной программы.

- **Использование уязвимости rTorrent** – F5 Labs обнаружили уязвимость rTorrent, которая позволяла заражать ПК пользователей криптомайнером. От данной уязвимости весьма просто защититься – достаточно запретить внешние подключения в rTorrent.
- **CoinHive Miner**— браузерный майнер, работающий на JavaScript, попадающий в систему в виде бесплатных расширений для браузера. Вирус способен задействовать до 90% мощности процессора и видеокарты устройства, перегревая и выводя их из строя. Исследователи из Trend Micro обнаружили CoinHive в рекламе на YouTube.

Глава 2. Методы борьбы с криптоджекингом

2.1 Как обнаружить криптоджекинг

Обнаружить ПО для скрытого майнинга весьма проблематично, так как простому пользователю будет тяжело обнаружить вирус, который может маскироваться под стандартные процессы. Однако существуют признаки, указывающие на наличие майнера в системе. Обнаружение криптоджекинга может оказаться затруднительным, поскольку этот процесс часто скрыт или выглядит как стандартная работа устройства. Однако существует три признака, на которые следует обратить внимание:

1. Возросшие счета за электричество

Работа персонального компьютера на повышенных мощностях приводит к повышенному энергопотреблению, что в свою очередь заметно влияет на показания счетчика.

2. Проблемы с автономностью устройства

Из-за большой нагрузки на комплектующие и возросшего энергопотребления страдает аккумулятор устройства, что приводит к проблемам с автономной работой система

3. Уменьшение производительности

Проблемы с производительностью и сбои в работе устройства возникают в связи с негативным влиянием майнера на комплектующие и операционную систему. Троттлинг, вылеты приложений, синие экраны смерти, все это – признаки того, что на устройстве зарабатывают деньги без ведома хозяина.

4. Проблемы с браузером

У систем, атакованных вредоносным ПО, часто возникают проблемы, связанные с выходом в Интернет. Это связано с тем, что майнер может перехватывать пакеты траффика и потреблять ресурсы ПК, что приводит к медленному запуску веб-страниц и перегруженному веб-браузеру.

5. Повышенные температуры устройства

Из-за того, что криптоджекинг использует максимум ресурсов, компьютер перегревается, что может привести к выводу комплектующих из строя, а в крайних случаях к возгоранию. Высокие обороты кулера компьютера также могут указывать на неисправность системы.

6. Некорректная работа диспетчера задач

Посторонние процессы в диспетчере задач, исчезновение базовых процессов системы и их некорректное расположение, а также аномально большая нагрузка на процессор или видеокарту.

7. Инпут-лаг устройств ввода.

В связи с тем, что некоторые майнеры могут отслеживать положение курсора на экране, а также с большой нагрузкой на систему может происходить существенная задержка между вводом и выводом данных.

2.2 Как защититься от криптоджекинга

Скрытые майнеры являются неоспоримой угрозой для любого персонального компьютера, не защищенного должным образом. В данном разделе будут рассмотрены методы противодействия заражению майнером. И хоть рассмотренные в индивидуальном порядке меры не способны обеспечить

абсолютную защиту, совокупность этих мер способна снизить риск заражения в десятки раз.

В связи с тем, что практически каждый день появляются новые уязвимости и вредоносное ПО, а также способы заражения системы, именно поэтому необходимо изучать актуальную информацию о криптоджекинге и новых уязвимостях. Эта мера безопасности поможет не только избежать непредвиденных ошибок и понять устройство программ-майнеров, но и позволит избежать угроз информационной безопасности других видов.

- Существуют расширения для браузера, позволяющие блокировать скрипты майнинга на различных сайтах, это сделает интернет-серфинг гораздо более безопасным.
- Блокировщики рекламы позволяют не только избавиться от надоедливых объявлений, но и пресечь попытки злоумышленников доставить вредонос на вашу систему.
- Один из радикальных методов борьбы с криптоджекингом – отключение JavaScript, на котором написано большинство скрытых майнеров. К сожалению, отключение JS может привести к некорректной работе нужных сервисов.
- Необходимо устанавливать расширения и приложения только из официальных источников, не посещать подозрительные сайты и не переходить по подозрительным ссылкам.

Заключение

Очевидно, что анонимность и доступность криптовалют, а также неосведомленность пользователей в сфере информационной безопасности позволяют киберпреступникам обогащаться незаконным путем за счет малограмотных посетителей веб-страниц, трекеров и приложений.

В данной работе были рассмотрены основные виды майнеров, принцип их работы и примеры криптоджекинг-атак, а также методы противодействия таким атакам.

Несмотря на то, что получить гарантированную защиту от теневого майнинга не представляется возможным, ряд мер по укреплению информационной безопасности системы позволяет частично обезопасить себя от атак подобного рода.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Cryptojacking Threat Continues to Rise https://www.darkreading.com/threat-intelligence/cryptojacking-threat-continues-to-rise Дата обращения: 19.10.22
2. SONICWALL 2022 CYBER THREAT REPORT https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2022-cyber-threat-report.pdf Дата обращения: 19.10.22
3. Хавьер Мертенс: «Криптоджекинг – одна из самых блестящих атак, которые я видел» https://habr.com/ru/post/358674/ Дата обращения: 19.10.22
4. Cryptojacking surges in popularity growing by 31% over the past month https://adguard.com/en/blog/november_mining_stats.html Дата обращения: 20.10.22
5. July’s Most Wanted Malware: Attacks Targeting IoT and Networking doubled since May 2018 https://blog.checkpoint.com/2018/08/15/julys-most-wanted-malware-attacks-targeting-iot-and-networking-doubled-since-may-2018/ Дата обращения: 20.10.22
6. Cryptominers. Part 2 https://blog.checkpoint.com/2017/10/23/crypto-miners-part-2/ Дата обращения: 20.10.22
7. THE ILLICIT CRYPTOCURRENCY MINING THREAT https://cyberthreatalliance.org/wp-content/uploads/2018/09/CTA-Illicit-CryptoMining-Whitepaper.pdf Дата обращения: 21.10.22

8. Here’s What I Learned From the Latest Comodo Cybersecurity Global Threat Report https://blog.comodo.com/cybersecurity/comodo-cybersecurity-quarterly-global-threat-report/ Дата обращения: 21.10.22

9. CryptoMiner, WinstarNssmMiner, Has Made a Fortune By Brutally Hijacking Computers https://blog.360totalsecurity.com/en/cryptominer-winstarnssmminer-made-fortune-brutally-hijacking-computer/ Дата обращения: 21.10.22

10. rTorrent Client Exploited In The Wild To Deploy Monero Crypto-Miner https://www.f5.com/labs/articles/threat-intelligence/rtorrent-client-exploited-in-the-wild-to-deploy-monero-crypto-miner Дата обращения: 21.10.22

11. Google’s DoubleClick Abused to Deliver Miners https://www.trendmicro.com/en_us/research/18/a/malvertising-campaign-abuses-googles-doubleclick-to-deliver-cryptocurrency-miners.html Дата обращения: 21.10.22

12. Mining Is The New Black https://securelist.com/mining-is-the-new-black/84232/ Дата обращения: 21.10.22

Шульга А.А.,

студент 1 курса Крылов Григорий Олегович, МТУСИ, профессор, д.ф-м.н.

КВАНТОВЫЙ КОМПЬЮТЕР

1. Традиционный ПК – принцип работы

Для того, чтобы разобраться в работе КК, давайте сначала рассмотрим принцип работы традиционного ПК, работающего на основе кремневых чипов [1].

Основой компьютера является материнская плата, к которой подключены остальные устройства. От конфигурации материнской платы зависит и то, сколько дополнительных устройств может быть подключено к компьютеру.

BIOS расшифровывается как “Basic Input/Output System” («Базовая Система Ввода/Вывода») и является микропрограммой, которая хранится на чипе материнской платы компьютера [9].

1.1 Процессор

Процессор, «мозг компьютера» - электронный блок либо интегральная схема, исполняющая машинные инструкции. Центральный процессор выполняет все вычислительные операции в компьютере. На мониторе компьютера мы видим картинки, фотографии, текст, можем слушать музыку через колонки. Но для компьютера всё это - вычислительные операции, он работает только с числовыми значениями, для него существуют только цифры и наборы цифр.

Сам процессор состоит из десятка миллионов транзисторов, при помощи которых собраны отдельные логические схемы, находящиеся в специальном кремниевом корпусе.

В основе внутренних схем процессора лежит арифметико-логическое устройство, внутренняя память и кеш-память, которые в свою очередь образуют ядро процессора, а также схемы для управления всеми операциями и схемы управления с внешними устройствами – шинами.

1.2 Бит

Бит — единица измерения количества информации [2]. 1 бит информации – это символ или сигнал, способный принимать только одно значение из двух: true / false. В двоичной системе исчисления это 1 или 0.

2. Квантовый компьютер – принцип работы и его применение

Квантовый компьютер — устройство, которое использует явления квантовой механики, такие как квантовая суперпозиция, квантовая запутанность для передачи и обработки информации.

Квантовый компьютер применяет для вычисления не классические алгоритмы, а процессы квантовой природы - квантовые алгоритмы, использующие эффекты квантовой механики, такие как квантовый параллелизм и квантовая запутанность.

2.1 Кубит

Кубит — это специальный квантовый объект, настолько маленький, что уже подчиняется законам квантового мира. В то время, как бит может принимать положение либо нуля, либо единицы, кубит способен находиться в так называемой суперпозиции между данными значениями, то есть одновременно в значении нуля и единицы [3]. Ну а точнее, суперпозицию состояний можно представить себе, как то, что в каждый момент времени у квантового объекта есть определенные

вероятности «схлопнуться» в каждый из своих граничных уровней. Состояние кубита описывается уравнением (1) [4].

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \qquad (1)$$

где $|\psi\rangle$ – описываемое состояние кубита;

$|0\rangle$, $|1\rangle$ – базовые состояния кубита, соответствующие состояниям 0 и 1 классического бита;

α, β – комплексные числа, описывающие амплитуды соответствующих состояний кубита.

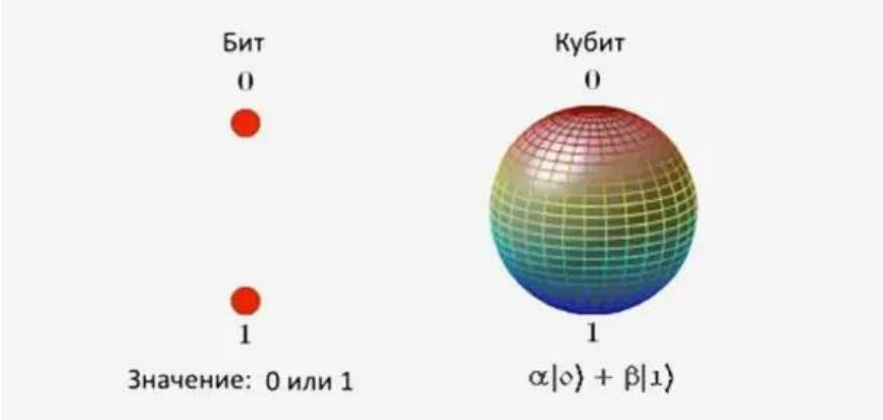


Рис. 1 Внешний вид бита и кубита [10].

Для выполнения вычислений на квантовом компьютере необходимо привести во взаимодействие несколько кубитов, причем таким образом, чтобы они образовали единую квантовую систему.

С ростом числа объединенных кубитов в квантовую систему, вычислительная мощность такой квантовой системы растет в прогрессии. Теоретически это позволяет квантовому компьютеру справляться с задачами, на которые обычному цифровому компьютеру понадобятся миллионы лет.

2.1.1 Свойства кубита

Кубит — объект квантового мира, который проявляет квантовые свойства:

- Имеет определенное состояние с двумя граничными уровнями.
- Находится в суперпозиции своего состояния до момента измерения.
- Связывается с окружающими квантовыми объектами для создания квантовых систем.

Чтобы понять свойства квантового объекта, рассмотрим каждое подробнее. Для наглядности и доступности, будем использовать пример из реальной жизни: самую обычную монету и систему, в которой эту монету подбрасывают.

- Монета имеет сторону, которая способна принимать два граничных уровня – «орел» и «решка».
- Если монету подбросить, то в момент вращения невозможно сказать, в какой позиции в данный момент она находится. Но если в момент вращения ее взять в руку, после чего посмотреть, то суперпозиция состояний тут же превращается в одну из двух граничных, а именно в «орел» или «решку».
- Допустим, мы подбросили три монетки так, что в воздухе они цепляются друг за друга, создавая некую систему. В каждый момент времени не только одна из них находится в суперпозиции состояний, но эти состояния взаимно влияют друг на друга, создавая общую суперпозицию.

Любой объект, для которого выполняются данные свойства и который мы можем создать, может использоваться как носитель информации в квантовом компьютере.

2.1.2. Квантовая система

Квантовая система — система запутанных квантовых объектов, обладающая следующими свойствами:

- Квантовая система находится в суперпозиции в каждый момент своего существования относительного каждого возможного варианта состояния отдельного объекта;
- Состояние системы до момента ее измерения нельзя узнать;
- В момент измерения система реализует один из возможных вариантов своих граничных состояний [5].

2.2. Применение квантового компьютера. Криптография

В 1994 году ученый Питер Шор разработал первый квантовый алгоритм для разложения целого числа на простые множители. Даже для самых мощных современных компьютеров разложить число длиной в несколько сотен цифр на два простых множителя — невероятная по затратам времени задача. Именно на этом строятся самые современные системы шифрования и защиты информации [7].

Связь, основанную на передаче единичных микрочастиц, невозможно прослушивать, поскольку законы квантовой физики не позволяют измерить параметры микрочастицы, не исказив их. Это явление, известное как принцип наблюдателя. Попытка прослушать сигнал искажает сообщение.

Квантовые криптосистемы обычно используют «квантовую» линию связи для передачи одноразового ключа шифрования, который, в свою очередь, применяется для шифровки сообщения и трансляции по обычной линии связи. Так вот, в случае подозрения на прослушивание потенциально перехваченный ключ просто не используется, и передача важных данных идет, только если квантовая передача ключа прошла успешно [8].

3. Различия между КК и ПК

3.1 Квантовый компьютер – лампочка, а классический компьютер – свечка

И лампочка, и свеча излучают свет, но работают по разным принципам. Лампочка нуждается в одном источнике энергии, а свеча совершенно в другом. Так

же и в случае с компьютерами. Чтобы традиционный ПК стал мощнее, нужно: заменить процессор на более новый, поменять видеокарту, увеличить оперативную память, объем SSD накопителя. В случае с КК дело обстоит иначе: он обладает настолько мощной вычислительной мощью, что измерить ее практически невозможно.

3.2 Квантовый компьютер > несколько взаимосвязанных стационарных компьютеров по вычислительной мощности

Но тут речь идет конкретно о вычислительной мощности. Если ставится вопрос о 3D-моделировании, редактировании фотографий, просмотре видео, то самый обычный домашний ПК будет более практичным. Но если идет речь о сложных процессах, таких как прогнозирование погоды на Марсе или изучении сложных метеорологических явлений, то квантовый компьютер справится гораздо лучше. Для таких сложных вычислений даже несколько взаимосвязанных компьютеров окажутся слишком медленными и слабыми, нежели квантовый.

3.3 Чувствительность квантового компьютера

Эффективность обычного компьютера не будет изменяться в зависимости от внешних факторов: ветер на улице, громкий звук из проезжающей мимо машины. Самое главное для него – это мощные составляющие устройства. С квантовым компьютером дело обстоит иначе: для его работы необходимы идеальные условия. Каждая маленькая помеха, каждый всплеск или незначительный шум могут повлиять на правильное считывание суперпозиции. Но и не только это является его проблемой. Кубиты перестают находиться в суперпозиции, если наблюдать за ними. Можно сравнить это с получением подарка: пока подарок не открыт, вы можете прокрутить в голове тысячи вариантов того, что внутри, так и с Кубитами, но тут это либо 0, либо 1.

3.4 Телепортация данных или передача данных?

У обычного компьютера, когда файлы становятся большими, нужно увеличить объем диска или качество интернета. Квантовый же компьютер данные не передает, а телепортирует. Две разные квантовые частицы могут переплетаться так, что информация, хранящаяся в одной, будет идентична информации в другой – независимо от расстояния между ними [6].

Заключение

Рассмотрев принцип работы квантового компьютера, можно с легкостью понять, в чем он лучше традиционного компьютера. Он намного быстрее решает математические и логические задачи, гораздо быстрее способен перебирать различные комбинации чисел и символов, что полезно для применения в сфере информационной безопасности.

В области бытовых применений более практичным будет обычный цифровой компьютер, также он более устойчив в работе, нежели квантовый. Но если технология продолжит свое развитие, а различные «гиганты» информационной сферы, такие как Google, IBM или Amazon будут инвестировать в усовершенствование квантовых компьютеров, то в скором будущем мы увидим практичное, универсальное и мощное устройство, способное максимально быстро решать задачи различного вида и справляться с простыми бытовыми вещами.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Вычислитель/Начинающему пользователю ПК/Как работает компьютер и как он устроен [электронный ресурс]: https://dzen.ru/media/id/5b484380800a6800a9242246/nachinaiuscemu-polzovateliu-pk-

kak-rabotaet-kompiuter-i-kak-on-ustroen-5e0921c4d5bbc300b1029a24 (дата обращения 15.09.2022)

2. Словарь бизнес-терминов [электронный ресурс]: https://dic.academic.ru/dic.nsf/business/1576 (дата обращения 16.09.2022)

3. istishev/Что такое квантовый компьютер? Разбор/Что же такое кубиты? [электронный ресурс]: https://habr.com/ru/company/droider/blog/531708/ (дата обращения 17.09.2022)

4. Актаева А.У./Квантовая информатика: безопасность информации [электронный ресурс]: https://cyberleninka.ru/article/n/kvantovaya-informatika-bezopasnost-informatsii (дата обращения 19.09.2022)

5. kruegger/Как работают квантовые компьютеры. Собираем паззл [электронный ресурс]: https://habr.com/ru/post/480480/ (дата обращения 19.09.2022)

6. Andrey Ku/Квантовый компьютер против обычного компьютера/5 основных отличий [электронный ресурс]: https://bezopasnik.info/квантовый-компьютер-против-обычного/ (дата обращения 19.09.2022)

7. Hitecher/Как работает квантовый компьютер: простыми словами о будущем/ПРИМЕНЕНИЕ КВАНТОВЫХ КОМПЬЮТЕРОВ [электронный ресурс]: https://hitecher.com/ru/articles/how-does-a-quantum-computer (дата обращения 20.09.2022)

8. Serge Malenkovich/Квантовые компьютеры и конец безопасности [электронный ресурс]: https://www.kaspersky.ru/blog/kvantovye-kompyutery-i-konec-bezopasnosti/1989/ (дата обращения 24.09.2022)

9. Vladimir Mareev/Технический писатель/Что такое BIOS, как и в каких случаях им пользоваться? [электронный ресурс]: https://hetmanrecovery.com/ru/recovery_news/what-is-a-bios-how-and-when-to-use-it.htm (дата обращения 29.09.2022)

10. Фарид Мамедов/Квантовое превосходство съело чижика, или Когда нас поработит квантовый ИИ [электронный ресурс]: https://e-news-su.mirtesen.ru/blog/43464684587/Kvantovoe-prevoshodstvo-selo-chizhika,-ili-Kogda-nas-porabotit-k?nr=1&utm_referrer=mirtesen.ru (дата обращения 01.10.2022)

Потыкун Н. А.,
Юргпу(НПИ) им. М.И. Платова 10.05.02-ЗИСа-017, 5 курс
Potikun.nika@yandex.ru
Научный руководитель:
Косиченко Н. В.
ЮРГПУ(НПИ) им. М. И. Платова, Доцент кафедры ИБ, к.т.н., доцент
Kosichenkonv@mail.ru

СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

По данным Всемирной организации здравоохранения, количество людей, нуждающихся в психологической или психиатрической помощи, сейчас растет быстрее, чем число страдающих сердечно-сосудистыми и онкологическими заболеваниями.

Таблица 1.

Статистика различия заболеваемости в разных диагнозах.

Год	Заболевание психическими и психологическимирасстройствами (на 10.000 чел)	Заболевание онкологическими болезнями (на 10.000 чел)
2015	9,7	2,8
2016	9,8	3,0
2017	10,3	3,0
2018	10,7	3,0

Во время психологических консультаций наших бывших соотечественников, обратившихся за помощью в связи с различными проявлениями душевного неблагополучия (неврозы, депрессии, страхи, фобии и пр.), выясняется, что их

причиной часто является информация.

Средства массовой информации - телевидение, радио, Интернет, многочисленные печатные издания - ежедневно обрушивают на нас лавину самой различной информации, интересной, познавательной и... негативной, внушающей порой страх за нашу жизнь и жизнь наших близких. Не каждый человек может с этим справиться.

Источники опасности. В современном мире на первом месте среди источников информации находится телевидение, которое обладает неограниченными возможностями информационного воздействия. Зрительный (визуальный) канал является ведущим каналом получения информации из внешнего мира, более 90% информации получаем мы с его помощью. Десятки европейских, в том числе и русскоязычных, телевизионных каналов и радиостанций в своих выпусках новостей в первую очередь извещают нас о

новых человеческих трагедиях и гибели десятков, сотен, а то и тысяч людей, связанных с природными катаклизмами, терактами, техногенными катастрофами и авариями. В многочисленных сериалах и кинофильмах нам показывают ужасные сцены убийства, насилия и жестокости. Политические комментаторы постоянно делают мрачные прогнозы на будущее. Журналисты смакуют жуткие сенсационные подробности различных преступлений.

Возникла серьезная проблема влияния компьютеризации на психику человека, на его душевную организацию. Психологи отмечают серьезные изменения в познавательной и коммуникативной сферах личности человека, чья деятельность связана с использованием компьютера. Человек часто не в состоянии проверить достоверность получаемой информации, увлекаясь

«знаковой информацией», он теряет т.н. «смысловую чувствительность», у него появляется безучастность к происходящему в мире. Психологи и психиатры всерьез обеспокоены появлением интернет-зависимости, уводящей личность в виртуальный мир, когда человек страдает маниакальным стремлением часами

бродить по киберпространству, забывая о сне и еде. Особенно их волнует чрезмерное увлечение компьютерными играми - компьютерная игромания, увлечение общением через Интернет – чато-мания, от которых нередко трудно избавиться.

Негативную информацию человек получает не только через телевидение или Интернет. На концертах беснующихся поп-звезд и на дискотеках на молодежную, как правило, публику обрушиваются сверхдопустимые для слухового восприятия децибелы, в которых зачастую, кроме ритма и грохота, нет вообще никакой информации...

Общаясь с другими людьми, человек получает также не всегда приятную для него информацию. По каналу ОБС - часто распространяются различные сплетни и слухи, волнующие получателя информации. Наши встречи со знакомыми не всегда обходятся без рассказов о болезнях и других

неприятностях, произошедших с их родными и знакомыми... Бесконечны потоки негативной информации, от которых многие не знают, как защититься.

Современные информационные технологии, широко используемые СМИ, оказывают на человека воздействие, имеющее цель изменить его потребности, взгляды, социальную ориентацию в интересах тех, кто оплачивает эти средства массовой информации, власть, политические силы, коммерческие структуры и пр. При таком информационном воздействии происходит деформация психики человека, затрагивающая не только сферу его сознания, но и область бессознательного. Личность постепенно теряет свою индивидуальность, происходит ее зомбирование, она становится легко управляемой. Изменяются критерии добра и зла. Жестокость и насилие становятся привычными атрибутами жизни. Исчезают такие присущие человеку качества, как сочувствие, сострадание, сопереживание, терпимость. В конечном счете, всё это приводит к тому, что возникает бездуховность, появляется стремление обеспечивать только свое биологическое существование, пассивность становится нормой жизни. Поэтому неслучайно перед

человечеством встала острая проблема обеспечения его информационно-психологической безопасности. Информационно-психологическая безопасность личности – это определенная защищенность сознания и бессознательной сферы психики от вредных информационных воздействий, способных против воли и желания человека изменять его психологические характеристики и поведение. Как и какими средствами ее можно обеспечить?

Люди подвержены информационному воздействию по-разному. Это зависит от возраста, индивидуально-психологических особенностей личности, жизненного опыта. Часто СМИ при информационно-психологическом воздействии на человека используют не метод убеждения личности, при котором происходит активное осмысливание получаемой информации и ее принятие или неприятие в зависимости от приводимых аргументов, а метод внушения, при котором информация воспринимается человеком пассивно, при этом она не осмысливается, не перерабатывается.

Существуют различные приемы и техники внушения, позволяющие нужной информации проникать в глубины психики (в область бессознательного), минуя защитные барьеры сознания (известный «эффект 25- го кадра», например). Внушению в большей или меньшей мере поддаются все люди, но если человеку присущи такие личностные качества как безответственность, робость, доверчивость, тревожность, мечтательность, суеверность, религиозность, склонность к подражанию, подверженность влиянию мнения группы, толпы и т.п., он становится более внушаемым. Кроме того, физическое напряжение, недосыпание, утомление, сильное эмоциональное возбуждение, ощущение невостребованности, ненужности, оторванности, скука усиливают вероятность внушения. Восприимчивость к внушению со стороны СМИ снижается по мере приобретения жизненного опыта и научных знаний.

Для обеспечения информационно-психологической безопасности личности можно рекомендовать различные способы психологической защиты. Они позволяют

предотвратить или нейтрализовать негативное воздействие информации в различных ситуациях, например, масс-коммуникационных (получение информации через средства массовой коммуникации - СМК или СМИ), контакт-коммуникационных (получение информации во время массовых зрелищных мероприятий, на митингах, собраниях и пр.) и межличностных (получение информации при общении с людьми, во время бесед, встреч и пр.).

Способ защиты 1-й: «Уход» - увеличение дистанции, прерывание контакта, выход за пределы досягаемости информационного воздействия. Действия в различных информационных ситуациях могут быть такими:

-отключение определенных каналов СМИ (раздражающего канала телевидения, выход из Интернета и пр.), отказ от просмотра (прослушивания) конкретных теле-радиопрограмм;

-отказ от чтения некоторых газет, статей, рубрик и пр.;

-уход, под различными предлогами, с массовых зрелищных мероприятий: театра, концертного зала, кинотеатра и пр., митингов, собраний и др.;

-смена неприятной темы беседы, стремление не обострять межличностные отношения во время беседы, уклонение от встреч с теми, кто является источником неприятных переживаний, прерывание под различными предлогами встреч, бесед.

В некоторых случаях защита может выразиться в более резких формах – «изгнании» или «игнорировании».

При использовании способа «изгнание» средство или источник негативного информационного воздействия изгоняется (или вытесняется) из информационной среды (отказ от пользования телевизором или компьютером, отказ посещать театральные постановки или концерты и пр.).

«Игнорирование» предполагает невосприятие информации, котораязатрудняет или препятствует определенной деятельности человека, может спровоцировать

конфликт, вызвать негативные эмоции.

Способ защиты 2-й: «Блокировка» - контроль информационного воздействия, выставление психологических барьеров, ограждение психики от внешнего негативного информационного воздействия.

Действия, выполняемые при «блокировке»:

-критическое восприятие информации;

-эмоциональное отчуждение (восприятие негативной информации «без эмоций»);

-увеличение межличностного пространства – «зоны общения» во время беседы;

-использование «психологических барьеров» (принижение источника информации, внутреннее осмеяние, развенчание авторитета, несерьезное восприятие информации, недоверие, настороженность, невнимательность, отвлечение и переключение внимания на другие объекты, не связанные с содержанием информационного воздействия и пр.).

Способ защиты 3-й: «Управление» - контроль процесса информационного воздействия, влияние на его характеристики и источник. Выполняемые действия:

-использование обратной связи (участие в опросах рейтинга популярности определенных каналов или программ телевидения, популярности периодических изданий и пр.);

-выражение в зрелищных мероприятиях своего отношения к происходящему (неодобрения, недовольства выступающими);

-использование при беседе принципа «своих не обижают», для чего продемонстрировать желание стать другом, членом одной общности; ослабить или дестабилизировать активность собеседника неожиданным отвлечением (например, сделать комплимент, высказать сочувствие) и др.

Способ защиты 4-й: «Затаивание» - контроль своей реакции на внешнее

информационное воздействие. Выполняемые действия:

-отсрочка своих реакций, поспешных выводов и оценок, задержка или отказ от действий и поступков, вызываемых информационным воздействием (например, при нахождении в толпе, чтобы не поддаться «эффекту толпы»,психическому заражению и не совершить поступков, о которых потом можнобудет сожалеть);

-маскировка, сокрытие чувств, проявлений эмоций и др.

Умение человека в зависимости от ситуации воспользоваться тем или иным способом психологической защиты от негативного воздействия информации способствует формированию его информационной культуры, которая, в конечном счете, и обеспечит информационно-психологическую безопасность личности. Кроме того, для того чтобы успешно решать будущие проблемы, должна производиться разработка эффективных стратегий по охране психического здоровья, поддерживаться с помощью различных психологических и психиатрических тренингов, которые будут помогать людям не подвергаться внешнему воздействию. В ходе обсуждения проделанной работы обычно возникает важная для тренинга идея, что для борьбы со стрессом и эмоциональным выгоранием необходима общая коллективная работа. Соблюдение правил коммуникации, вежливость, взаимоуважение и взаимопомощь, а для этого надо быть внимательным, наблюдательным,восприимчивым и заинтересованным.

Участники группы тренинга со своим куратором более открыто говорят отом, что в рабочей среде вызывает у них дискомфорт, более искренне высказывают свои наболевшие проблемы, разрешают затяжные конфликты.

Придумываются новые способы борьбы со стрессом, эмоциональным выгоранием и прокрастинацией.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. https://cyberleninka.ru/article/n/statistika-zabolevaemosti-psihicheskimi-rasstroystvami-v-rossiyskoy-federatsii/viewer
2. https://www.who.int/ru
3. https://www.partner-inform.de/partner/detail/2007/6/272/2445/informacionnopsihologicheskaja-bezopasnost-lichnosti?lang=ru
4. Тренинг для персонала "профилактика эмоционального выгорания" | HR-elearning- современные тренды управления, обучения, оценки, мотивации персонала
5. Информационно-психологические воздействия (psyfactor.org)
6. https://moluch.ru/archive/288/65050/
7. https://cyberleninka.ru/article/n/oblasti-primeneniya-informatsionno-psihologicheskogo-vozdeystviya
8. http://www.evartist.narod.ru/text24/0001.htm
9. https://www.mediagram.ru/netcat_files/108/110/h_1eaef80e566efbfa041bafd712f9b13c
10. https://cyberleninka.ru/article/n/informatsionno-psihologicheskoe- vozdeystvie-na-massovoe-soznanie-v-usloviyah-novoy-politicheskoy- realnosti

НАУЧНАЯ СЕКЦИЯ

«Кибербезопасность автоматизированных и компьютерных систем»

Руководитель: **Симонян Айрапет Генрикович**,
Московский технический
университет связи и информатики,
доцент кафедры «Информационная
безопасность», кандидат
технических наук, доцент

Ананьев В.А., Гладких Е.А., Наточий Н.М.,
Курганский государственный университет
Безопасность информационных и автоматизированных систем, 2 курс
ananyev_2002@mail.ru
Научный руководитель:
Иванов Д.С.,
Курганский государственный университет, ассистент
daniil_ivanov_97@mail.ru

CSRF-АТАКИ И МЕТОДЫ ЗАЩИТЫ ОТ НИХ

В многообразии опасностей, которые поджидают в интернете, можно выделить атаки на данные пользователей, одной из которых является CSRF (Cross-Site Request Forgery). Она использует файлы-Cookie данные для того, чтобы выполнять действия злоумышленника от лица владельца. Для того чтобы стать жертвой CSRF атаки пользователю достаточного перейти по «зараженной» ссылке, о чем он может даже не подозревать. Находясь на «плохом» сайте, используя сессионные Cookie, от лица пользователя автоматически формируется и отправляется POST-запрос. В результате чего злоумышленник может выполнять такие действия, как смена пароля или email почты, для смены владельца аккаунта, отправка сообщений, перевод денег со счета на счет и т.д. [1]

По мнению проекта OWASP Top 10 в 2017 году уязвимость приложений от CSRF-атак занимала седьмое место, а в списке слабых сторон ПО в рейтинге CWO Top 25 на 2022 год она находится на девятой строчке рейтинга, что дает понимание об её актуальности. [2] Для того, чтобы обезопасить данные пользователей, создатели веб–сайтов используют ряд решений, таких как:

1. Использование токенов;
2. Применение SameSite атрибута;

3. Использование заголовков Origin и Referer;

4. Создание пре-сессий;

5. Подтверждение запроса капчей или кодом;

6. Применение двухфакторной аутентификации.

Рассмотрим эти методы по порядку, начиная с самого распространённого – использования токенов. Для каждого запроса сервер генерирует секретный ключ, который передается пользователю через API. Продолжительность жизни такого кода – небольшой период времени или одна операция. При получении запроса, сервер сверяет свой токен с полученным, в результате чего происходит проверка отправителя запроса. Мошенник не сможет провести атаку, так как он не будет знать ключ. [3]

В целях обеспечения большей безопасности и ненадобности хранения кодов аутентификации на стороне сервера прибегают к использованию double submit Pattern. Преимуществом данного метода является использование двух токенов: один содержится в Cookies файлах, другой – в одном из параметров запроса. При выполнении запроса происходит сравнение ключей. В случае, если они не совпадают, то сервер протоколирует и отклоняет запрос. [4]

Иногда возникает проблема, что приложение не использует HTTPS, в таком случае злоумышленник способен перехватить сетевые пакеты и увидеть токен в виде обычного текста. Самым простым решением данной уязвимости является использование HTTPS и защищенных Cookie. Примером является официальный вебсайт спортивного канала ESPN на 10 мая 2019 года передавал файлы-Cookie авторизации через незащищенный HTTP.

Чтобы избежать уязвимости к CSRF-атакам, а также XSS угрозам, не следует сохранять токены локально на устройстве. Злоумышленник может внедрить в запущенное в браузере приложение JavaScript-код, который передаст коды своему хозяину. Однако предотвратить эту проблему можно, используя флаг HttpOnly или Secure Cookies, что ограничит доступ к файлам.

В том случае, если злоумышленник получит управление над сервером или к базой данных путем атаки на нее, то он может овладеть не только действующими токенами, но и JWT/SSL ключом, что является более серьёзной угрозой. Имея эту информацию можно легко перехватывать сессии. Защититься от этой угрозы можно, храня в базе данных только хэшированные токены авторизации. При утере закрытого ключа требуется немедленно изменить его и аннулировать все текущие JWT.

При достаточных вычислительных ресурсах злоумышленник может случайным перебором угадать токен авторизации. Защитой от этого является применение длинных токенов с высокой энтропией.

Следующий метод защиты от CSRF-атак – использование SameSite Cookie. Применяя данный атрибут, мы контролируем отправление файлов с данными на запросы со сторонних ресурсов. SameSite имеет три значения: None, Strict и Lax. None – отправляет Cookie по запросу любого источника, Strict – отвечает только внутрисайтовые запросы, а Lax – сохраняет баланс между безопасностью и удобством, не блокируя обращения пользователей, совершенные надежным способом – через Https протокол. Однако не стоит использовать SameSite, как единственный способ защиты от CSRF-атак, так как множество старых версий браузеров не совместимы с данным атрибутом. Однако в наше время ряд популярных браузеров нацелены на обеспечение безопасности пользователей, например в Chrome, начиная с 76 версии появился флаг same-site-by-default-coolies, который в случае отсутствия выставленного атрибута SameSite, автоматически указывает значение Lax. [5]

Еще одним способ защититься от CSRF-атаки является чтение HTTP-заголовков Origin и Referer. Серверная часть сайта проверяет заголовки, если хранящиеся там значения совпадают с ресурсом, то такой запрос считается валидным. В случае, если эти данные отсутствуют, то следует отклонять и

сохранять в журнал. Для того, чтобы избежать даже небольшой потери трафика, следует считать запросы с одним отсутствующим заголовком корректными. [6]

Однако, чтобы сессионные данные клиента не были скомпрометированы на входной форме, организации Google и PayPal разработали следующий метод. [7] Он заключается в создании пре-сессии, которая позволяет пользователю получить токен для аутентификации, что для злоумышленника, не имеющего сведений об авторизационной информации, делает недоступным доступ к чужой учетной записи. [8]

Следующим средством защиты является использование капчи. Применяя её или высылая код подтверждения, мы сможем противостоять CSRF-атакам, но данный метод не стоить использовать для каждого запроса. Это обусловлено тем, что работа в такой системе окажется чрезмерно осложнена. Применять подтверждение капчей следует только определенные команды, такие как запрос на перевод денежных средств или на смену пароля. Данный метод используется, например, в сервисах Google при редактировании аккаунтов, а также при настройке их на новых устройствах.

Также для защиты от рассматриваемой атаки применяют двухфакторную аутентификацию. Она является методом идентификации пользователя при помощи данных разных типов, что обеспечивает эффективную защиту от несанкционированного доступа (НСД). Такие комбинации состоят из двух компонентов первый – логин и пароль, а второй: SMS–сообщения (приложение Сбербанк Онлайн), PUSH–уведомления (ВТБ онлайн), электронные письма (приложение онлайн-магазина Ozon и ВКонтакте), специальные USB–ключи, NFC–устройства и биометрия (ITunes Store, App Store и Apple Books [9]). [10]

Выше перечисленные методы защиты применяются при условии отправки пользователем POST-запросов. В качестве альтернативы, и как еще один способ защиты, применяются AJAX–запросы.[11] Их преимущество заключается в том, что создается временное Cookie, прочитать которую может только JavaScript,

находящийся в том же домене, не зависимо от того, является ли эта форма авторизации или регистрации статической или сгенерирована динамической генерацией. [12]

В заключение можно отметить, что в хоть в наше время все больше разработчиков веб-приложений заботятся об обеспечении защиты от CSRF-атак, но сама проблема никуда не исчезла, злоумышленники постоянно находят новые уязвимости в протоколе HTTP. Поэтому стоит придерживаться ряда правил, для обеспечения безопасности от CSRF–атак:

- Не переходить по ссылкам, предложенными незнакомыми третьими лицами;
- При использовании токенов, они должны соответствовать основным требованиям безопасности: иметь кратковременный период жизни, быть устойчивым к атакам полного перебора (brute force), создаваться надежным криптографическим генератором, храниться в базах данных в зашифрованном или хэшированном виде;
- Для обеспечения безопасности не стоит обходиться реализацией только одного из перечисленных методов. Защитой не стоит пренебрегать, так как комплексная защита является более эффективной;
- Не следует злоупотреблять применением капчей для подтверждения запросов в связи с увеличением нагрузки на пользовательское устройство;
- Устанавливать защиту от XSS–атак позволяет усилить безопасность веб-страниц от CSRF–угроз;
- Чтобы обезопасить свои данные, по возможности, необходимо пользоваться последними версиями браузеров, так как в них реализованы новые методы защиты информации пользователя.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Межсайтовая подделка запроса: защита от CSRF атак [электронный ресурс] Режим доступа: https://tproger.ru/articles/mezhsajtovaja-poddelka-zaprosa-zashhita-ot-csrf-atak/

2. 2022 CWE Top 25 Most Dangerous Software Weaknesses [электронный ресурс] Режим доступа: https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html

3. Как обеспечить безопасность токенов аутентификации [электронный ресурс] Режим доступа: https://tproger.ru/translations/user-session-security/

4. Cross-Site Request Forgery Prevention Cheat Sheet [электронный ресурс] Режим доступа: https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html

5. Объяснение SameSite атрибута файлов cookie [электронный ресурс] Режим доступа: https://web.dev/i18n/ru/samesite-cookies-explained/

6. CSRF-атака или межсайтовая подделка запроса [электронный ресурс] Режим доступа: https://jino.ru/journal/articles/csrf-ataka/

7. K. Sentamilselvan Cross-Site Request Forgery: Preventive Measures / S. Lakshmana Pandian, N. Ramkumar // International Journal of Computer Applications Volume 106. – 2014. – №. 11. – С. 20-25.

8. Шпаргалки по безопасности: CSRF [электронный ресурс] Режим доступа: https://habr.com/ru/company/acribia/blog/476880/

9. Использование Touch ID на iPhone и iPad [электронный ресурс] Режим доступа: https://support.apple.com/ru-ru/HT201371

10. Двухфакторная аутентификация: что это и зачем оно нужно? [электронный ресурс] Режим доступа: https://www.kaspersky.ru/blog/what_is_two_factor_authenticatio/4272/

11. Атака CSRF [электронный ресурс] Режим доступа: https://learn.javascript.ru/csrf

12. Защита ajax-приложения от Cross Site Request атак (CSRF) [электронный ресурс] Режим доступа: https://habr.com/ru/post/144406/

Баулина А.А.,
ЯрГУ им. П.Г. Демидова, компьютерная безопасность, 5 курс,
annika10@list.ru
Научный руководитель:
Мурин Д.М.,
ЯрГУ им. П.Г. Демидова,
директор института информационной безопасности, к. ф.-м.н.,
nirum87@mail.ru

СПОСОБЫ ЗАЩИТЫ ОТ УЯЗВИМОСТЕЙ В ЯЗЫКЕ JAVA

Сериализация — это процесс преобразования объекта в поток байтов для сохранения или передачи в память, базу данных или файл [1]. К сожалению, нельзя слепо полагаться на встроенные механизмы сериализации, которые есть во всех распространенных языках программирования. По данным Национальной базы данных уязвимостей США с начала 2022 года было зарегистрировано уже более 80 уязвимостей, возникших в процессе десериализации в различных программных продуктах. В том числе, например, уязвимость в Cisco Webex Meetings, позволяющая злоумышленнику внедрить вредоносный код в приложение [2]. Цель настоящей работы – исследование процесса сериализации и обеспечение его безопасности.

Для сериализации объекта – его преобразования в последовательность байтов – он должен быть экземпляром класса, реализующего интерфейс Serializable (маркерный интерфейс без методов). При десериализации JVM пытается восстановить объект, создавая его новый экземпляр в куче, при этом конструктор класса не вызывается. Экземпляр класса инициализируется с помощью вызова скрытого конструктора без параметров, затем открытые и закрытые поля класса заполняются с использованием отражения; сеттеры не вызываются. Переходным

переменным присваивается пустое значение или значение по умолчанию (для ссылок на объекты и простых типов соответственно) [3-5].

Приведем пример уязвимости процесса десериализации. Допустим, веб-приложение общается с сервером через REST API и для передачи данных объектов используется сериализация. Это позволяет серверу обрабатывать полученные данные так, как будто это и есть оригинал объекта. Таким образом, весь трафик между приложением и сервером основан на передаче сериализованных объектов. Это дает ложное чувство безопасности: весь трафик – это не удобочитаемые потоки байтов, сразу не видно, какие данные передаются. На самом деле этот код подвержен атаке. Эта уязвимость существует, потому что при десериализации объекта отсутствует какая-либо валидация. JVM никак не может проверить, что объект имеет такое же внутреннее состояние, как и в момент сериализации. Вся информация доступная в момент десериализации — это только информация, содержащаяся в потоке. Если изменить содержимое потока, то Java слепо доверится ему.

В Java валидность и ограничения, наложенные на параметры, обычно проверяются в конструкторе во время создания Objecttype. Но эта проверка не пригодна для обеспечения большей безопасности десериализации. В процессе десериализации экземпляр класса инициализируется с помощью вызова скрытого конструктора без параметров, затем открытые и закрытые поля класса заполняются с использованием отражения; сеттеры не вызываются. Поэтому валидация может быть применена в геттере – даже если злоумышленник задаст открытое или закрытое поле непосредственно в сериализованном объекте, его значение будет проверено до того, как будет доступно для использования JVM. Стоит заметить, что это решение не идеально – вредоносный объект всё еще будет существовать в JVM и вызовет ошибку при первом же использовании.

Для обхода защитных механизмов, применяемых в процессе сериализации, может быть использовано отложенное выполнение – исполнение кода в момент

зачистки объекта. С этой целью используется метод Object.finalize(). Вредоносный код, расположенный в одноименных функциях объектов, исполняется сборщиком мусора, когда объект уже больше не используется.

Отложенное выполнение основывается на инициализации объекта в процессе десериализации. Даже если в процессе приведения типов будет сгенерированоClassCastException, будет уже поздно. Объект станет целью сборщика мусора, а тот, в процессе «зачистки», вызовет метод finalize(), таким образом исполняя вредоносный код.

В процессе изучения разных источников ([6-10]) и исследования процесса десериализации были найдены следующие решения, которые должны уменьшить уязвимость ПО:

1. Ограничить использование сторонних библиотек, оставив лишь самые необходимые.
2. Переопределять методы readObject() и writeObject() в классах, которые наследуют интерфейс Serializable, так, чтобы они генерировали NotSerializableException.
3. Вести чёрный список, определяющий классы, которые не должны быть десериализованы. Ведение черного списка относится к негативной модели безопасности: «Что не запрещено – то разрешено». Такие модели легко внедрить в существующий проект, но злоумышленники всегда оказываются на шаг впереди – новые уязвимости обнаруживаются каждый день, и невозможно отследить их все.
4. Вести белый список. Противоположный подход заключается в том, чтобы самостоятельно разрешать определенные классы. Все остальные по умолчанию запрещены. Белый список считается надежнее черного, но его сложнее поддерживать, особенно в больших enterprise-приложениях. Проблема белого списка в том, что многим вредоносным программам не нужны какие-то особые классы для успешной работы. DDoS атаки

проводятся и с помощью таких классов и структур как Array, HashMap, HashSet и Strings, которые обычно находятся в белом списке.

5. Использовать Adhoc Security Manager. Security manager в Java определяет политику безопасности, которая определяет, какие действия считаются небезопасными. Если в процессе исполнения кода вызывается небезопасное действие, генерируется SecurityException. Класс ObjectInputStream проверяет, установлен ли менеджер безопасности, если да – вызывает его метод checkPermission. В нём проверяется SerializablePermission("enableSubclassImplementation"), показывающее, разрешен ли класс-наследник ObjectInputStream. Недостаток этого подхода в том, что злоумышленник может обойти ограничения security manager, например, с помощью отложенного выполнения. Если выполнение вредоносного кода будет происходить уже после десериализации, security manager перестанет выполнять свои обязанности к этому моменту.
6. Необходимо тщательно проверять права, применяющиеся к десериализации, при наличии security manager. Например, некоторые несериализуемые классы с наследниками имеют конструкторы без аргументов, допустим, ClassLoader. Пусть существует вредоносный сериализуемый класс, который является наследником Class Loader. Как мы знаем, в процессе десериализации вызывается конструктор без параметров, затем метод readObject(). В момент вызова конструктора Class Loader проверки безопасности пройдут, т.к. никакого непривилегированного кода в стеке нет. Именно поэтому данные должны быть десериализованы с наименьшими привилегиями.
7. Использовать Web Application Firewall (WAF). Для защиты процесса десериализации от гаджетов, WAF может использовать фильтр, который будет отсеивать все сериализованные объекты, содержащие уже известные вредоносные классы.

8. Использовать виртуализацию. В случае развертывания приложения в виртуальной среде, например, на виртуальной машине или в контейнере Docker, обеспечивается изоляция на уровне файловой системы, процессов и сети. Таким образом, даже в случае, казалось бы, успешной попытки злоумышленника достичь своих целей с помощью десериализации он не получает доступ к реальным данным, процессам и сети.
9. Использовать RASP. Runtime Application Self-Protection (RASP) - инструменты самозащиты приложения во время исполнения - развертываются на серверах приложения для перехвата всей коммуникации между клиентом и сервером, отслеживают потоки данных, поведение пользователей, паттерны в структурах данных и объектах, чтобы составить образ нормального поведения пользователя. Нестандартное поведение расценивается как потенциальная угроза. Инструменты RASP в диагностическом режиме могут использоваться для оповещения команды о попытках атаки.
10. Скрывать важную информацию. Предположим, что какой-то класс содержит важную информацию, например, возраст человека. В таком случае можно в методе writeObject применить битовый сдвиг влево, а в методе readObject - вправо соответственно. В таком случае, даже при перехвате данных злоумышленник не будет располагать достоверной информацией.
11. Относиться к десериализации как к созданию объекта. Кроме проверки в геттерах, валидацию можно производить в методе readObject(). Перед использованием объекта необходимо убедиться, что десериализация успешно завершилась, например, с помощью установки флага.

К сожалению, предложенные выше методы не гарантируют абсолютной безопасности процесса десериализации, потому что нельзя утверждать, что:

- данные не были изменены в процессе передачи (хранения);
- данные были отправлены доверенным лицом в случае передачи по сети.

В работе предлагается десериализовать данные исключительно из доверенных источников, проверяя их целостность. Именно поэтому реализуем элемент модели безопасности с нулевым доверием. Будем подписывать сериализованные объекты с помощью хеш-функции, проводя таким образом аутентификацию отправителя. Полученный поток байтов может быть проверен получателем перед началом процесса десериализации, чтобы максимально обезопасить код ПО. При проверке хеша можно сказать, был ли изменен изначальный объект. Кроме того, будем использовать шифрование для защиты конфиденциальности. Из приведенных рассуждений следует логичный вопрос: что делать сначала – подписывать или шифровать?

Предположим, сначала мы зашифровали объект, а потом подписали, поместив в SignedObject. В таком случае злоумышленник, перехватив SignedObject, может извлечь оттуда подпись, заменив на её свою собственную–это пример атаки посредника. Да, злоумышленник не сможет прочитать содержимое, но и получатель тоже (расшифровать сообщение можно только после проверки подписи). Адресат не может с уверенностью утверждать, что полученный объект был подписан именно отправителем.

Именно поэтому предлагается использовать следующий алгоритм:

- подписать пересылаемый объект с помощью алгоритма SHA3-512withDSA, поместив его в SignedObject;
- зашифровать SignedObject по ГОСТ 34.12-2018, используя симметричный алгоритм блочного шифрования “Кузнечик” [11].

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Serialization (C#) [Электронный ресурс]. – Режим доступа : https://docs.microsoft.com/en-us/dotnet/csharp/programming-guide/concepts/serialization.
2. NIST [Электронный ресурс]. – Режим доступа : https://nvd.nist.gov/vuln/search.

3. Сьерра Кэтти, Бейтс Берт. Изучаем Java [Текст] / Кэтти Сьерра, Бейтс Берт. – 2-е изд. – Москва : Эксмо, 2021. – 720 с. – ISBN 978-5-699-54574-2.

4. Эккель Брюс. Философия Java [Текст] / Брюс Эккель. – 4-е изд. – СПб : Питер, 2015. – 1168 с. – ISBN 978-5-496-01127-3.

5. Хорстманн, Кей С. Java. Библиотека профессионала [Текст]. В 2 т. Т. 2. Расширенные средства программирования / Кей С. Хорстманн ; перевод с английского М.В. Берштейна. – 11-е изд. – Москва : ООО «И.Д. Вильямс», 2020. – 864 с. – ISBN 978-5-907144-38-5.

6. Secure Coding Guidelines for Java SE [Электронный ресурс]. – Режим доступа : https://www.oracle.com/java/technologies/javase/seccodeguide.html.

7. Sudip Sengupta. Serialization in Java: Examples and Prevention [Электронный ресурс]. – Режим доступа : https://crashtest-security.com/java-serialization.

8. Ted Neward. Java Object Serialization [Электронный ресурс]. – Режим доступа : https://developer.ibm.com/articles/j-5things1.

9. How to protect your Apps from the Java Serialization Vulnerability [Электронный ресурс]. – Режим доступа : https://www.contrastsecurity.com/security-influencers/protect-your-apps-from-java-serialization-vulnerability.

10. Gorka Vicente. The Top 5 Reasons Why WAF Users Are Dissatisfied [Электронный ресурс]. – Режим доступа : https://hdivsecurity.com/bornsecure/the-top-5-reasons-why-waf-users-are-dissatisfied.

11. ГОСТ 34.12-2018. Информационная технология. Криптографическая защита информации. Блочные шифры [Текст]. – Взамен ГОСТ 28147—89 в части раздела 1 «Структурная схема алгоритма криптографического преобразования» ; введ. 2019-06-01. – Москва : Стандартинформ, 2018 ; М.: ИД «Юриспруденция», 2018. – 13 с.

Виноградов И. В., Волков Д. И.,
НИУ МИЭТ, Информационная безопасность, 3 курс,
ivanvinogradov1111@gmail.com, d.i.volkov2002@mail.ru
Научный руководитель:
Воеводин В. А.,
НИУ МИЭТ, доцент кафедры «Информационная безопасность», к. т. н.,
vva541@mail.ru

О ПРОБЛЕМЕ ВНЕДРЕНИЯ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА ПРИ РЕШЕНИИ ЗАДАЧ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ

Введение. В силу Федерального закона «Об информации, информационных технологиях и о защите информации» обладатель информации «обязан принять меры по защите информации» (ЗИ) [1, ст. 6]. Для управления ЗИ сегодня существует два основных подхода:

– первый – директивный, при котором Регулятор формирует требования к ЗИ, организует проверку их исполнения. Регулирование отношений осуществляется через институт ответственности за нарушения законодательства РФ об информации, информационных технологиях и о ЗИ. Парадоксально, но в этом случае основная угроза исходит от самого Регулятора;

– второй – риск-ориентированный: решение о допустимом уровне риска принимает владелец риска на основе оценки реальных угроз информационной безопасности (ИБ) и уязвимостей рубежей защиты. При внедрении этого подхода включается экономическая составляющая. В докладе акцентируется внимание на том, что современный технологический уклад в экономике все больше ориентируется на управление технологическими процессами через управление рисками [2, 3], чего нельзя сказать о технологии управления ИБ.

Цель доклада – сообщить о результатах исследования правовой (РФ), организационной и методической составляющих, препятствующих внедрению риск-ориентированного подхода к управлению ЗИ. Для достижения поставленной цели в докладе будут рассмотрены три вопроса, которые связаны с результатами анализа правового, нормативного и методического обеспечения процесса внедрения риск-ориентированного подхода к управлению ИБ.

Результаты анализа правового обеспечения

С одной стороны, ссодержательное исследование Федерального закона №149-ФЗ [1, ст. 16] позволяет сделать вывод о том, что государственное регулирование отношений в сфере ЗИ осуществляется путем установления требований о ЗИ, а также ответственности за их нарушение. Это означает, что основным регулятором названных отношений является директивный (административный), а не риск-ориентированный подход. Если же последний реализуется, то по остаточному принципу, что не соответствует современной тенденции развития технологического уклада экономики. Названное несоответствие препятствует внедрению страхования информационных рисков как экономического метода обеспечения ИБ, закрепленного в предыдущей Доктрине ИБ, утвержденной Президентом РФ в 2000 г. [4]. В действующей (новой) Доктрине ИБ [5] институт страхования информационных рисков вообще не обозначен. Аналогичная тенденция просматривается и при реализации федерального проекта «Информационная безопасность» Национальной программы «Цифровая экономика РФ. Так, в [6, p. 5.10] было закреплено, что в 2024 г. должны быть разработаны механизмы государственного содействия росту рынка услуг по страхованию информационных рисков, однако этот документ пережил много редакций, и в действующих редакциях [7, 8] положение о страховании информационных рисков полностью отсутствует, поэтому есть основания утверждать, что существующее положение дел не соответствует тенденции развития рынка страхования киберрисков, который

к 2025 г. должен составить порядка 20 млрд долларов [9]. Более того, названное несоответствие препятствует применению в практике управления ИБ положений УК РФ [10]. В ст. 41 «Обоснованный риск» УК РФ устанавливается, что не является преступлением причинение вреда охраняемым уголовным законом интересам при обоснованном риске для достижения общественно полезной цели. Внимание акцентируется на том, что риск признается обоснованным, если указанная цель не могла быть достигнута не связанными с риском действиями (бездействием) и лицо, допустившее риск, предприняло достаточные меры для предотвращения вреда охраняемым уголовным законом интересам. Для устранения данного несоответствия авторский коллектив намерен внести предложение по введению в ст. 16 [1] дополнения, суть которого заключается в том, что регулирование отношений основывается на целесообразном сочетании обязательных требований с элементами риск-ориентированного подхода.

Результаты анализа организационного обеспечения

Учитывая, что в силу Федерального закона «О стандартизации в Российской Федерации» от 29 июня 2015 г. № 162-ФЗ [11] национальные стандарты позиционируются как документы по стандартизации, в которых «для добровольного и многократного применения устанавливаются общие характеристики объекта стандартизации» [11, ст. 2], в рамках настоящего доклада национальные стандарты позиционируются, совместно с методиками оценки риска, как элемент организационного обеспечения. Результат исследования парка национальных стандартов [12–15], регулирующих управление рисками в области ЗИ, позволяет утверждать, что его возможности в основном способствуют внедрению риск-ориентированного подхода, при этом следует учитывать, что в ближайшее время (до полугода) можно ожидать новую редакцию стандарта ИСО/МЭК 27005–2022. С 2008 г. это будет четвертая редакция в Европе, в РФ

действует лишь вторая редакция (2012 г.), т. е. внедрение риск-ориентированного подхода к управлению ИБ в России идет со значительным запозданием.

Результаты анализа методического обеспечения

Дальнейшие рассуждения базируются на утверждении, что документы по стандартизации (стандарты), в силу закона [11], содержат общие характеристики объекта стандартизации, а также правила и общие принципы в отношении этого объекта, а методическое обеспечение остается за их рамками. В некоторых случаях элементы методического обеспечения содержатся в примечаниях к стандартам, что не может считаться полноценным методическим обеспечением для оценки риска ИБ. Названное методическое обеспечение должно быть стандартизировано, иначе оценки риска, полученные разными аудиторами, будут отличаться, что породит недоверие лица, принимающего решение, к этим оценкам и к самому оценщику. Методическое обеспечение внедрения риск-ориентированного подхода, в зависимости от методов моделирования объектов оценки, можно разделить на две группы:

– первая группа характеризуется тем, что имеется потенциальная возможность наблюдения за объектом оценки и получения репрезентативной статистики, ее обработки и разработки на ее основе вероятностной модели объекта оценки. Полученная вероятностная модель может использоваться для оценки риска ИБ [12–14]. В настоящее время имеется достаточный научный задел, позволяющий применять эти методы на практике;

– вторая группа характеризуется тем, что: а) риск связан с редкими событиями, для которых в принципе невозможно получить статистику; б) не представляется возможным зафиксировать саму обстановку для сбора статистики. Ретроспективный анализ доступной литературы по оценке рисков ИБ, связанных с наступлением редких событий, позволяет утверждать, что научный материал по этому направлению недостаточно развит и апробирован на практике. Данное

положение дел не позволяет внедрить национальный стандарт по страхованию информационных рисков [15]. Особенно остро стоит задача оценки риска ИБ для условий компьютерных атак, когда статистика о случайных процессах в принципе отсутствует и потоки повреждений нельзя, без грубых допушений, принять стационаными и эргодическими. В этом случае методы математической статистики дают существенные ошибки, которые не позволяют полноценно применить их на практике.

Постановка задачи. А) Определены исходные данные:

– атрибуты интенсивности (1) компьютерной атаки (КА):

$$\lambda = \{F(t), n\}, \quad (1)$$

где $F(t)$ – множество функций распределения (2) случайных интервалов времени η_i до очередной i-й КА:

$$F(t) = \{F_i(t)\}, \quad (2)$$

где $F_i(t)$ – функция распределения случайного η_i интервала времени до i-ой КА, $i = 1, 2, \ldots, n$, n – число КА;

– характеристики надежности и живучести (3) объекта информатизации (ОИ):

$$u = \{T_н, P\}, \quad (3)$$

где $T_н$ – наработка между отказами ОИ в нормальных условиях применения; P – множество вероятностей поражения ОИ (4) в результате КА:

$$P = \{P_i\}, \quad (4)$$

где P_i – вероятность поражения ОИ при i-й КА. Подход к определению вероятностей поражения с применением экспертных методов приведён в [16, 17, 18];

– варьируемые (изменяемые) характеристики восстанавливаемости ОИ (5):

$$r = \{T_в, G(t)\}, \quad (5)$$

где $T_в$ – прогнозируемый интервал времени восстановления (временная избыточность) после i-й КА (6); $G(t)$ – множество функций распределения случайных интервалов времени восстановления работоспособности (временной избыточности) после i-й КА (6):

$$T_в = \{\tau^{н}_{вi}, \tau^{в}_{вi}\}; G(t) = \{G_i(t)\}, \quad (6)$$

где $\tau^{н}_{вi}$ и $\tau^{в}_{вi}$ – нижняя и верхняя границы случайной величины времени восстановления ОИ $T_в$ после i-й КА соответственно. Порядок экспертной оценки $\tau^{н}_{вi}$ и $\tau^{в}_{вi}$ приведен в [16];

– требуемый для восстановления работоспособности ОИ после успешной КА ресурс (7):

$$R = \{T, r\}, \quad (8)$$

где T – допустимое (требуемое) время восстановления работоспособности ОИ; r – требуемый ресурс сил и средств для восстановления работоспособности ОИ;

– выделенный для восстановления работоспособности ОИ ресурс (8):

$$R_0 = \{T_0, r_0\}, \quad (8)$$

где T_0 – назначенное время для восстановления работоспособности ОИ;

r_0 – выделенный ресурс для восстановления работоспособности ОИ.

Б) Требуется разработать аналитическую процедуру и исследовать частные случаи определения наименьшего значения функции устойчивости (9) ОИ на заданном интервале (0, T]:

$$\nu_m = \inf_{\substack{t \in (0, T], \\ R \le R_0}} \nu(t, \lambda, r, u). \quad (9)$$

Функция устойчивости ОИ в общем виде записывается как (10) [19]:

$$\nu(t, \lambda, r, u) = K_{\Gamma}(u, r)\varphi(t, \lambda, r, u), \quad (10)$$

где $K_{\Gamma}(u, r)$ – коэффициент готовности ОИ; $\varphi(t, \lambda, r, u)$ – функция живучести (ФЖ) ОИ; t – текущий момент времени оценки ФЖ; T – интервал времени ожидания КА.

Общий порядок определения коэффициента готовности ОИ (11) приведен и исследуется в теории надежности технических систем [20]:

$$К_{г} = T_{н}(T_{н} + T_{в})^{-1}, \quad (11)$$

где $T_{н}$ – среднее время наработки на отказ в штатных условиях эксплуатации; $T_{в}$ – среднее время восстановления работоспособности в штатных условиях эксплуатации – определяются на основании статистических наблюдений, полученных в условиях штатной эксплуатации ОИ. Для большинства случаев имеют место соотношения (12):

$$К_{\Gamma} \geq 0{,}99; \varphi_{m} << К_{\Gamma}, \quad (12)$$

где φ_{m} – минимальное значение ФЖ на промежутке нанесения КА по ОИ. Поэтому $К_{\Gamma}$ при оценке живучести можно пренебречь. Тогда математическая модель сводится к определению (13):

$$\nu_{m} \approx \varphi_{m} = \inf_{\substack{t \in (0, T], \\ R \leq R_{0}}} \varphi(t, \lambda, r, u), \quad (13)$$

где ν_m – минимальное значение функции устойчивости на заданном интервале времени.

Выводы. Таким образом, для внедрения риск-ориентированного подхода основные усилия требуется сосредоточить на разработке и внедрении методического обеспе чения по оценке рисков ИБ для условий компьютерных атак, которые позиционируются как редкими события (в этом направлении уже имеются некоторые наработки [21, 22, 23, 24], однако целостные методики пока не разработаны, поэтому научные исследования в названном направлении можно считать актуальными. Для проведения исследований в качестве объекта взята автоматизированная система управления технологическими процессами климат-контроля в зданиях Московского института электронной техники, которая по структуре и по функционалу может быть позиционирована как объект критической информационной инфраструктуры. Предметом же исследования являются методы оценки устойчивости её функционирования в штатных условиях применения и в условиях компьютерных атак. В результате планируется получить научно обоснованные рекомендации для принятия решения по обеспечению защиты информации в заданных условиях. Полученные результаты планируется представить на конкурс работ в 2023 году.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ: [Принят Государственной Думой 8 июля 2006 года: Одобрен Советом Федерации 14 июля 2006 года]. [Электронный ресурс]. – Режим доступа: http://www.rg.ru/2004/08/05/taina-doc.html.

2. Садовничий В. А., Акаев А. А., Коротаев А. В., Малков С. Ю. Моделирование и прогнозирование мировой динамики // Научный совет по Программе фунд. исслед. Президиума Российской академии наук «Экономика и социология знания». – М.: ИСПИ РАН, 2012. – (Экономика и социология знания). – 359 с.

3. Глазьев С. Ю. Стратегия опережающего развития России в условиях глобального кризиса. – М.: Экономика, 2010. – 255 с.

4. Доктрина информационной безопасности Российской Федерации: [утв. Президентом Российской Федерации 9 сентября 2000 г. № 1895] [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/901770877 (дата доступа: 13.04.2022).

5. Доктрина информационной безопасности Российской Федерации: [утв. Президентом Российской Федерации 5 декабря 2016 г. № 646] [Электронный ресурс]. – Режим доступа: http://publication.pravo.gov.ru/Document/View/0001201612060002 (дата доступа: 13.04.2022).

6. Программа «Цифровая экономика Российской Федерации»: [утв. Распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р] [Электронный ресурс]. – Режим доступа: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (дата доступа: 13.04.2022).

7. Паспорт национального проекта «Цифровая экономика» [утв. протоколом от 24 декабря 2018 г. № 16 решением президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам] [Электронный ресурс]. – Режим доступа: http://government.ru/info/35568/__(дата доступа: 13.04.2022).

8. Паспорт федерального проекта «Цифровая экономика» [утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий предпринимательской деятельности протоколом от 28 мая 2019 г. № 9 [Электронный ресурс]. – Режим доступа: https://digital.gov.ru/uploaded/files/pasport-federalnogo-proekta-informatsionnaya-bezopasnost.pdf (дата доступа: 13.04.2022).

9. Global Cyber Insurance Market (2019-2025): Market Size is Expected to Reach $21.4 Billion - ResearchAndMarkets.com [Электронный ресурс]. – Режим доступа: https://bwnews.pr/3nxkwbl (дата доступа: 13.04.2022).

10.«Уголовный кодекс Российской Федерации» от 13 июня 1996 г. № 63-ФЗ (ред. от 25 марта 2022 г.) [Электронный источник] / http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 12.04.2022).

11.О стандартизации в Российской Федерации: Федеральный закон от 29 июня 2015 г. № 162-ФЗ (последняя редакция) [Электронный источник] / http://www.consultant.ru/document/cons_doc_LAW_181810/ (дата обращения 12.04.2022).

12.ГОСТ Р ИСО 31000–2019. Менеджмент риска. Принципы и руководство. Общие положения: нац. стандарт Рос. Федерации: изд. офиц.: утв. и введ. в действие Приказом Федер. агентства по техн. регулированию и метрологии от 10 декабря 2019 г. № 1379-ст: взамен ГОСТ Р ИСО 31000–2010: дата введ. 2020-03-01. – М.: Стандартинформ, 2021. 18 с.

13.ГОСТ Р МЭК 31010–2021. Надежность в технике. Методы оценки риска. Общие положения: нац. стандарт Рос. Федерации: изд. офиц.: утв. и введ. в действие Приказом Федер. агентства по техн. регулированию и метрологии от 24 сентября 2021 г. № 1011-ст: введ. впервые: дата введ. 2022-01-01. – М.: Стандартинформ, 2020. 94 с.

14.ГОСТ Р ИСО/МЭК 27005–2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. № 632-ст. М.: Стандартинформ, 2012. – 91 с.

15.ГОСТ Р 59516-2021. Информационные технологии. Менеджмент информационной безопасности. Правила страхования рисков информационной безопасности. М.: Стандартинформ, 2021. 20 с.

16. Воеводин В. А., Маркин П. В., Маркина М. С., Буренок Д. С. Методика разработки программы аудита информационной безопасности с учетом весовых коэффициентов значимости свидетельств аудита на основе метода анализа иерархий // Системы управления, связи и безопасности. 2021. № 2. С. 96–129. DOI: 10.24412/2410-9916-2021-2-96-129.

17. Воеводин В. А., Буренок Д. С., Маркин П. В., Маркина М. С. «Программа метода анализа иерархий». Свидетельство о государственной регистрации программ для ЭВМ № 2020667542. Дата регистрации 24.12.2020.

18.V. A. Voevodin. Monte Carlo method for solving the problem of predicting the steadiness of the functioning of an automated control system in the conditions of massive computer attacks. Марчуковские научные чтения-2021: Тезисы Междунар. конф., 4–8 октября 2021 г. / Ин-т вычислит. математики и матем. геофизики СО РАН. С 75. DOI 0.24412/CL-35064-2021-095.

19.Хохлачев Е. Н. Организация и технологии выработки решений при управлении системой и войсками связи. Часть 2. Выработка решений при восстановлении сетей связи. – М.: ВА РВСН, 2009. 241 с.

20.Надежность и эффективность в технике. Справочник Том № 5. Проектный анализ надежности/ под ред. В.И. Патрушева и А.И. Рембезы. – М.: Машиностроение, 1989, – 376 с.

21.Voevodin V. A., Burenok D. S., Cherniaev V. S. Monte Carlo method for solving the problem of predicting the computer network resistance against DoS attacks // International Conference «Marchuk Scientific Readings 2021» (MSR-2021). Journal of Physics: Conference Series 2099 (2021) 012069. DOI: 10.1088/1742-6596/2099/1/012069.

22.Voevodin V. A. Monte Carlo method for predicting the stability of the functioning of the informatization object in the conditions of massive computer attacks // International Conference «Marchuk Scientific Readings 2021» (MSR-2021). Journal of Physics: Conference Series 2099 (2021). DOI: 10.1088/1742-6596/2099/1/012070.

23.Буренок Д. С., Воеводин В. А. Программа обнаружения атак на Wi-Fi сеть // Свидетельство о государственной регистрации программы для ЭВМ № 2021664674 от 10 сентября 2021 г.

24.Воеводин В. А. Программа оценки минимума функции живучести объекта информатизации // Свидетельство о государственной регистрации программы для ЭВМ № 2021663763 от 23 августа 2021 г.

Задворьев Е.Ф.
МГТУ ГА, ИБТКС, 4 курс,
zadvorev@list.ru
Савицкий Е.В.
МГТУ ГА, ИБТКС, 4 курс,
barsukeughen@gmail.com
Научный руководитель:
Емельянов В.Е.
МГТУ ГА, профессор кафедры ОРТЗИ, д.т.н.,
v.emelianov@mstuca.aero

МОДЕЛЬ ОЦЕНКИ РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

Перспективным направлением в сфере защиты информации является рассмотрение процесса принятия решений по управлению рисками через призму теории игр [1].

Рассмотрим задачу, в которой соревнуется два игрока – злоумышленник и специалист по информационной безопасности (ИБ). Возможно несколько случайно выбираемых состояний, представляющих собой комбинацию вероятностей успешной реализации атаки, стоимостных показателей реализации средств защиты информации (СЗИ) и нанесённого ущерба. Каждое из таких состояний описывается отдельной матрицей.

Случайными образом происходит выбор одной из возможных матриц, каждая из которых описывает возможные атаки и методы защиты для каждой из команд; далее первый игрок выбирает тип атаки, и второй игрок – тип защиты (каждая команда действует согласно своей стратегии; атакующая команда стремится максимизировать убытки компании, защищающаяся – минимизировать). Возможные матрицы задаются элементами, представляющими собой заранее

известные вероятности. Любая из матриц в свою очередь описывает собой различные варианты типов атак. Каждая из сторон действует, согласно своей стратегии, при этом злоумышленник пытается максимизировать ущерб, а специалист по ИБ – минимизировать [2].

Набор возможных защитных приёмов у защищающейся команды всегда одинаков, независимо от выбора матрицы; таким образом, матрицы связаны воедино; стратегия защищающейся команды будет заключаться в выборе метода (режима) защиты, оптимального для всей суммы матриц.

Специалист по защите информации будет стремиться разработать стратегию защиты информации с целью защитить информационную систему.

Злоумышленник также будет стремиться разработать и реализовать ряд стратегий по проведению атак на информационную систему, с целью максимизировать свой успех (ущерб предприятия). [5]

Возможно рассматривать матрицы в различном ключе; например, каждая матрица может являть собой различные состояния системы (обычная работа, повышенная готовность и другие возможные состояния), или различный профессиональный уровень атакующего злоумышленника. Количество матриц в таком случае будет соответствовать количеству различных состояний системы (злоумышленника). В примере, рассмотренном в данной статье, различные матрицы рассматриваются как атаки двух различных злоумышленников (внутренний и внешний).

В качестве исходных данных как пример рассмотрения такой системы рассмотрим две матрицы, которые представляют собой (после сбора и обработки данных) наиболее вероятные стратегии для внутреннего или внешнего злоумышленника и защищающейся стороны, соответственно.

Введём следующие обозначения:

$A_1 = \{a_1, ..., a_{n_1}\}$ – множество возможных атак внутреннего злоумышленника.

$A_2 = \{a_1, ..., a_{n_2}\}$ – множество возможных атак внешнего злоумышленника.

$B = \{b_1, ..., b_m\}$ – множество возможных методов распределения ресурсов защищающегося.

$C_1 = \{c_1, ..., c_{n_1}\}$ – ущерб, который понесёт защищающаяся сторона в случае удачного проведения внутренним злоумышленником соответствующей атаки.

$C_2 = \{c_1, ..., c_{n_2}\}$ – ущерб, который понесёт защищающаяся сторона в случае удачного проведения внешним злоумышленником соответствующей атаки.

$D = \{d_1, ..., d_m\}$ – затраты на выбранный метод (режим) защиты.

$P_1 = \{p_{11}, ..., p_{ij}, ..., p_{mn_1}\}$ – вероятность проведения успешной атаки при выборе *i*-й стратегии защищающимися и *j*-й стратегии внутренним злоумышленником.

$P_2 = \{p_{11}, ..., p_{ij}, ..., p_{mn_2}\}$ – вероятность проведения успешной атаки при выборе *i*-й стратегии защищающимися и *j*-й стратегии внешним злоумышленником.

На основе исходных данным составляются матрицы:

$$M_1 = \begin{pmatrix} & a_1 & a_2 & \dots & a_{n_1} & \\ b_1 & p_{11} & p_{12} & \dots & p_{1n_1} & d_1 \\ b_2 & p_{21} & p_{22} & \dots & p_{2n_1} & d_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ b_m & p_{m1} & p_{m2} & \dots & p_{mn_1} & d_m \\ & c_1 & c_2 & \dots & c_{n_1} & \end{pmatrix}, \quad (1)$$

$$M_2 = \begin{pmatrix} & a_1 & a_2 & \dots & a_{n_2} & \\ b_1 & p_{11} & p_{12} & \dots & p_{1n_2} & d_1 \\ b_2 & p_{21} & p_{22} & \dots & p_{2n_2} & d_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ b_m & p_{m1} & p_{m2} & \dots & p_{mn_2} & d_m \\ & c_1 & c_2 & \dots & c_{n_2} & \end{pmatrix}, \quad (2)$$

где M_1 – матрица состояний для игрока 1 (внутренний злоумышленник), M_2 – матрица состояний для игрока 2 (внешний злоумышленник).

Исходя из того, что злоумышленник будет иметь целью максимизацию ущерба при минимуме риска (максимум средней прибыли за одну игру), возможно определить его оптимальную стратегию максиминным решением (например, критерием Вальда).

Получив оптимальную стратегию злоумышленника, возможно определить оптимальную стратегию для защищающегося; защищающийся преследует цель минимизации убытков, поэтому используем минимаксное решение (например, критерием Сэвиджа). [3, с. 177-185, 200][4].

Обозначим такие оптимальные стратегии для каждой матрицы β_1 и β_2, соответственно.

Если оптимальная стратегия одинакова для всех матриц - данная стратегия всегда оптимальна. Если оптимальные стратегии различные, необходимо разработать стратегию применения различных методов для достижения наименьших убытков.

При рассмотрении совокупности матриц частотность злоумышленников (и, соответственно, вероятности появления соответствующей матрицы) будет выступать как весовой коэффициент.

Обозначим их:

$p_{вн}$ – вероятность выбора матрицы внутреннего злоумышленника;

$q_{вн} = 1 - p_{вн}$ – вероятность выбора матрицы внешнего злоумышленника.

Вероятности выбора метода для каждой из стратегий умножаются на вероятность появления матрицы, для которой эта стратегия оптимальна (если стратегия оптимальна для всех матриц, она остаётся неизменной).

Тогда матрица оптимальной стратегии имеет вид:

$$\beta_{опт} = \begin{pmatrix} b_1 & b_2 & b_3 \\ p_{вн} \cdot p_{\beta_1}(b_1) & p_{вн} \cdot p_{\beta_1}(b_2) & p_{вн} \cdot p_{\beta_1}(b_3) \\ +q_{вн} \cdot p_{\beta_2}(b_1) & +q_{вн} \cdot p_{\beta_2}(b_2) & +q_{вн} \cdot p_{\beta_2}(b_3) \end{pmatrix}. \quad (4)$$

Таким образом, получаем оптимальную стратегию, учитывающую вероятность появления матриц и оптимальные стратегии для каждой из них.

Рассмотрение множества возможных матриц с случайным выбором с помощью теории игр позволяет изучить игры, рассматривающие набор различных ситуаций, и с помощью сравнительно простого набора методов проанализировать их. Среди возможных применений – рассмотрение различных режимов готовности службы ИБ, атаки злоумышленников различной квалификации или направленности, или же обладающих различным уровнем ресурсов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Лаврентьев А.В., Зянин В.П. Теоретико-игровая модель принятия решения по управлению рисками информационной безопасности. // Журнал Спецтехника и связь. 2012. № 3. С. 47-53. URL: https://cyberleninka.ru/article/n/teoretiko-igrovaya-

model-prinyatiya-resheniy-po-upravleniyu-riskami-informatsionnoy-bezopasnosti (дата обращения: 05.09.2022).

2. Емельянов В.Е. Исследование операций. Применение теории игр в задачах защиты информации: учебное пособие. - М.: ИД Академии Жуковского, 2021.

3. Вентцель Е.С. Исследование операций: задачи, принципы, методология : учебное пособие — 6-е изд., стер. — Москва : ЮСТИЦИЯ, 2018.

4. Рубцов Н.В. Влияние модели злоумышленника на процесс оценки уязвимостей информационной системы. // Известия ЮФУ. Технические науки. 2011. С. 120-123. URL: https://cyberleninka.ru/article/n/vliyanie-modeli-zloumyshlennika-na-protsess-otsenki-uyazvimostey-informatsionnoy-sistemy (дата обращения: 05.09.2022).

5. Цыбулин А. М., Шипилева А.В. Математическая модель злоумышленника в корпоративной сети. Управление большими системами. Выпуск 19. – М.: ИПУ РАН. 2007. С. 127-133.

6. Савченко С.О., Капчук Н.В. Алгоритм построения модели нарушителя в системе информационной безопасности с применением теории игр. // Динамика систем, механизмов и машин. 2017. С. 84-89. URL: https://cyberleninka.ru/article/n/algoritm-postroeniya-modeli-narushitelya-v-sisteme-informatsionnoy-bezopasnosti-s-primeneniem-teorii-igr (дата обращения: 07.09.2022).

7. Миков Д.А. Анализ методов и средств, используемых на различных этапах оценки рисков информационной безопасности. // Вопросы кибербезопасности. 2014. №4(7). С. 49-54. URL: https://cyberleninka.ru/article/n/analiz-metodov-i-sredstv-ispolzuemyh-na-razlichnyh-etapah-otsenki-riskov-informatsionnoy-bezopasnosti (дата обращения: 07.09.2022).

8. Цибулин А.М., Никишова А.В., Умницын М.Ю. Исследование противоборства службы безопасности и злоумышленников на многоагентной модели. // Известия ЮФУ. Технические науки. 2008. С. 94-99. URL:

https://cyberleninka.ru/article/n/issledovanie-protivoborstva-sluzhby-bezopasnosti-i-zloumyshlennikov-na-mnogoagentnoy-modeli (дата обращения: 06.09.2022).

9. Канаев А.К., Опарин Е.В., Опарина Е.В. Имитационная модель противоборства организованного злоумышленника и системы обеспечения информационной безопасности при реализации атак на систему управления сетью тактовой сетевой синхронизации. // Труды учебных заведений связи. 2021. Т.7, №4. URL: https://cyberleninka.ru/article/n/imitatsionnaya-model-protivoborstva-organizovannogo-zloumyshlennika-i-sistemy-obespecheniya-informatsionnoy-bezopasnosti-pri (дата обращения: 10.09.2022).

10. Зайченко Ю. П. Исследование операций: Учеб. пособие для студентов вузов. — 2-е изд., перераб. и доп.—• Киев: Вища школа. Головное изд-во. 1979.

Лазорин Д.С.,
РГУ нефти и газа (НИУ) имени И.М. Губкина,
информационная безопасность автоматизированных систем, 2 курс,
lazorindanya@yandex.ru
Научный руководитель:
Правиков Д.И.,
РГУ нефти и газа (НИУ) имени И.М. Губкина, заведующий кафедрой комплексной безопасности критически важных объектов, к.т.н.,
dip@gubkin.pro

О ПОДХОДАХ К ОБЕСПЕЧНЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЦИФРОВЫХ ДВОЙНИКОВ

Введение. Понятие «цифровой двойник» в настоящее время прочно заняло позиции в современных цифровых технологиях. Данный термин достаточно широк и в первом приближении описывает математическую или компьютерную имитационную модель, связанную с физическим объектом потоками передачи информации, которая может быть отчуждена или отделена от исходного объекта в целях воспроизведения его функционирования или выполнения действий с указанным объектом [1, 2].

Актуальность цифровых двойников сегодня общепризнана. Об этом свидетельствуют, в частности, документы Министерства Энергетики [3].

Одной из наиболее острых является проблема информационной безопасности цифровых двойников. Вместе с имитацией процессов объектов физического мира при помощи данной технологии появляется возможность их контролировать, следовательно, не допускать наступления негативных событий. Приоритетной задачей становится обеспечение информационной безопасности организаций и технологических процессов, использующих технологию цифровых двойников.

Элементы системы «Физический Объект – Цифровой Двойник» (ФОЦД).

Рассмотрим основные компоненты системной целостности, включающей физический объект и виртуальный объект.

1. Физический объект (ФО).

2. Виртуальный объект или специальная модель, соответствующая физическому объекту (цифровой двойник, ЦД).

3. Взаимосвязи в системе, включающей виртуальный объект и физический объект.

Цифровым двойником в этой целостности является второй компонент, который может иметь связи с физическим объектом для его мониторинга и управления (третий компонент системной целостности).

Для объединения в ФОЦД вышеперечисленных частей используются различные, как принято говорить в современной информатике, интеграции, обеспечивающие получение реальных данных от модели ФО, которая может строиться на основе технологий «Интернет вещей» (Internet of Things, сокращённо IoT), а также различных математических моделях. К ним могут относиться, например, CAE-системы (Computer-aided engineering, автоматизированное проектирование), предназначенные для решения инженерных задач [4].

Стоит отметить, что вопрос обеспечения информационной безопасности ЦД конструктивно решается в том случае, если учитываются следующие априорные требования: контроль получаемых от ФО параметров, обеспечение целостности и конфиденциальности при обмене данными, обеспечение доступности и, самое главное, соответствие модели реальному объекту.

Специфические свойства цифровых двойников. С точки зрения системного анализа необходимо выявить специфические свойства и общие требования, которые можно предъявить к ФОЦД.

В первую очередь, это целостность, понимаемая как неразрывная взаимосвязь всех трех компонентов, их актуальность (в смысле соответствия текущему

состоянию параметрам), наличие исчерпывающих связей между элементами системной целостности ФОЦД и их полнота. В этом смысле весьма конструктивным представляется подход к описанию ФОЦД как некоторой платформы или ее части.

С точки зрения реализации угроз ЦД может не соответствовать ФО, который управляется или мониторируется с его помощью.

Проверка соответствия ЦД ФО может проводиться через оценку качества управления. Цифровой двойник должен представлять собой адекватную модель существующего физического продукта или целостного процесса.

При необходимости можно зафиксировать и другие требования: актуальность цифрового двойника, защита канала связи двойника и объекта.

Основные подходы к безопасности цифровых двойников. Нами были проанализированы актуальные источники и определены основные подходы и методы обеспечения информационной безопасности, которые могут быть применены к технологии цифровых двойников: блокчейн-структура, подход к организации информационного взаимодействия в многоуровневой системе, система иерархической токенизации элементов системы, Digital ID или цифровой сертификат, методика многоуровневого шифрования команд для управления удалёнными компьютерными системами, комплексный подход с использованием машинного обучения и искусственного интеллекта, обеспечение безопасности ЦД в рамках концепции многоуровневой платформы [5, 6, 7, 8, 9]. Для каждого из них проведено краткое описание, изложена конструктивная критика данных подходов и методов в полной нашей работе.

На основе проанализированных подходов и методов к безопасности цифровых двойников построена таблица 1 «Некоторые способы обеспечения комплексной безопасности цифровых двойников».

Таблица. 1. Некоторые способы обеспечения комплексной безопасности цифровых двойников

Информационное взаимодействие в многоуровневой системе	✓
Проверка подлинности поступаемых запросов к модели	✓
Шифрование данных при передаче по каналам связи	✓
Решения на основе машинного обучения и искусственного интеллекта	✓
Соответствие модели реальному объекту	**X**

Отечественные индустриальные криптомодули ViPNet SIES Core & Pack.

На данный момент большинство нефтегазовых месторождений находятся на завершающей стадии эксплуатации и не оснащены порой элементарными средствами автоматики. Следовательно, некоторые АИУС нефтегазовые Общества, а также АСУ ТП месторождения используют отечественное оборудование фирмы Infotecs. Существуют решения по анализу информационной безопасности АСУ ТП от компании Infotecs.

Нами было протестировано следующее программное обеспечение от данной фирмы: ViPNet Client 4. Это программное обеспечение для защиты трафика на рабочих местах пользователей. Оно фильтрует весь входящий и исходящий трафик компьютера и позволяет обмениваться данными с другими узлами ViPNet по защищенному VPN-каналу. В программе имеется доступ к сетевым фильтрам, которые используются, чтобы пропускать или блокировать трафик по определенным признакам. Сетевые фильтры, настроенные по умолчанию, блокируют входящий открытый (незашифрованный) трафик за исключением

протоколов DHCP, NetBIOS, WINS. При необходимости имеется возможность настроить собственные сетевые фильтры для открытого и зашифрованного трафика. Программа обеспечивает контроль над сетевой активностью приложений, установленных на компьютере. Если какая-либо программа пытается получить доступ к сети, на экране появляется предупреждение. Помимо этого, появляется возможность отправлять сообщения электронной почты и вложения пользователям других узлов ViPNet. Стандартно сообщения зашифрованы и подписаны электронной подписью.

Стоит обратить внимание на криптографический модуль ViPNet SIES Core. Это средства защиты данных интеллектуальных устройств автоматики, входящие в состав комплекса продуктов ViPNet SIES, предназначенные для защиты информации, обрабатываемой устройствами автоматизации индустриальных систем. Они обеспечивает защиту данных в устройствах автоматизации, например, программируемые логические контроллеры (PLC), устройства сбора и передачи информации (RTU), промышленные контроллеры автоматизации (PAC), сенсоры, датчики, счетчики, различные исполнительные устройства.

Защищаемое устройство со встроенным ViPNet SIES Core может реализовывать различные сценарии защиты данных в зависимости от модели угроз и нарушителя информационной безопасности, разработанной для защищаемого устройства или индустриальной системы. Например, с помощью ViPNet SIES Core можно реализовать следующие сценарии: обеспечение целостности при передаче данных по существующим каналам связи; обеспечение конфиденциальности при передаче данных по существующим каналам связи; защита от навязывания индустриальной системе ложных данных, защита от повторов и навязывания индустриальной системе устаревших данных, доверенное обновление программного обеспечения (ПО) и конфигурации защищаемого устройства, доверенное хранение данных о функционировании защищаемого устройства [10].

На данный момент нами проводится тестирование криптографического модуля ViPNet SIES Core.

Заключение. Проведенный анализ существующих подходов к обеспечению информационной безопасности цифровых двойников позволяет сделать вывод, что практически ни один из предложенных способов в отдельности не обеспечивает комплексной безопасности в рамках актуальных для цифровых двойников моделей угроз и нарушителя. Использование технологий распределенных реестров, метода иерархической токенизации, цифровых сертификатов, многоуровневого шифрования, машинного обучения и искусственного интеллекта на современном уровне весьма оправдано, но направлено на решение частных задач.

В связи с этим целесообразно развивать методологию обеспечения информационной безопасности цифровых двойников в соответствии с концепцией многоуровневой платформы, поскольку в понятие платформы уже включен комплексный подход и иерархия решений от низкоуровневых способов защиты канала связи ФОЦД при помощи криптографических алгоритмов до высокоуровневых задач, связанных с проверкой соответствия моделей функционирования цифрового двойника и обеспечения корректности бизнес-процессов, отражаемых цифровым двойником.

При этом отдельные способы обеспечения информационной безопасности могут включать уже готовые решения (например, средства шифрования данных при передаче по каналам связи), а для части методов (направленных, например, на обеспечение соответствия виртуальной модели реальному объекту) необходимо использовать другие средства и подходы, которые будут сформулированы в следующих работах.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Намиот Д.Е. Цифровые двойники и системы дискретно-событийного моделирования. / Д.Е. Намиот, О.Н. Покусаев, В.П. Куприяновский, М.Г.

Жабицкий. // International Journal of Open Information Technologies ISSN: 2307-8162 vol. 9, no.2, 2021.

2. Цифровое зеркало, «Газпром Нефть» [Электронный ресурс]: Электрон. текстовые дан. (дата обращения: 12.01.2022) – Режим доступа: https://www.gazprom-neft.ru/press-center/sibneft-online/archive/2018-september-projects/1863687/

3. Паспорт: «Программы инновационного развития» ПАО «Газпром» до 2025 года. Министерство энергетики: инновационное развитие отраслей ТЭК [Электронный ресурс]: Электрон. текстовые дан. (дата обращения: 13.01.2022) – Режим доступа: https://minenergo.gov.ru/node/4844

4. Перспективы использования цифровых двойников на производстве и технологии для их создания. Control Engineering, Россия [Электронный ресурс]: Электрон. текстовые дан. (дата обращения: 27.02.2022) – Режим доступа: https://controleng.ru/innovatsii/cifrovye-dvojniki/chto/

5. Дроговоз П.А., Кошкин М.В. Проекты внедрения технологий блокчейн и интернета вещей в трансграничных цепочках поставок // Управление научно-техническими проектами: сб. материалов III междунар. науч.-техн. конференции. М.: Изд-во МГТУ им. Н.Э. Баумана, 2019. С. 153–156.

6. Mandolla C., Petruzzelli A.M., Percoco G., Urbinati A. Building a digital twin for additive manufacturing through the exploitation of blockchain. Comput. Ind. 2019. Vol. 109. P. 134–152.

7. Воробьев А. В. Концепция информационного пакетного взаимодействия в многоуровневой системе цифровых двойников // Известия Саратовского университета. Новая серия. Серия: Математика. Механика. Информатика. 2021. Т. 21, вып. 4. С. 532-543. DOI: 10.18500/1816-9791-2021-21-4-532-543.

8. Бытый, Д. Э. Методика многоуровневого шифрования команд для системы управления удалёнными компьютерами / Д. Э. Бытый // Наукосфера. – 2021. – № 10-1. – С. 92-95.

9. Правиков Д.И., Глейм А.В., Егоров В.И., Рязанова А.А., Щербаков А.Ю. К вопросу о формулировании системного подхода к исследованиям в области цифровых платформ, распределенных реестров и цифровых активов // Вестник современных цифровых технологий. 2021. № 9. С. 5-14.

10. Защита информации для АСУ ТП и M2M [Электронный ресурс] // Infotecs. URL: https://infotecs.ru/resheniya/zashchita-informatsii-dlya-asu-tp-i-m2m.html (дата обращения: 11.09.2022)

Лупашко Р. В.,
Курганский государственный университет,
Информационная безопасность автоматизированных систем, 4 курс,
komogvr@gmail.com
Лупашко С. Г.,
Курганский государственный университет, доцент, к.ф.-м.н., доцент,
sofirom@mail.ru
Научный руководитель:
Дик Д. И.,
Курганский государственный университет, доцент, к.т.н., доцент,
ddibox@mail.ru

АЛГЕБРАИЧЕСКИЙ ПОДХОД В АЛГОРИТМЕ МОДИФИКАЦИИ ЛОГИЧЕСКИХ ВЫРАЖЕНИЙ

Выражения булевой алгебры или булевы выражения - неотъемлемая часть криптографических алгоритмов и алгоритмов в информационных системах, программно-аппаратных комплексах [3]. Их анализ, запутывание и сокрытие предназначения — является важной задачей, стоящей перед криптоаналитиками и реверс-инженерами. Для решение данной задачи требуется разработка соответствующих алгоритмов и инструментов.

Для сокрытия и запутывания используют алгоритмы модификации и усложнения логических выражений, применяемых в обфускаторах, а для атаки — алгоритмы упрощения, применяемые в деобфускаторах.

Существуют различные подходы к модификации булевых выражений в программных комплексах, которые можно систематизировать следующим образом:

1) логический подход — использование и добавления пустых внешних зависимостей, таких как переменные, циклы, условия в логическое выражение;

2) алгебраический подход — усложнение исходных логических выражений путем применения законов булевой алгебры;
3) гибридный подход — объединяющий предыдущие подходы.

В алгоритмах усложнения и модификаций логических выражений широко распространен логический подход [11]. А в алгоритмах упрощения — метод приведения к нормальной форме (алгебраический подход) [11].

В данной статье предлагается обучающийся алгоритм, реализующий алгебраический подход к модификации булевых выражений.

В основе алгоритма лежит система преобразования алгебраических формул (выражений) [1]. Для описания выражения внутри системы используется дерево логических выражений, как основной структурный объект, состоящее из логических элементов. В качестве таких элементов могут выступать операторы B или переменные V.

Оператор выражения, в данном случае, является логическим оператором, представляющим собой логическую константу, которую можно использовать для соединения логических формул (выражений) [10]. Результатом применения оператора является объединенная логическая формула [5]. Все логические операторы системы включены в множество:

$$\boldsymbol{B} = \left\{ \boldsymbol{B}_1, \dots, \boldsymbol{B}_n \right\}. \tag{1.1}$$

Переменная — минимальная формула (выражение), не имеющая подформул (операторов, подвыражений) [2].

Переменные выражения принадлежат множеству уникальных переменных выражения V:

$$\boldsymbol{V} = \left\{ \boldsymbol{V}_1, \dots, \boldsymbol{V}_n \right\}. \tag{1.2}$$

Обозначим через A логическую формулу (выражение), которая будет в дальнейшем модифицирована. Можно сказать, что формула A построена из переменных V (1.2), если в ней нет других переменных [1].

Введем структуру boolean expression tree (BET), описывающую выражение. Boolean expression tree — это особый вид arithmetic expression tree [8, с. 396]. A arithmetic expression tree — это особый вид бинарного дерева [4]. Таким образом, структура дерева логических выражений выглядит следующим образом (Рис. 1) [6].

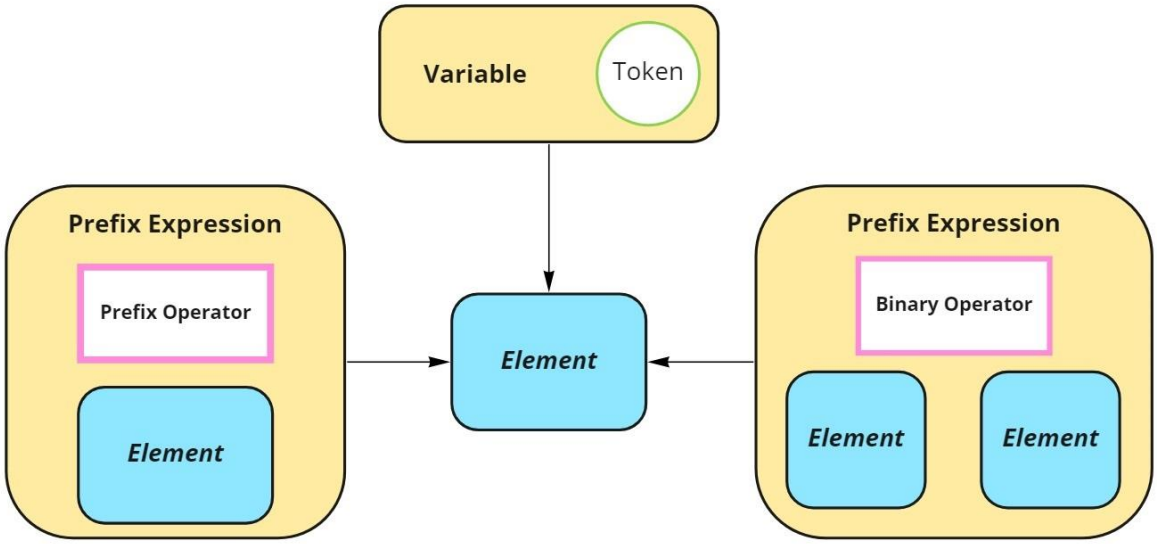


Рис. 1. Структура Boolean Expression Tree

Для модификации A используются правила и аксиомы булевой алгебры L [1]:

$$L = \{L_1, \dots, L_n\} . \quad (1.3)$$

Каждое правило и аксиома булевой алгебры обратимо, т. е. содержит две равносильные формулы: исходная (S) и конечная (E). Все правила имеют общее пространство переменных и операторов:

$$L_i = S \leftrightarrow E, \quad \neg L_i = E \leftrightarrow S, \quad \neg \neg L_i \cong L_i . \quad (1.4)$$

Применение правила на формуле A означает изменение подформулы формулы A. Правило — это двустороннее преобразование, т. е. использование правила может как упростить, так и усложнить исходную формулу.

Для оценки формулы введем функцию усложненности θ, значения которой вычисляются по формуле:

$$\theta(A) = N_{OA} + N_{VA} - \left|V_A\right| , \quad (1.5)$$

где N_{OA} — количество операторов в формуле A,

N_{VA} — количество встречающихся переменных в формуле A,

$\left|V_A\right|$ — мощность множества переменных формулы A.

Например, $A = X \vee Y \vee (Z \wedge X \wedge Y)$. В данной формуле N_{OA} равно 4, N_{VA} равно 5, а $\left|V_A\right|$ равно 3. Таким образом $\theta(A)$ = 4 + 5–3 = 6.

Для оценки правила L_i (1.4) будет использовать разность оценок исходной (S) и конечной (E) подформул L_i:

$$\psi(A) = \theta\left(S \middle| S \preceq L_i\right) - \theta\left(E \middle| E \preceq L_i\right) , \quad (1.6)$$

где $S \preceq L_i$ означает, что S подформула L_i, если $\psi\left(L_i\right) < 0$ — правило упрощает формулу, если $\psi\left(L_i\right) > 0$ — правило усложняет формулу, если $\psi\left(L_i\right) = 0$ — правило изменяет формулу, не меняя $\theta\left(L_i\right)$.

Задачей алгоритма будет приведение оценки выражения $\theta(A)$ к предельной величине $\theta_{lim}(A)$, которая задается в качестве входного параметра. Соответственно, если $\theta(A)$ больше $\theta_{lim}(A)$, то алгоритм будет упрощать формулу, а если $\theta(A)$ меньше $\theta_{lim}(A)$ — усложнять. Важно подметить, что теоретически, при $\theta_{lim}(A) \to \infty$, такой подход может бесконечно усложнять формулу, пока в системе не кончится память. В реальных системах усложнение выражений будет замедлять работу программы, поэтому стоит разумно подходить к заданию величины $\theta_{lim}(A)$.

Входными параметрами алгоритма являются: mode — режим работы; A — формула или логическое выражение; V — множество переменных (1.2); B — множество операторов (1.1); L — множество правил, которые будет применяться в работе.

Перед началом работы мы проверяем формулу A на тавтологию или противоречие. Если такие свойства обнаружены и алгоритм работает в режиме

упрощения, то он останавливается, так как при замене выражения на константы True или False оценка $\theta(True \mid False) = 0$.

Шагом алгоритма будет считаться применение правила к подформуле A^S начальной формулы A_0, результатом которого будет являться формула:

$$A = L_i\left(A^S \middle| A^S \preceq A_0\right), \tag{2.1}$$

где $A^S \preceq A_0$ — подформула формулы A_0.

Таким образом, можно представить работу алгоритма, как последовательное применение правил к подформулам формулы A.

$$A = L_j\left(L_k\left(\ldots \; L_g\left(A^S \middle| A^S \preceq A_0\right) \ldots \right)\right), \tag{2.2}$$

где L_j, L_j, L_j — правила, принадлежащие множеству правил L (1.3)

Тогда оценкой работы алгоритма будет являться сумма оценок примененных правил:

$$\theta(A) = \theta\left(A_0\right) - \sum_i \psi\left(L_i\left(A^S \middle| A^S \preceq A_0\right)\right). \tag{2.3}$$

Логический оператор может создавать связи с одной формулой (унарные связи) или с двумя формулами (бинарные связи) [7, 9]. Таким образом, один оператор составляет уровень BET или на одном уровне BET могут находиться только операторы, не связанные друг с другом [8]. Если в формуле присутствует хотя бы два оператора, такая формула будет находиться на 2 уровнях BET и т. д. (Рис. 2).

Введем характеристику d_A, показывающую количество уровней дерева формулы A, т. е. глубину дерева выражения.

Структура правила хранит исходное BET_S и конечное BET_E выражение, характеристику d_A каждого выражения, оценку $\theta\left(BET_S\right)$ и $\theta\left(BET_E\right)$ (1.5), общую оценку правила (1.6).

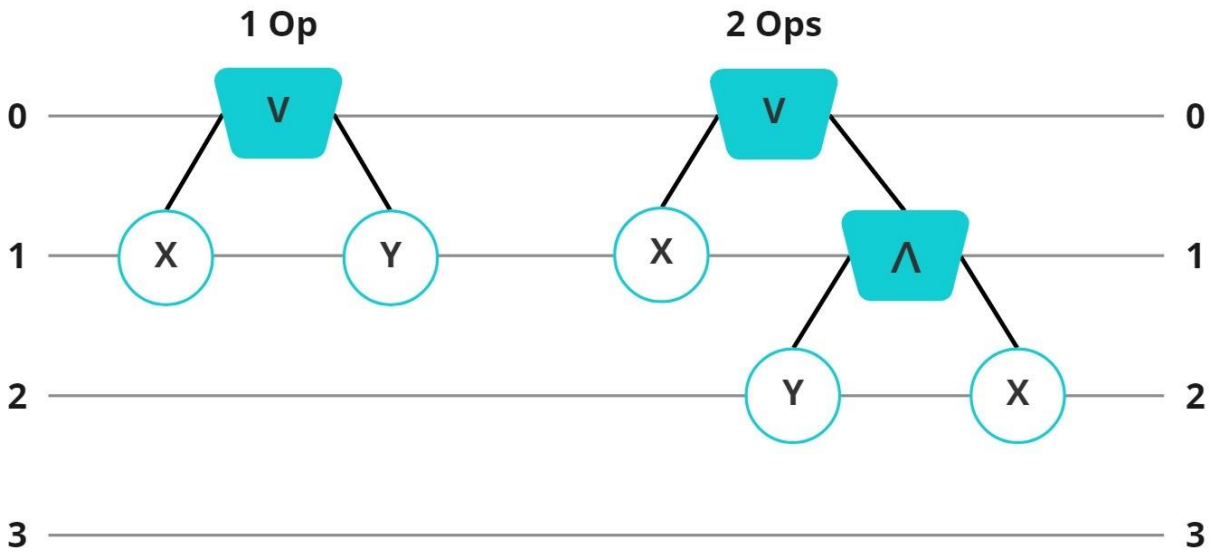


Рис. 2. Уровни выражений в BET

Из сказанного выше, шаг алгоритма — применение правила. Для применения правила нужно найти $A^S \preceq A$. Логическая формула (выражение) описывается структурой BET (Рис. 1). Таким образом, задача нахождения подформулы сводится к задаче нахождения поддерева.

Предлагается следующий подход к модификациям дерева. Обход дерева начинается с уровня d_A. Выбираем все поддеревья уровня d_A, потом $d_A - 1$ и т. д. пока не достигнем уровня 0. Каждое выбранное поддерево сравнивается с правилами из множества правил. Если правило подходит, то оно применяется и шаг алгоритма заканчивается. Если подходят несколько правил, то применяется правило с самой высокой оценкой, зависящей от режима работы алгоритма:

$$max\left(\left|\psi\left(L_i\right)\right| for\ L_i\ in\ L\right). \qquad (2.4)$$

После завершения шага происходит переоценка полученного выражения. Если текущая оценка не достигла предельной оценки $\theta_{lim}(A)$, то шаг запускается снова, иначе алгоритм останавливается.

Дополнительно, алгоритм использует отсечене пустых итераций J. Если оценка $\theta(A)$ перестала меняться в течение J шагов — алгоритм останавливается.

Описанный алгоритм модифицирует выражение, применяя установленные правила. Исходя из этого, можно сделать динамическое обновление списка правил, используя единственное правило вывода — Modus Ponens (MP) [1].

Результатом работы алгоритма является не только преобразованная формула, но и путь преобразования — это последовательность применяемых формул. По правилу MP можно породить новую аксиому

$$\frac{A, A \to B}{B}, \frac{B, B \to C}{C}, \frac{C, C \to D}{D}, \frac{A, A \to D}{D}, \tag{2.5}$$

где A, B, C, D — произвольные формулы. Эта запись показывает, как можно вывести новую аксиому $A \to D$ [1].

Предложенный алгоритм может быть использован в системах обфускации для усложнения процесса реверс-инжиниринга. Также алгоритм может быть использован в деобфускаторах для упрощения запутанных логических выражений при выполнении анализа кода.

Система преобразования выражений может лечь в основу анализатора, который по сигнатурам выражений и прочим факторам может классифицировать алгоритм, используемый криптосистемой.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Шехтман, В. Б. Введение в математическую логику (осень 2018) [Электронный ресурс] / В. Б. Шехтман. — Режим доступа: https://www.hse.ru/data/2019/04/04/1189341797/vml2018_lectures_all.pdf , свободный. — Загл. с экрана. (Дата обращения: 17.09.2022).

2. Atomic formula [Электронный ресурс] // Wikipedia, сайт. — Режим доступа: https://en.wikipedia.org/wiki/Atomic_formula, свободный. — Загл. с экрана. (Дата обращения: 13.09.2022).

3. Binary expression [Electronic resource] // IBM Documentation. — Access mode: https://www.ibm.com/docs/en/zos/2.4.0?topic=operators-binary-expressions, free. — Title from screen. (Дата обращения: 13.09.2022).

4. Binary expression tree [Электронный ресурс] // Wikipedia, site. — Режим доступа: https://en.wikipedia.org/wiki/Binary_expression_tree, свободный. — Загл. с экрана. (Дата обращения: 13.09.2022).

5. Boolean algebra with operators [Electronic resource] // Encyclopedia of mathematics, site. — Access mode: https://encyclopediaofmath.org/wiki/Boolean_algebra_with_operators#:~:text=An%20operator%20on%20a%20Boolean,the%20least%20element%20of%20B, free. — Title from screen. (Дата обращения: 04.09.2022).

6. Build Binary Expression Tree in Python [Electronic resource] // Medium, site. — Access mode: https://medium.com/swlh/build-binary-expression-tree-in-python-36c04123e57b, free. — Title from screen. (Дата обращения: 25.08.2022).

7. Create and Evaluate Simple Expression Tree in Python in Object Oriented style [Electronic resource] // Medium. — Access mode: https://levelup.gitconnected.com/create-and-evaluate-simple-expression-tree-in-python-in-object-oriented-style-5eb27b6376c8, free. — Title from screen. (Дата обращения: 26.08.2022).

8. Goodrich, M. Data Structures and Algorithms in Java / M. T. Goodrich, R. Tamassia. — 4th ed. — Wiley, 2005. – 720 с. (Дата обращения: 15.09.2022).

9. Laws of Boolean Algebra [Electronic resource] // Electronic Tutorials. — Access mode: https://www.electronics-tutorials.ws/boolean/bool_6.html, free. — Title from screen. (Дата обращения: 12.09.2022).

10. Logical connective [Электронный ресурс] // Wikipedia, сайт. — Режим доступа: https://en.wikipedia.org/wiki/Logical_operation, свободный. — Загл. с экрана. (Дата обращения: 18.09.2022).

11. Logical optimization [Электронный ресурс] // Wikipedia, сайт. — Режим доступа: https://en.wikipedia.org/wiki/Logic_optimization, свободный. — Загл. с экрана. (Дата обращения: 13.09.2022).

Наточий Н.М., Ананьев В. А., Гладких Е.А.,
Курганский государственный университет
Безопасность информационных и автоматизированных систем, 2 курс
natochiy_n@mail.ru
Научный руководитель:
Иванов Д.С.,
Курганский государственный университет, ассистент
daniil_ivanov_97@mail.ru

АНАЛИЗ МЕТОДОВ ГАРАНТИРОВАННОГО УДАЛЕНИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА ЭЛЕКТРОННЫХ НОСИТЕЛЯХ.

В последние годы компьютерные технологии стали неотъемлемой частью документооборота. Это привело к тому, что в сфере бизнеса и государственного управления скопилось множество конфиденциальной информации, хранящейся в базах данных (БД) на персональных компьютерах. Ввиду появления проблемы их утечки образуется множество программных и аппаратных средств защиты от разнообразных утечек.

В нынешнем быстроизменяющемся мире любые компьютерные комплектующие достаточно быстро устаревают. Люди, которые стремятся идти в ногу со временем вынуждены достаточно часто их обновлять. Также в свою очередь и крупные ИТ-компании должны заменять своё оборудование, обычно срок, в течении которого следует полностью обновить ПК, составляет около 4 лет. [1] Это также касается и электронных носителей информации, которые также приходится заменять на новые.

Важным аспектом защиты информации от кражи является её правильное удаление. Чем чаще мы записываем и сохраняем различные файлы, тем выше шанс того, что

мы сотрем их неправильно, а злоумышленник получивший доступ к ПК сможет украсть важные данные.

Для того чтобы разобраться с тем, как правильно удалять данные с электронных носителей нужно знать некоторые тонкости данного процесса:

1. Обычное удаление файлов и последующая очистка корзины не дают практически никакого эффекта. Сектор, на котором записан файл, помечается как свободный и это означает лишь то, что когда вы в следующий раз вы захотите внести на компьютер новый файл, то возможно этот сектор будет использован именно для новых данных. [2] Но пока вы этого не сделали, информация все также остается лежать на своих местах до тех пор, пока поверх неё не будут записаны новые данные;

2. При быстром форматировании, информация о файлах также остается на носителе, система лишь стирает оглавление накопителя, и удаляет таблицу файловой системы. В этом случае информация о файлах остается на носителе и не будет затерта или замена на другую при простом копировании.

Рассмотрим выполнение различных средств удаления файлов. При уничтожении информации через контекстное меню или с помощью комбинации клавиш, удаляется лишь его оглавление, атрибут, но сам файл так и остался на жестком диске. Это сделано для того, чтобы не занимать рабочее время компьютера. Полное удаление файла осуществляется с помощью замены его значения по адресу хранения на бинарную комбинацию 0x0000. Но на выполнение такого преобразования процессору необходимо задействовать собственные ресурсы, что приводит к остановке выполнения других процессов и, как следствие, замедление работы системы.

Поэтому удаляется лишь информация о файле, а физически он остаётся на носителе. [3] Рассмотрим типичные действия при удалении данных, которые делает обычный пользователь:

- Помещает папку в корзину.

• Очищает корзину.

• Проверив жёсткий диск убеждается в том, что свободного пространства стало больше, как раз в размер с удалённым файлом.

На первый взгляд, такая процедура должна гарантировано удалить данные. Но на самом деле вся структура папки и все содержащиеся в ней файлы, остались на накопителе. Система лишь стёрла информацию о них, но физически они ещё не перезаписаны другой информацией и велик шанс того, что данные еще долго пролежат на жестком диске. [4]

Для носителей информации с большим объемом, перезапись секторов хранения информации может произойти через большой промежуток времени. Это обусловлено тем, что на носителе могут оставаться еще не задействованные адреса памяти, и чтобы ресурс носителя не истратился раньше срока, внесение новой информации будет осуществляться в свободную область.

Исходя из данного принципа, любой человек, с базовыми знаниями ПК, сможет за пару тройку часов восстановить множество данных.

Для надежного удаления информации хорошо подходят специальные программы, так называемые "вайперы", они позволяют удалять файлы методом затирания. Такой метод не обеспечивает полноценную гарантию уничтожения информации, но усложняет достаточно серьезно препятствует возможности её восстановления.

Рассмотрим способ удаления файла на примере программы «Victoria». [5] После полной установки программы можно перейти в настройки и ознакомиться с широким списков методов удаления. По умолчанию приложение использует заполнения случайными данными в один проход. Один проход – это одна перезапись данных, чем больше их количество, тем надёжнее метод. Об алгоритмах удаления данных спорят достаточно много, кто-то говорит о том, что достаточно всего лишь одного прохода, а кто-то исключительно использует алгоритм Гутмана, один из самых надёжных способов затирания данных, он состоит из 35 проходов и его реализация занимает достаточно много времени.

Стоит понимать, что выбор алгоритма затирания данных должен основываться не только на надёжности, но и на времени, которое он занимает, да и постоянная множественная перезапись накопителя негативно сказывается на его долговечности. К примеру, полная зачистка жёсткого диска объёмом 150 гигабайт методом Гутмана может отнять до 20 часов. Наиболее универсальный способ затирания данных, который использует Министерство обороны США – "US DoD 5220.22-M (8-306./E, C & E) ". Данный метод реализуется на выбор тремя или семью проходами.

Программа имеет широкий выбор инициализации зачистки данных, по расписанию или вызывать для удаления конкретных файлов. Очень полезной разовой опцией может оказаться затирка свободного пространства диска, которая поможет полностью зачистить места, где хранятся ранее удалённые файлы.

Проблема всех программных методов зачистки данных состоит в основном лишь во времени их реализации, что приводит к долгому удалению даже небольших файлов.

Существует также метод частичной перезаписи данных, который заметно сложнее в реализации и вряд-ли найдутся стандартные утилиты, способные выполнять его. Данный метод, используя прямое подключение к жёсткому диску на нижнем уровне, через API драйвер диска или собственный драйвер, может быстро испортить информацию, перезаписывая промежутки данных псевдослучайными числами, напрямую указывая адрес памяти, в которых нужно выполнить запись. Также, через него можно получить адреса, в которых хранится информация, и перезаписывать только эту область данных.

Данный способ самый сложный в реализации, с другой стороны, он позволяет быстро уничтожить информацию. [6]

Работа с драйвером предполагает 2 стадии:

1. Получения адреса и длинны данных, обычно один файл разделён на диске в различных местах, поэтому мы получаем массив адресов и массив длин.

2. Запись псевдослучайных чисел в данной области памяти, её необходимо воспроизводить также, через драйвер, для того чтобы ОС не заблокировала или не перенаправила процесс в другую область диска.

Для того чтобы использовать этот метод, понадобится множество специальных знаний, но данный способ защищает нас от прочтения данных стандартными средствами ОС или другими программными утилитами.

Также один из возможных методов удаления конфиденциальной информации – это уничтожения данных вместе с самим диском, этот способ является достаточно быстрым и самым эффективным. К примеру, для уничтожения данных с жёсткого диска достаточно испортить его блины. Однако нанесение или присутствие "ранних" физических царапин не гарантирует потерю всей информации, а только на поврежденных секторах. Безвозвратное уничтожение всех данных с носителя может быть выполнено путем использования устройства "edr solutions". Оно позволяет поместить устройство под пресс и продавить его блины.

Все вышеперечисленное в большей части относится к жестким дискам и особенностям их работы, но сейчас активной популярностью начали пользоваться твердотельные накопители. Они более устойчивы к вибрациям и падениям, обладают большей скоростью чтения и записи и работают не создавая шума. Обычные программные методы на твердотельных накопителях лучше не использовать, они могут просто привести устройство в негодность.

Если рассматривать удаление данных с ssd-накопителей, то оно существенно отличается от методов для обычных жестких дисков. [7] Суть заключается в том, что в большинстве случаев, файлы, которые были удалены с ssd-накопителей, восстановить не удастся, а все потому, что отличительной чертой твердотельного

накопителя, является TRIM – специальная команда интерфейса ATA, которая, заставляет контроллер в буквальном смысле физически очищать блоки данных, которые ранее использовались для того, чтобы сохранять удаленные файлы. [8]

Достигнуть гарантированного удаления данных на ssd-накопителе достаточно просто, стоит лишь убедиться, что команда TRIM включена. Для этого в командной строке нужно вписать специальную команду: *fsutil behavior query disabledeletenotify*. Если в результате выполнения вы получите *DisableDeleteNotify = 0*, значит TRIM включена, если = 1 — соответственно отключена. Для включения TRIM (если он выключен), в командной строке нужно ввести следующее: *fsutil behavior set disabledeletenotify 0.* Чаще всего, операционные системы поддерживают данную команду по умолчанию, но на старых ОС, например Windows XP или на накопителях с файловой системой FAT32, TRIM не исполняется. [9]

Но даже если он отключен, не стоит сильно переживать за сохранность данных, т.к. большинство твердотельных накопителей ввиду архитектуры их контроллеров все равно достаточно скоро безвозвратно очистят удаленные данные. Однако время на выполнение может наступить через длительный период времени, который зависит от интенсивности использования ssd.

Из всего вышесказанного следует, что гарантированно удалить конфиденциальные данные с любого электронного носителя можно лишь его полным уничтожением. [10] Однако этот метод неприемлем для сферы бизнеса и государственного управления, поэтому способ программной зачистки данных с жестких дисков является наиболее подходящим в соотношении цена/качество. Если рассматривать альтернативу в виде применения твердотельных накопителей, то это будет экономически не выгодно, т.к. даже в самых бюджетных сравнениях, цена твердотельного накопителя почти в 1.5 раза выше, чем на жесткий диск (5,83 руб/гб против 3,89 руб/гб). Поэтому в ближайшее время в сфере бизнеса и государственного управления появления твердотельных накопителей ждать не стоит. Именно по причине распространённости жестких дисков и невозможности

идеального удаления информации с них, требуется всегда соблюдать основные правила эксплуатации данных, во избежание потенциальной кражи или взлома.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Коженевский Р.С.: Методы гарантированного уничтожения данных на накопителях на жёстких магнитных дисках // Научно технический журнал «Защита информации» №3, 2003, С. 36.
2. Удаление файлов без возможности восстановления [электронный ресурс] // Режим доступа: https://hetmanrecovery.com/ru/recovery_news/secure-data-destruction.htm
3. Как восстановить данные с жесткого диска? [электронный ресурс] // Режим доступа: https://pc-azbuka.ru/urok-13-kak-vosstanovit-dannye/
4. Болдырев А.И., Методические рекомендации по поиску и нейтрализации средств негласного съема информации. / Болдырев А.И., Василевский И.В., Сталенков С.Е. // М.:ЗАО НПЦ Фирма «НЕЛК». 2001.
5. Программа «Victoria» [электронный ресурс] // Режим доступа: https://hdd.by/victoria/
6. Программа, удаляющая файлы без возможности восстановления [электронный ресурс] // Режим доступа: https://gtavrl.ru/programma-udalyayushchaya-faily-bez-vozmozhnosti-vosstanovleniya/
7. Как восстановить данные SSD диска [электронный ресурс] // Режим доступа: https://hetmanrecovery.com/ru/recovery_news/vosstanovlenie-informacii-s-ssd-nakopit.htm#plan_1
8. Важность очистки памяти и процессов TRIM для производительности твердотельных накопителей [электронный ресурс] // Режим доступа: https://www.kingston.com/ru/blog/pc-performance/ssd-garbage-collection-trim-explained

9. Как включить TRIM для SSD в Windows и проверить, включена ли поддержка TRIM [электронный ресурс] // Режим доступа: https://remontka.pro/enable-trim-ssd-windows/

10. Корицкий Ю.В., Справочник по электротехническим материалам. / Ю.В. Корицкий, В.В. Пасынков // Т.3. Л.: Энергоатомиздат. ЛО, 1988. С.10

Нефедов В.В.,

СПбГУТ, Информационная безопасность, 2 курс магистратуры,

vit02.08.19992@mail.ru.ru

Научный руководитель:

Штеренберг С.И.,

МТУСИ, к.т.н., доцент кафедры ИБ МТУСИ,

shterenberg.stanislaw@yandex.ru

МЕТОДЫ ВНЕДРЕНИЯ САМОМОДИФИЦИРУЮЩЕГОСЯ КОДА В ИСПОЛНЯЕМЫЕ ФАЙЛЫ PE-ФОРМАТА

В современном мире большое количество пользователей используют устройства на базе операционных систем Windows и Linux. Популярность данных платформ обусловлена различными факторами. Ни для кого не секрет, что Windows, как правило, используют простые пользователи как для выполнения рабочих задач, так и для домашнего пользования. ввиду удобства данной операционной системы. Одновременно с этим можно заметить, что различные дистрибутивы, основанные на базе операционной системы Linux, почти полностью захватили рынок веб-серверов. Так, по данным рейтинга W3Techs, Unix и Linux подобные операционные системы используются на 80.2% от десяти миллионов первых доменов по рейтингу Alexa. Все остальные серверы используют Windows. Данную тенденцию можно объяснить тем, что использовать Linux на серверах наиболее выгодно, ведь эта операционная система является бесплатной. Что, в свою

очередь, дает возможность пользователям без проблем развернуть необходимый дистрибутив на сервере, минуя этапы согласования, покупки лицензии и т.д.

В связи с массовым использованием этих операционных систем возникает вопрос о их безопасности. Любая операционная система требует дополнительных специальных средств защиты информации помимо тех, которые имеются в стандартном наборе операционной системы. Обычно средства защиты информации работают в автоматизированном режиме, выполняя наиболее простые действия по защите информации, а сложные решения принимает человек на основе подготовленных шаблонов. В дополнение к имеющимся средствам защиты информации имеется возможность использовать самомодифицирующийся код, внедренный в исполняемые файлы [1]. Существует популярное мнение, что самомодифицирующийся код используется в качестве атакующего инструмента. Попадая в систему жертвы код в зараженном файле самостоятельно модифицировался, заставляя программу работать некорректно, но это можно использовать и в целях защиты информации. Например, можно «зашифровать» часть кода программного обеспечения таким образом, что злоумышленник не сможет изучить исходный код, используя различные обфускаторы и отладчики. Таким образом, скрытие части кода поможет замаскировать слабые места и значительно повысит безопасность информации.

Но возникает вопрос: куда внедрять самомодифицирующийся код? В данной работе были рассмотрены методы внедрения самомодифицирующегося кода в исполняемые файлы PE-формата.

Для начала стоит подробнее ознакомиться со структурой этих файлов. Непосредственно сам исполняемый файл представляет собой отдельный модуль с разрешением .exe, .dll, .efi, .sys и т.д. [5]. В него включены библиотеки, код, ресурсы, данные программы и т.д. Ознакомиться со структурой исполняемого файла можно на рисунке 1.

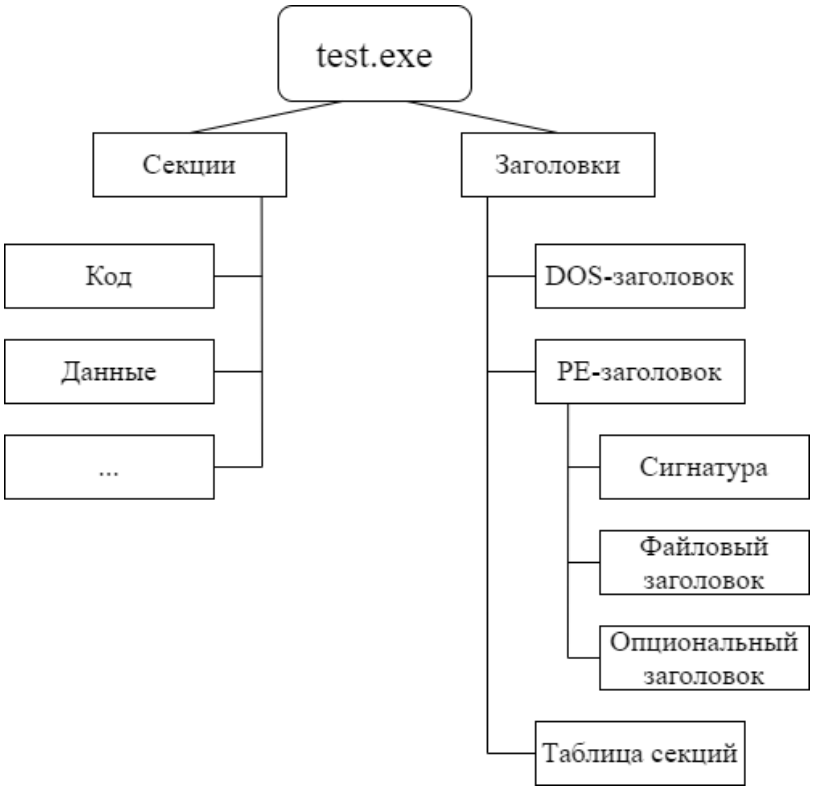


Рис. 1. Структура исполняемого файла

Исполняемый файл состоит из двух основных частей:

- Заголовки;
- Секции.

Заголовки содержат в себе технические детали об исполняемом файле (необходимые данные для загрузки программы), а секции – «начинку» исполняемого файла (код, виртуальные адреса функций, ресурсы и т.д.) [2].

Подробнее остановимся на заголовках исполняемых файлов. Все они являются обязательными и находятся в файле в определенном порядке:

- DOS-заголовок;
- PE-заголовок;
- Таблица секций.

DOS-заголовок. Данный заголовок, как и любой другой, состоит из множества полей, каждое поле хранит в себе определенное значение. Остановимся только на тех полях, которые необходимы для запуска исполняемого файла. На рисунке 2 показана структура DOS-заголовка.

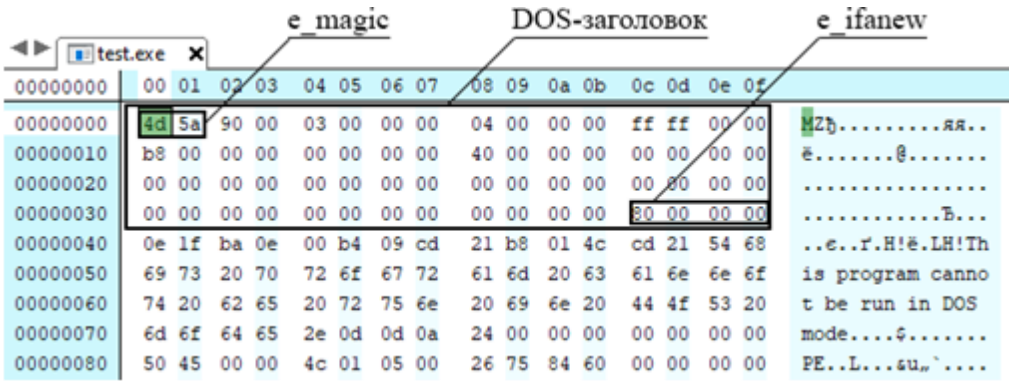


Рис. 2. Структура DOS-заголовка

PE-заголовок. Данный заголовок состоит из трех частей: сигнатуры PE-заголовка, файлового заголовка и опционального заголовка. Каждая часть также состоит как минимум из одного поля [3].

```
typedef struct _IMAGE_NT_HEADERS {
DWORD Signature;
IMAGE_FILE_HEADER FileHeader;
IMAGE_OPTIONAL_HEADER32 OptionalHeader;}
```

Листинг 1. Код PE-заголовка

Так же структура PE-заголовока показана на рисунке 3.

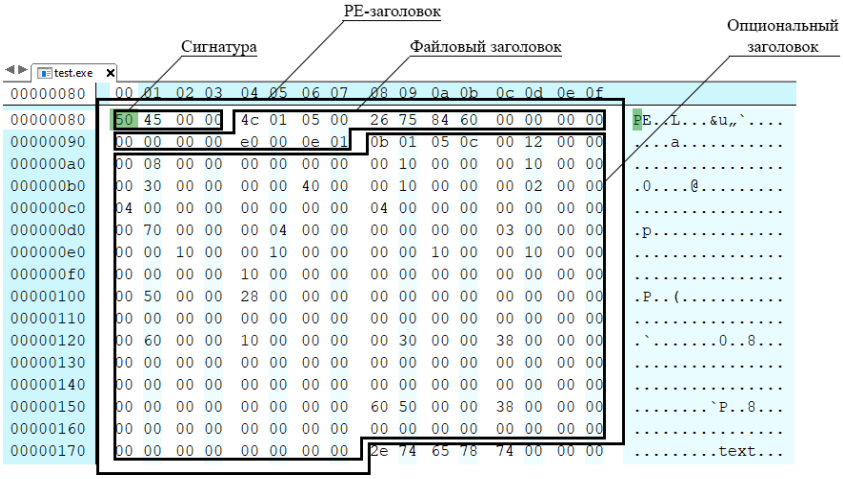


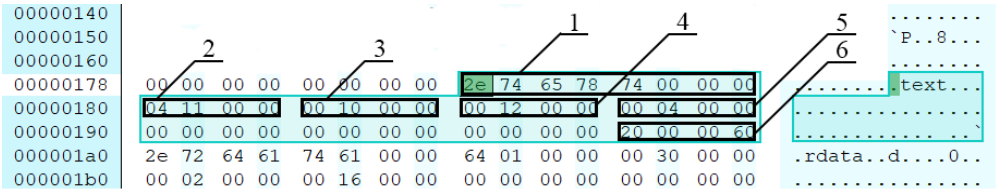
Рис. 3. Структура PE-заголовка

Начнем с сигнатуры PE-заголовка. Данное четырехбайтовое поле является началом всего PE-заголовка и содержит в себе сигнатуру 50 45 00 00 («PE/x00/x00»), указывающую на то, что это действительно PE-файл.

Далее рассмотрим файловый заголовок. В нем хранятся базовые характеристики исполняемого файла.

Опциональный подзаголовок является завершающим в PE-заголовке. В нем находится необходимая информация для запуска PE-файл [4].

Таблица секций. Завершающий заголовок, в котором хранится различная информация о секциях исполняемого файла. На рисунке 4 изображены основные поля элемента таблицы секций.



1 - Поле *Name*
2 - Поле *VirtualSize*
3 - Поле *VirtualAddress*
4 - Поле *SizeOfRawData*
5 - Поле *PointerToRawData*
6 - Поле *Characteristics*

Рис. 4. Элемент таблицы секций

После того, как были рассмотрены основные моменты, касающиеся структуры PE-файла, можно переходить к непосредственному рассмотрению наиболее популярных методов вложения в исполняемые файлы PE-формата.

1. Расширение заголовка. Важно понимать, что расширение заголовка является сложной задачей и вызывает большое количество трудностей, для решения которых приходится изменять структуру файла-носителя. Например, необходимо увеличить физический адрес начала всех секций до величины, кратной степени выравнивания, а также физически перенести конец файла, поместив тело внедряемого кода в образовавшееся место [6].

Возникает закономерный вопрос, какой объем свободного места можно получить, если прибегнуть к данному методу. Для ответа на этот вопрос стоит обозначить пару важных моментов:

- Размер заголовка не может превышать виртуальный адрес первой секции (т.е. максимальный размер заголовка равен виртуальному адресу первой секции);
- Минимальный виртуальный адрес составляет 1000h;
- Средний размер заголовка составляет 300h.

Путем нехитрых вычислений можно сделать вывод о том, что есть возможность получить порядка 3 Кб объема свободного пространства.

На рисунке 5 приведена упрощенная схема, визуально показывающая то, как происходит вложение кода с помощью расширения заголовка файла.

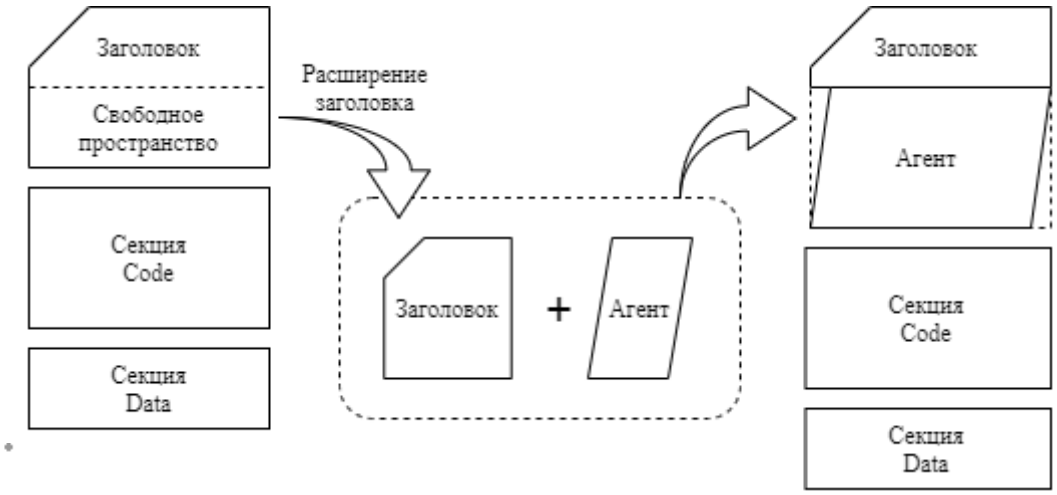


Рис. 5. Вложение кода с помощью расширения заголовка

Далее стоит обратиться к схеме, изображенной на рисунке 6, на ней показан алгоритм, которому стоит придерживаться при осуществлении вложения внедряемого кода с помощью расширения заголовка.

Для начала стоит выяснить, присутствуют ли в DATA DIRECTORY структуры, которые привязаны к своему физическому смещению. Если же такие структуры есть, то придется сделать выбор: осуществить вложение, но вручную корректировать структуры, или же отказаться от вложения. Далее нужно проверить, равен ли размер заголовка виртуальному адресу первой секции, если равен, то отказываемся от вложения, так как вкладывать банально некуда, если же не равен, то нужно убедиться, что файл-носитель не содержит оверлей, так как после вложения в такой файл, он может перестать функционировать [7].

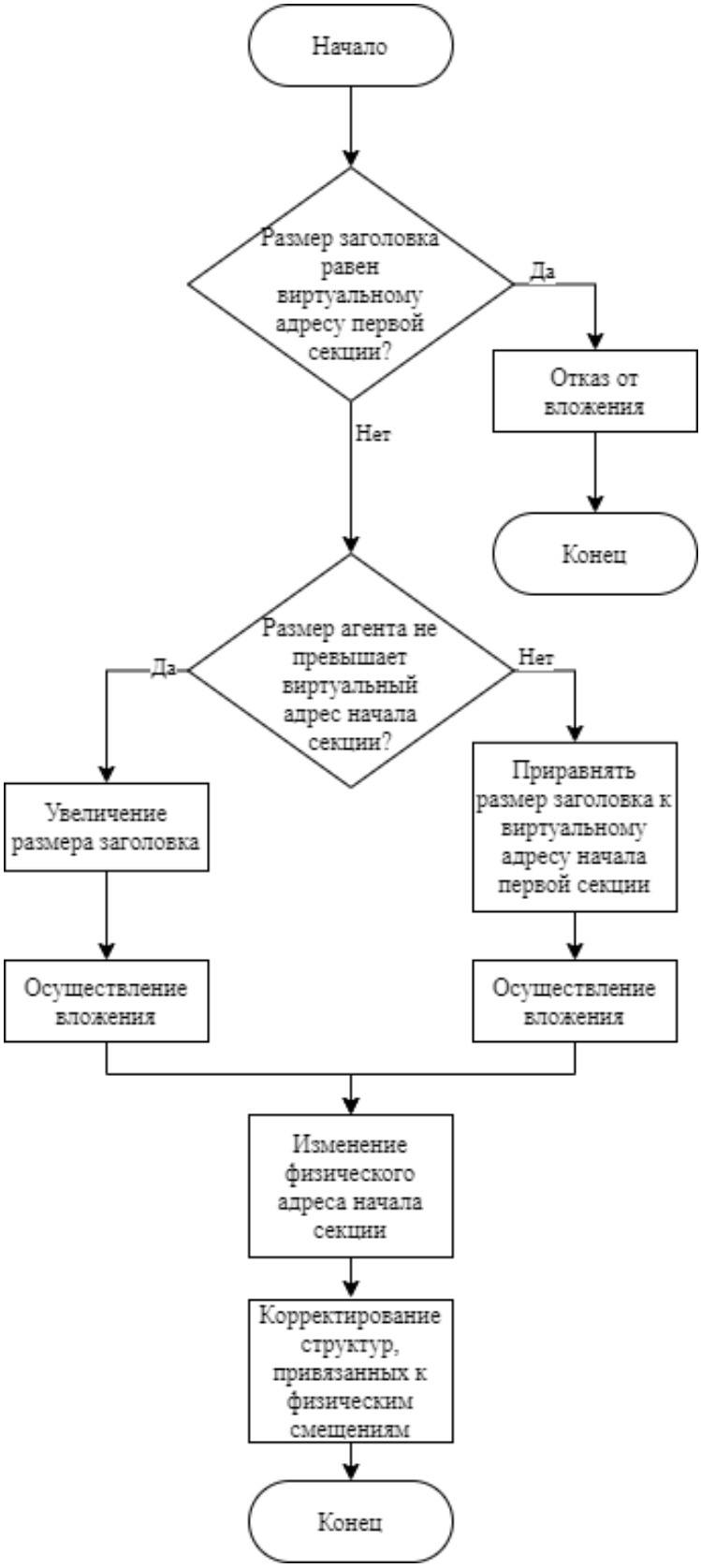


Рис. 6. Алгоритм вложения кода с помощью расширения заголовка

Следующим шагом следует проверить, меньше ли размер внедряемого кода виртуального адреса начала секции. Если да, то увеличиваем размер заголовка и добавляем необходимое количество байт (не стоит забывать про выравнивание) между концом заголовка и началом секции. Если же нет, то приравниваем размер заголовка к виртуальному адресу начала секции, после чего добавляем часть тела внедряемого кода в образовавшееся пространство. Важно понимать, что в таком случае системный загрузчик спроецирует только часть тела внедряемого кода, а все последующее ему придется подгружать самостоятельно.

Далее нужно увеличить физический адрес начала секции на величину физического расширения файла. После чего по необходимости привести в порядок все структуры, которые привязаны к физическим смещениям внутри файла.

2. Расширение последней секции файла. Данный метод является наиболее популярным. Может показаться, что он является оптимальным, ведь от разработчика требуется только поместить тело внедряемого кода в конец последней секции, увеличить размер на нужную величину (не забывая про выравнивание), после чего передать управление внедряемому коду. Но у этого метода есть существенные недостатки, которые стоит учитывать. Во-первых, такой метод является крайне конфликтным, во-вторых, его очень легко обнаружить, в-третьих, он способен работать только с некоторыми исполняемыми файлами PE-формата. Стоит отметить, что внедряемый код может изменить атрибуты последней секции на нужные ему, но это повлечет за собой уменьшение скорости работы [8].

На рисунке 7 приведена схема, показывающая то, как происходит вложение внедряемого кода с помощью расширения последней секции файла.

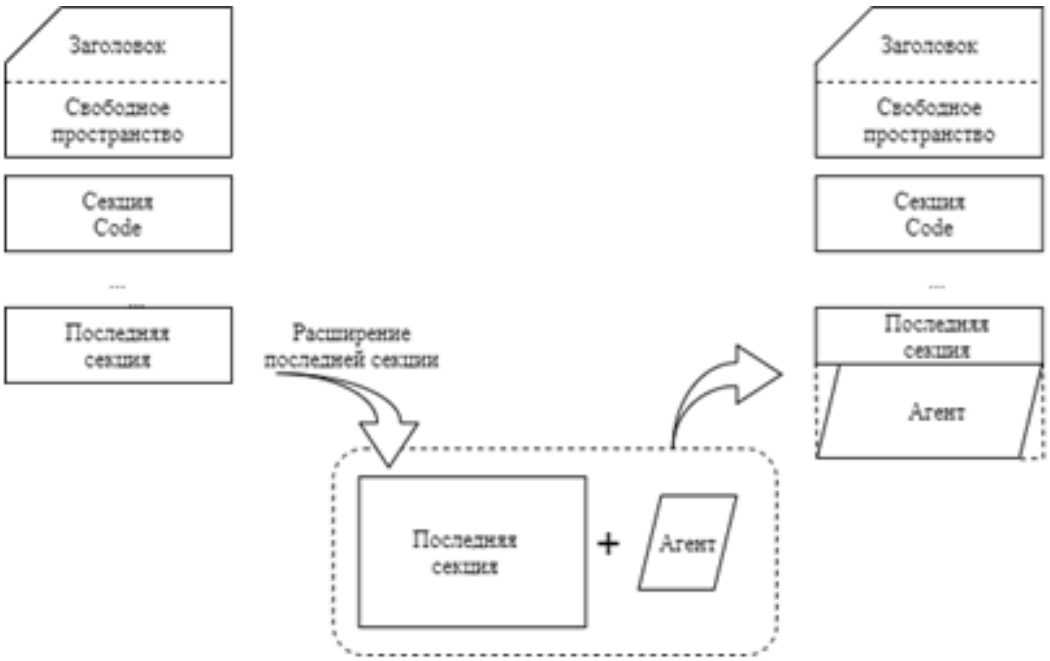


Рис. 7. Вложение кода с помощью расширения последней секции

Рассмотрим алгоритм вложения внедряемого кода с помощью расширения последней секции файла. Первым действием нужно проверить, располагают ли атрибуты секции к внедрению. Если нет (IMAGE_SCN_MEM_SHARED установлен, IMAGE_SCN_MEM_DISCARDABLE установлен и IMAGE_SCN_CNT_UNITIALIZATION_DATA установлен), то стоит либо отказаться от вложения, либо изменить все атрибуты вручную [9][10].

После этого нужно убедиться в отсутствии оверлея в файле, если он присутствует, то стоит отказаться от вложения. Следующим шагом проверяем, больше ли виртуальный размер последней секции реального размера и содержит ли конец секции нули. Если это условие выполняется, то стоит либо отказаться от вложения, либо перед передачей управления основной программе «подчистить» всё за собой.

Затем производим вложение тела внедряемого кода в файл с последующим изменением реального размера последней секции на величину *Размер файла – физический адрес начала последней секции*. Далее сравниваем виртуальный размер последней секции с физическим размером последней секции. Если виртуальный

размер оказался меньше, то приравниваем его к нулю, в противном случае оставляем как есть. При необходимости корректируем атрибуты внедряемой секции.

Алгоритм, описывающий вложение с помощью расширения последней секции показан на рисунке 8.

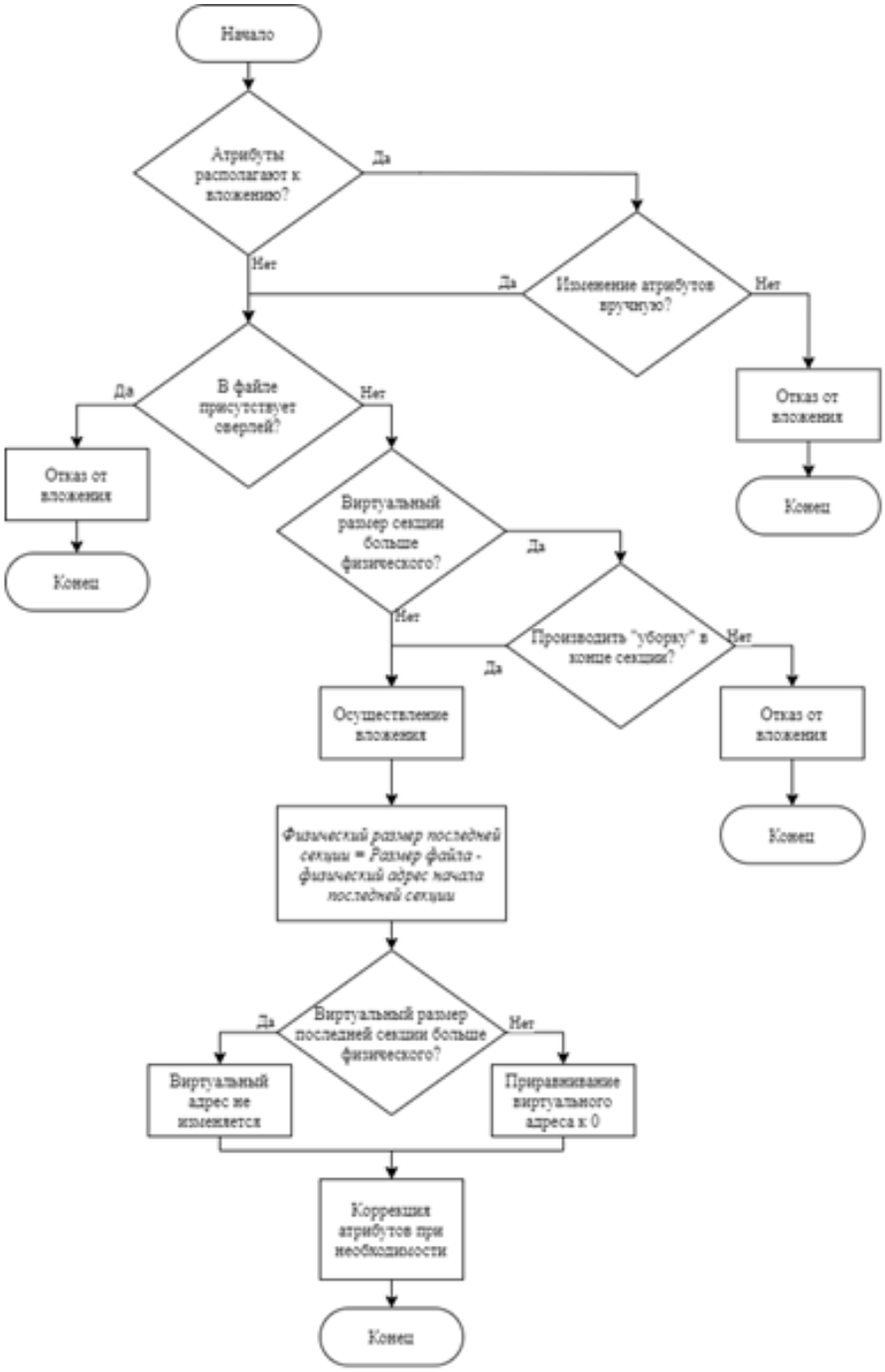


Рис. 8. Алгоритм вложения кода с помощью расширения последней секции файла

Таким образом можно подвести некие итоги. Основным результатом данной работы является описание некоторых методов вложения кода в файл, что в дальнейшем поможет значительно повысить безопасность, внедряя самомодифицирующийся код в исполняемые файлы.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Штеренберг С.И. Анализ работы алгоритмов защиты информации на основе самомодифицирующегося кода с применением стеговложений. // H&ES Research. – 2016. – № 2 – С. 86-90.

2. Исследуем Portable Executable (EXE-файл) [Формат PE-фала] [электронный ресурс] // CODEBY.NET. M., 2010 – 2021. URL: https://codeby.net/threads/0x01-issleduem-portable-executable-exe-fajl-format-pe-fajla.65415/

3. IMAGE_NT_HEADERS structure (winnt.h) [электронный ресурс] // Microsoft. M., 2021. URL: https://docs.microsoft.com/en-us/windows/win32/api/winnt/ns-winnt-image_nt_headers32

4. IMAGE_FILE_HEADER32 structure (winnt.h) [электронный ресурс] // Microsoft. M., 2021. URL: https://docs.microsoft.com/en-us/windows/win32/api/winnt/ns-winnt-image_optional_header32

5. Штеренберг С.И. Методы построения цифровой стеганографии в исполняемых файлах на основе и принципах построения самомодифицирующегося кода // Известия высших учебных заведений. Технология легкой промышленности. – 2016. – Т. 31. – №1. – С. 28 – 36.

6. Трегубенко В.В. ZeroAccess: полная биография // Хакер. 2013. №171.

7. Техника внедрения кода в PE-файлы и методы его удаления [Электронный ресурс] // URL: https://konyakov.ru/pubs/books/kris-kaspersky-r_i_p/kris-kaspersky-16.pdf

8. Malware Analysis Tutorials: a Reverse Engineering Approach [Электронный ресурс] // Dr. Fu`s Security Blog // URL;http://fumalwareanalysis.blogspot.com/p/malware-analysis-tutorials-reverse.html

9. IMAGE_DATA_DIRECTORY structure (winnt.h) [электронный ресурс] // Microsoft. M., 2021. URL: https://docs.microsoft.com/en-us/windows/win32/api/winnt/ns-winnt-image_data_directory

10. IMAGE_SECTION_HEADER structure (winnt.h) [электронный ресурс] // Microsoft. M., 2021. URL: https://docs.microsoft.com/en-us/windows/win32/api/winnt/ns-winnt-image_section_header

Свиридов В.В.,
РТУ МИРЭА, Институт кибербезопасности и цифровых технологий,
кафедра КБ-1 «Защита информации», студент,
Научный руководитель:
Головченко Д.А.,
РТУ МИРЭА, Институт кибербезопасности и цифровых технологий,
кафедра КБ-1 «Защита информации», ст.преподаватель,
Vladislavsviridov04@gmail.com
golovchenko@mirea.ru

ОТСЛЕЖИВАНИЕ ПОЛЬЗОВАТЕЛЕЙ WEB-САЙТАМИ.

В 2006 году британским бизнесменом Клайвом Хамби была произнесена фраза, на долгие годы описавшая политику компаний в отношении данных: «Данные – это новая нефть». В прошлом компании управляли только материальными активами, затем появилась интеллектуальная собственность, теперь появился новый актив – данные. Economist утверждает, что данные сыграют в XXI веке такую же роль, как нефть в XX. В таких условия неизбежно появляются компании, сконцентрированные на сборе и обработке данных, например компания Krux ежемесячно собирает данные более 200 миллиардов раз, взаимодействуя более чем с 3 миллиардами браузеров и устройств. Следящие скрипты этой компании присутствуют на тысячах никак не связанных между собой сайтов и позволяют маркетологам на основание действий пользователя показывать ему ту рекламу, которая с большей вероятностью его заинтересует.

Таким образом, можно сделать вывод о том, что так или иначе большинство web ресурсов собирают данные пользователей и более того, эти данные часто передаются третьим лицам, которые в основном используют их в рекламных целях, однако возможности их использования поистине безграничны.

Самым простым способом сбора данных являются cookies, небольшие фрагменты данных, которые хранятся на устройстве пользователя. Изначально они разрабатывались в 1995 году программистами компании Netscape Communications как средство реализации виртуальной корзины покупок для MCI. Но сейчас они обычно используются для аутентификации, хранения персональных предпочтений и пользовательских настроек и отслеживания сеанса доступа пользователя, однако сайты часто сохраняют излишнюю статистическую информацию о пользователе, которая в ряде случаев позволяет идентифицировать его по косвенным признакам.

Владельцы сайтов часто используют специализированные сервисы для получения данных о пользователях, например, «Яндекс.Метрика». В таком случае наибольшую опасность представляют не те данные, которые эти сервисы могут собрать с одного web ресурса, а совокупность всех данных, которые эти сервисы собирают о пользователях, с тысяч web ресурсов, которые их используют. Эти сервисы записывают все действия пользователя, в том числе движения мыши и нажатия на клавиатуру. На основании этих данных возможно идентифицировать личность человека, без привязки к устройствам, которые он использует.

Третий достаточно распространенный способ отслеживания пользователя — это цифровые отпечатки браузера. В данном случае для идентификации используется информация об устройстве такая как: версия операционной системы, версия браузера, ход часов, предпочитаемый язык, часовой пояс информация о CPU и GPU, разрешение монитора, список установленных в системе шрифтов, элементы кеша (они могут быть получены с помощью атаки по времени, web ресурс инициирует соединение с одним из других популярных web ресурсов и измеряет время загрузки, если оно превышает ожидаемое в случае если данные этого web ресурса уже были сохранены в кеше, то соединение разрывается), кроме того для идентификации могут быть использованы настройки браузера, отличные от стандартных, таким образом пользователи повышая свою конфиденциальность от наиболее распространенных средств отслеживания становится более уязвимым

перед другими, более сложными. Большая часть таких данных может быть получена стандартными средствами и не требует от разработчика больших усилий, но в совокупности они позволяют достаточно точно идентифицировать пользователя, причем такое отслеживание может действовать не только в пределах одного web ресурса.

Таким образом, при достаточном объеме собранных данных о пользователе возможна его однозначная идентификация по косвенным признакам при работе с сети Интернет.

Существует множество способов борьбы со сбором данных web ресурсами, но как утверждают специалисты Лаборатории Касперского: «Единственный действительно эффективный метод защиты — выключить компьютер и спрятать его в сейф».

Все большую обеспокоенность сбором данных высказывают и правительства различных стран, так, например, по действующему законодательству Европейского Союза все файлы cookies должны быть разделены на обязательные, которые необходимы для обеспечения работоспособности сайта, и необязательные, к которым относятся все остальные. При посещении сайта пользователь должен явно выразить свое согласие на сохранения, либо только обязательных cookies, либо всех. Согласно законодательству Европейского союза, некоторые данные cookies могут быть приравнены к персональным данным. В Российской Федерации так же существует прецедент, когда компания была вынуждена выплатить штраф за нарушение правил обработки персональных данных, указанных в Федеральном законе "О персональных данных" от 27.07.2006 N 152-ФЗ, применительно к обработке данных, собранных о действиях пользователя в сети Интернет, позволяющих прямо или косвенно идентифицировать пользователя.

Многие браузеры автоматически блокируют потенциально опасные cookies. Такими считаются, например, cookies, происхождение которых связано с доменом верхнего уровня (например, .com, .ru, .org и другие). Полностью отказаться от

cookies при работе в сети Интернет невозможно, но осторожное к ним отношение позволит сильно сократить вероятность отслеживания пользователя с их использованием. Так же периодическая очистка файлов cookies браузера позволяет удалять метки, которые были установлены недобросовестными web ресурсами для отслеживания пользователей.

Для блокировки следящих скриптов существует специализированные программные решения, анализирующие содержимое web ресурсов и блокирующие все скрипты, которые опознаны как отслеживающие. Они могут быть встроены в браузер, поставляться, в виде дополнений к нему или и в виде отдельного программного обеспечения, работающего одновременно для всех браузеров пользователя.

Кроме того, использование VPN или Proxy затрудняет определение примерного местоположения пользователя и его идентификацию на основании IP адреса.

Несмотря на то, что VPN является одним из самых распространённых и эффективных способов защиты от отслеживания, у него есть значительный минус. Недобросовестные поставщики VPN услуг могут собирать данные пользователей для дальнейшей их обработки, в том числе и для предоставления их третьим лицам. Существует два подхода к решению этой проблемы. Первый менее надежен и строится на доверии конечного пользователя к конкретному VPN сервису, пользователь выбирает VPN сервис, который считает наиболее надежным, внимательно читает политику конфиденциальности и в случае, если она его устраивает использует этот сервис. Этот подход достаточно прост и доступен любому пользователю, однако строится лишь на его доверии к поставщику VPN услуг. Второй подход более сложен, но и более надежен. Пользователь арендует сервер и перенаправляет свой трафик через него, по возможности настраивает шифрование. В некоторых случаях возможно построение цепи таких серверов, причем трафик шифруется таким образом, что все сервера, кроме последнего имеют доступ только к адресу сервера, на который необходимо перенаправить

данные. В таком случае даже если сервер имеет уязвимость, позволяющую его владельцу получить доступ ко всей обрабатываемой ей информации, то он не сможет получить передаваемую информацию с привязкой к конкретному пользователю. Минусы такого подхода очевидны, он дорог, увеличивает время ответа web ресурса, требует специальных знаний и излишен для обычного пользователя.

Одним из принципов построения системы защиты информации является принцип разумной достаточности, именно на его основе и строится защита от отслеживания web ресурсами. Абсолютную безопасность может обеспечить лишь полный отказ от их использования, однако существуют методы, способные значительно увеличить конфиденциальность при незначительном снижении уровня комфорта пользователя. Специализированное программное обеспечение в совокупности с иными методами повышения конфиденциальности, такими как VPN и регулярная очистка файлов cookies может обеспечивать высокий уровень борьбы с программными средствами отслеживания пользователей web ресурсов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ
2. Постановление Девятого арбитражного апелляционного суда от 23.05.2016 по делу N А40-14902/2016; Постановление Тринадцатого арбитражного апелляционного суда от 01.07.2016 по делу N А56-6698/2016.
3. Даглас Лейни Инфономика: информация как актив: монетизация, оценка, управление: [16+] / Даглас Лейни; перевод с английского [К. Ахметова]; под редакцией А. Железняка. — Москва: Точка, 2020. — 361 с.: ил.; 24 см. — (Библиотека «Айтеко»).
4. С. Кузнецов Ценность ваших данных / С. Кузнецов, А. Константинов, Н. Скворцов, – Москва: Альпина ПРО;, 2022. – 574 с.
5. Kesan, Jey; and Shah, Rajiv; Deconstructing Code Archived 2018-08-19 at Archive-It, SSRN.com, chapter II.B (Netscape's cookies), Yale Journal of Law and Technology, 6, 277–389
6. Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [Электронный ресурс]. — Режим доступа: https://eur-lex.europa.eu/eli/reg/2016/679/oj
7. Data is giving rise to a new economy [Электронный ресурс]. — Режим доступа: https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy
8. Yandex Metrica [Электронный ресурс]. — Режим доступа: https://metrica.yandex.com/about?
9. Большое Братство: кто следит за нами в Интернете [Электронный ресурс]. — Режим доступа: https://www.kaspersky.ru/blog/big-brotherhood-web-trackers/6853/
10. Как работает интернет-реклама, часть 3: отслеживание пользователей [Электронный ресурс]. — Режим доступа: https://www.kaspersky.ru/blog/internet-ads-103/13724/

Урванцев Д.Н.,
ПГТУ, студент группы БИ-51,
urvancev-00@mail.ru
Филонова М.В.,
ПГТУ, студентка группы БИ-51,
marina-layla@yandex.ru
Петухова Э.Э.,
ПГТУ, студентка группы БИ-51,
petukhova.elina99@mail.ru
Сидоркина И.Г.,
ПГТУ, зав. кафедрой ИБ, доктор технических наук, профессор
SidorkinaIG@volgatech.net

ОРГАНИЗАЦИЯ ПРОГНОЗИРОВАНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ БАНКА ДАННЫХ УГРОЗ

Актуальность темы определяется несколькими группами факторов. С одной стороны, системы обнаружения атак на компьютерные сети уже давно применяются как одно из средств защиты информации. С другой стороны, аналитические обзоры компаний, специализирующиеся в сфере интернет-технологий и защиты информации, показывают, что за последние несколько лет количество атак на различные информационные системы продолжает расти [1].

Представлен оригинальный подход к прогнозированию угроз информационной безопасности путём объединения: декомпозиции угрозы на составляющие, анализ безопасности критических точек инфраструктуры предприятия.

Исследование существующих способов прогнозирования угроз информационной безопасности для создания улучшенного подхода путём комбинирования.

Для наглядности разрабатываемого подхода изучены угрозы: УБИ.139: «Угроза преодоления физической защиты», УБИ.213: «Угроза обхода многофакторной аутентификации», УБИ.128: «Угроза подмены доверенного пользователя» банка данных угроз ФСТЭК. При построении схемы взаимодействия различных подходов прогнозирования воспользуемся открытым редактором онтологий Protégé.

Онтологии разрабатываются в целях:

1. Совместного использования людьми или программными агентами для общего понимания структуры информации;
2. Обеспечения возможности повторного использования знаний в предметной области;
3. Возможности явных допущений в предметной области;
4. Отделения знаний в предметной области от оперативных знаний;
5. Анализа знаний в предметной области [2].

Для предотвращения реализации угроз информационной безопасности необходимо их грамотное прогнозирование, чему способствует правильный выбор способов его выполнения. Наиболее встречающимися способами являются:

1. Описание тенденций изменения объекта или процесса;
2. Формирование параметров, характеризующих объект или процесс.

На основании известных способов были разработаны различные методики прогнозирования: интуитивные и формализованные [3]. Существующие методы прогнозирования/анализа (экспертная оценка, статистический анализ, факторный анализ, искусственный интеллект) имеют ряд недостатков. Недостатком большинства методов прогнозирования угроз является одностороннее рассмотрение проблемы. Для методов основанных на описании тенденций изменения объекта или процесса недостатком является невозможность отражения неизвестных атак.

Для методов основанных на формировании параметров, характеризующих объект или процесс, недостатком является невозможность отражения актуальных угроз. Это связано с тем, что усилия направлены на защиту всего периметра, а не конкретных целевых точек атаки. Частично данную проблему может решить построение модели нарушителя, но её актуальность может быстро устареть. Нивелировать эти недостатки может объединение различных подходов.

Первый рассматриваемый подход - декомпозиции угрозы на её составляющие (рис.1). Таким образом структурируется информация о данной угрозе: источники угрозы, объект воздействия, последствия, а также чем может быть обусловлена угроза и при каких условиях возможна ее реализация.

Рассмотрим одну из исследованных угроз. УБИ.139: Угроза преодоления физической защиты.

Угроза заключается в возможности осуществления нарушителем практически любых деструктивных действий в отношении дискредитируемой информационной системы при получении им физического доступа к аппаратным средствам вычислительной техники системы путём преодоления системы контроля физического доступа, организованной в здании предприятия. Данная угроза обусловлена уязвимостями в системе контроля физического доступа (отсутствием замков в помещении, ошибками персонала и т.п.).

Реализация данной угрозы возможна при условии успешного применения нарушителем любого из методов проникновения на объект (обман персонала, взлом замков и др.).

Выделены следующие характеристики угрозы:

1. Источник угрозы:

1.1. Внешний нарушитель со средним потенциалом

2. Объект воздействия:

2.1. Сервер, рабочая станция, носитель информации, аппаратное обеспечение;

3. Последствия реализации угрозы:

3.1. Нарушение конфиденциальности;

3.2. Нарушение целостности;

3.3. Нарушение доступности [4].

Декомпозиция, представленная в виде онтологии в среде Protégé, способствует наглядному пониманию предметной области.

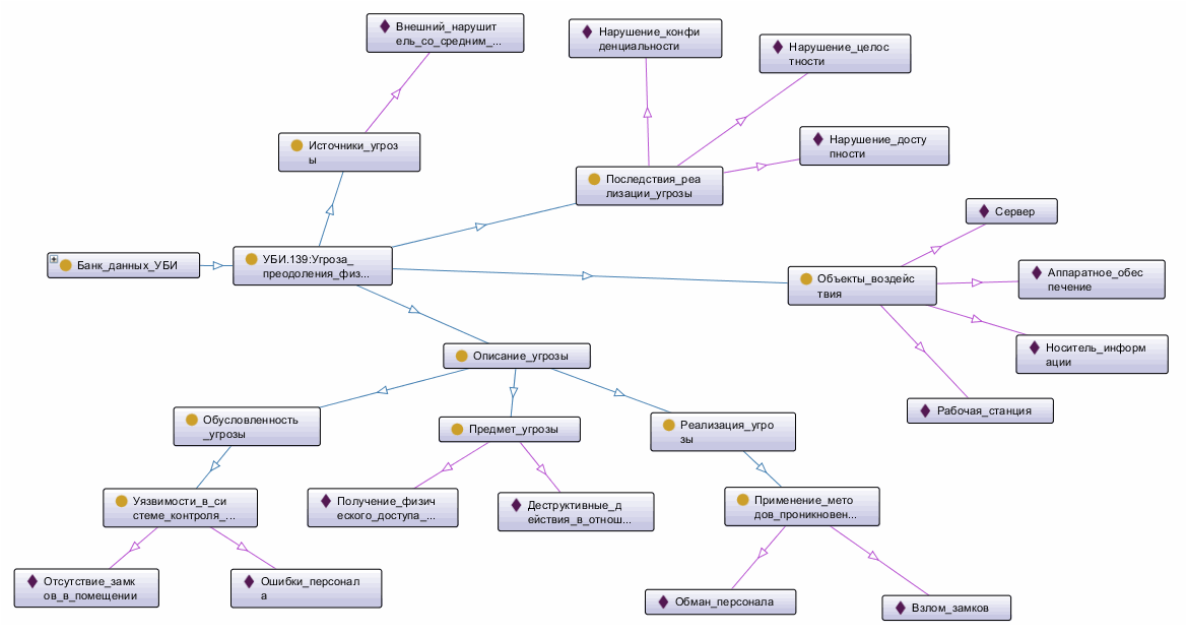


Рис. 1. Онтология декомпозиции угрозы

Второй рассматриваемый подход - анализ безопасности критических точек инфраструктуры предприятия (рис.2). Таким образом структурируется информация о важных объектах, которые должны обеспечивать защиту.

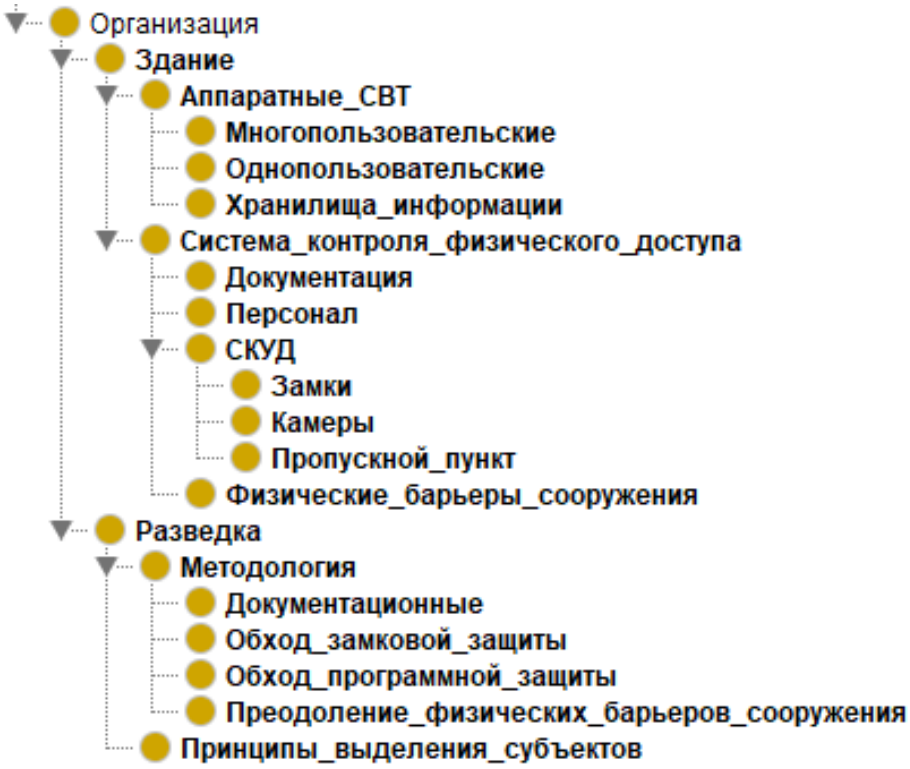


Рис. 2 Предлагаемая классовая структура организации

Для анализа безопасности критических точек требуется их выявить, выделив классы.

Первый классовый уровень подразумевает разделение организационной структуры на две области. Область разведки (нападения), которая представляет собой либо настоящего, либо псевдо-нарушителя (внутренний/внешний аудит). И область организационной структуры самого предприятия, его здания как совокупности уязвимых объектов изучаемой инфраструктуры

Второй классовый уровень представляет собой уже большую конкретизацию для данной угрозы возможных уязвимых точек, на которые может быть произведена атака с точки зрения организационной структуры. В свою очередь с точки зрения разведки второй уровень подразумевает уже общие методологические подходы в области реализации угрозы, а также может включать в себя принципы субъектирования (выделение субъекта)

Третий и далее классовые уровни визуализируют детальную классификацию предметной области по выбранному направлению защиты или нападения (разведки).

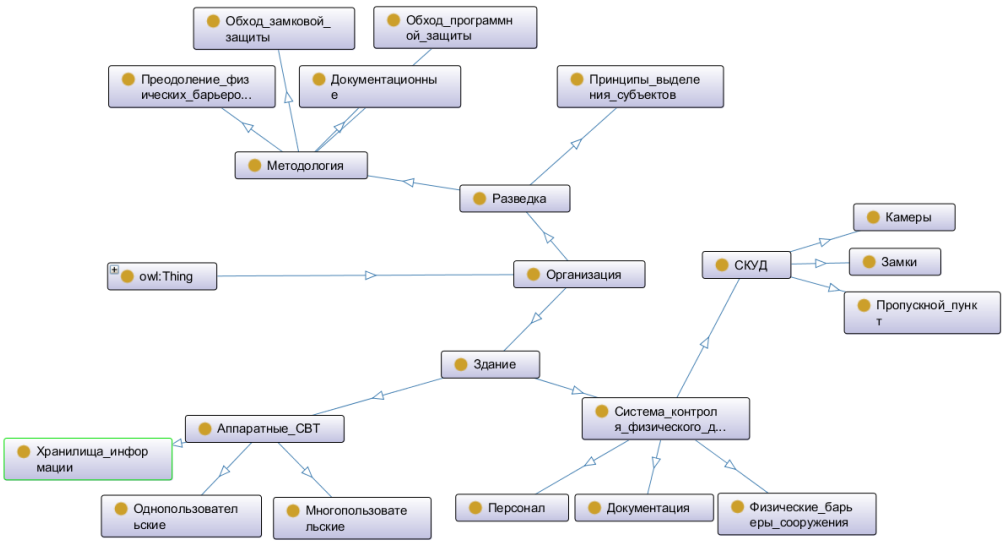


Рис 3. Предложенный онтограф инфраструктуры предприятия

Соотнесение двух представленных онтографов позволяет выявить критические точки инфраструктуры.

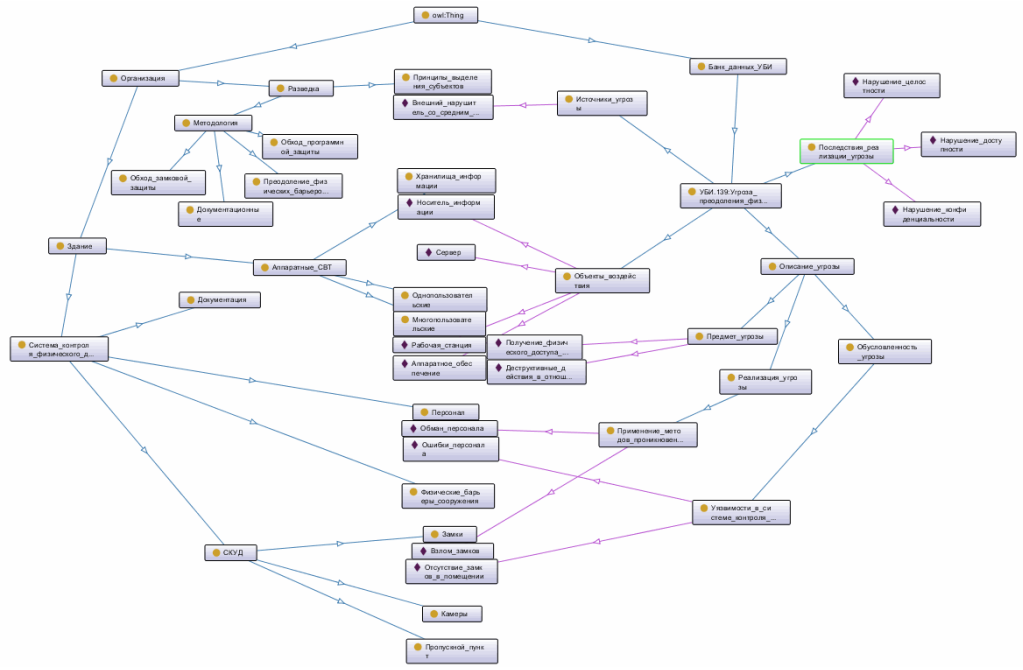


Рис. 4. Комбинированный онтограф, используемый для прогнозирования

Заключение.

Предложенная организация сочетает в себе преимущества подхода декомпозиции угрозы и анализ безопасности критических точек инфраструктуры предприятия. Это исключает недостаток одностороннего рассмотрения проблемы. В результате прогнозирования в инфраструктуре выявляются критические точки нескольких типов:

1. Точки, на которые нужно обратить внимание и добавить их в онтограф (не были учтены при проектировании инфраструктуры, но которые играют роль при реализации уязвимости);
2. Точки, которые можно не учитывать при анализе угрозы (не были учтены при проектировании инфраструктур и которые не играют роль при реализации уязвимости);
3. Точки, на которые не нужно уделять отдельное внимание (имеются в инфраструктуре, но не подвержены реализации угрозы).

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Kaspersky Security Bulletin 2010 [Электронный ресурс]. Режим доступа: http://www.securelist.com/

2. Сидоркина И.Г. Системы искусственного интеллекта [Текст]: учебное пособие / И.Г. Сидоркина. — М. : КНОРУС, 2020. — 246 с.

3. Тихонов Э.Е. Прогнозирование в условиях рынка. [Электронный ресурс]. Режим доступа: http://www.mirkin.ru/_docs/tiho.pdf

4. БДУ – Угрозы. – [Электронный ресурс]. Режим доступа: https://bdu.fstec.ru/threat

Хоромская А.Ю.,
Санкт-Петербургский государственный университет
телекоммуникаций им. проф. М.А. Бонч-Бруевича,
193232, Санкт-Петербург, пр. Большевиков д.22, к.1,
10.04.01 Информационная безопасность, 1 курс,
Angelina815@mail.ru
Научный руководитель:
Штеренберг С.И.,
Санкт-Петербургский государственный университет
телекоммуникаций им. проф. М.А. Бонч-Бруевича,
193232, Санкт-Петербург, пр. Большевиков д.22, к.1, доцент, к.т.н.,
stas.shterenberg.89@mail.ru

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ЗАЩИТА ПОЛЬЗОВАТЕЛЯ

Искусственный интеллект (ИИ) широко применяются в информационных системах для увеличения производительности труда, повышения продаж, обучения, его использование в защите от кибератак становится одним из ключевых направлений в информационной безопасности. На текущий момент количество атак растёт, а ландшафт угроз меняется с молниеносной скоростью. Продукты Kaspersky отражают более 700 млн. онлайн-атак в квартал по всему миру, а Cisco заявляет о блокировании 20 млрд. сетевых атак в день. При таких объёмах вредоносной деятельности активно применяют средства автоматизации кибератак, в том числе используют технологии искусственного интеллекта для их совершенствования и трансформации, а также для обхода известных средств защиты. Необходимо использовать ИИ для усиления атаки, встраиваясь в цепочки разговоров и используя анализ текста на естественном языке. Другой возможной сферой

вредоносного применения искусственного интеллекта мог стать более эффективный подбор паролей или обход аутентификации. Используя огромное количество различных источников данных для формирования базы знаний искусственного разума, злоумышленники могут сделать атаки на человека по-настоящему действенными. Для того чтобы справиться с растущим объёмом атак, производители систем защиты тоже начинают активно внедрять технологии искусственного интеллекта для обнаружения, прогнозирования киберугроз, реагирования на них в режиме реального времени.

С ростом технологий в ИТ-сфере всё большую актуальность приобретает вопрос о развитии и применении искусственного интеллекта в различных сферах, в том числе в системе обеспечения информационной безопасности. К основным преимуществам искусственного интеллекта можно отнести:

абсолютную память: машина способна сохранять весь массив данных и извлекать определённые фрагменты по необходимости;

точность действий: исключение «человеческого фактора»;

отсутствие эмоций: неподверженность манипуляциям и уловкам;

возможность абсолютного (предельно полного) прогнозирования всех возможных комбинаций, решений, вариантов развития событий.

Учитывая всё сказанное выше, алгоритмы искусственного интеллекта могут быть задействованы в следующих процессах:

- биометрическая аутентификация;
- ускорение обнаружения угроз;
- быстрое реагирование на атаки;
- создание динамической среды аутентификации;
- уменьшение участия человека.

Смоделируем схему применения искусственного интеллекта (рисунок 1).

Анализ данной схемы показывает, что в структуре искусственного

интеллекта важное место отводится машинному обучению, в частности, регрессионному анализу, методу статистического ансамбля, дереву решений, кластеризации, глубокому машинному обучению, что, в свою очередь, обеспечивает деятельность активно внедряющихся сегодня алгоритмов систем поведенческого анализа пользователей.

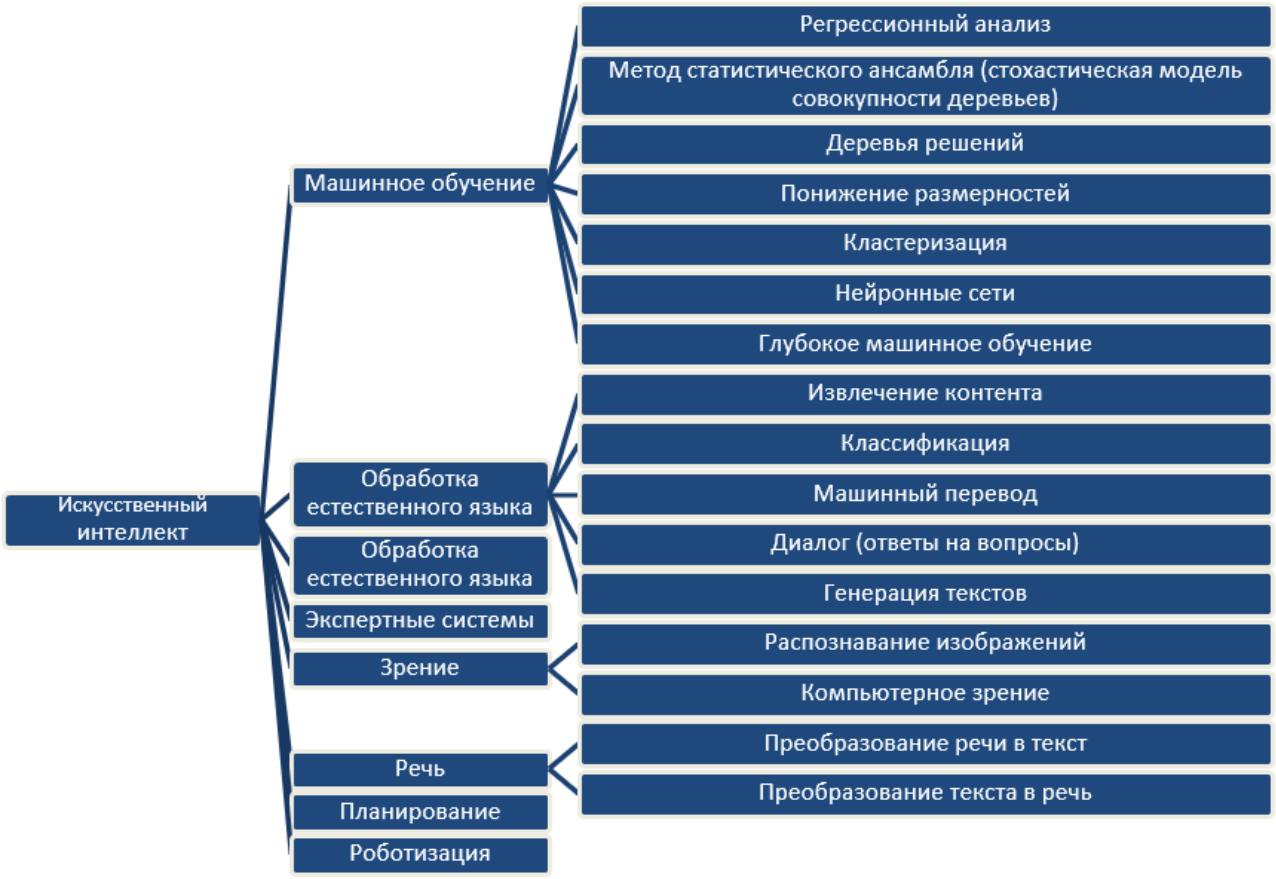


Рис. 1. Сферы применения искусственного интеллекта

Под системой анализа поведения пользователей мы понимаем решения, способные выполнить анализ поведения пользователей при помощи сбора информации на основе их действий и составить по полученным данным модель нормального поведения для каждого пользователя.

Основными целями анализа поведения пользователей считаются: упрощение процесса устранения инцидентов при помощи сокращения времени и числа сотрудников, повышение качества выявления инцидентов, а также прогнозирование и управление рисками информационной безопасности.

Задачи анализа поведения пользователей в обеспечении защиты информации:

- быстрое обнаружение атак и нарушений;
- расставление приоритетов событий при обработке информации;
- эффективное реагирование на события;
- обнаружение и предотвращение инсайдерских угроз;
- определение скомпрометированных объектов;
- мониторинг сотрудников.

Актуальность использования анализа поведения пользователей в защите информации обусловлена ростом количества данных, которые ежедневно обрабатывают специалисты. С одной стороны, развиваются технологии, причем не только в качестве части систем информационной безопасности, но и как системы, которые необходимо защищать. С другой стороны, злоумышленники изобретают новые способы нарушения конфиденциальности данных, а значит и атаки, которые изо дня в день проводятся с целью хищения информации или ее модификации в информационных системах, становятся все более «неуловимыми», то есть их становится очень сложно отличить от обычного поведения пользователей. Обгоняя темпы роста угроз, развиваются и системы защиты. Совокупность перечисленных факторов привела к появлению нового класса решений, модулей информационной безопасности.

Информация для обрабатываемого системой поведенческого анализа массива данных может поступать из различных источников:

- журналы систем безопасности;
- реестры систем контроля доступа и аутентификации;
- локальные журналы с конечных рабочих станций;

– переписки пользователей;

– данные других решений информационной безопасности и т.д.

Классифицировать продукты отобранных нами компаний, применяющие технологии поведенческого анализа и предиктивной аналитики, можно по двум направлениям: по функциональному и технологическому типу и по сценариям использования.

Рис.2. Распределение продуктов с применением технологий ИИ по сценариям использования

Перечислим основные типы:

EDR (Endpoint Detection and Response) — платформы обнаружения атак на рабочих станциях, серверах, любых компьютерных устройствах (конечных точках) и оперативного реагирования на них. С помощью технологий ИИ продукты данной

категории могут обнаруживать неизвестные вредоносные программы, автоматически классифицировать угрозы и самостоятельно реагировать на них, передавая данные в центр управления. ИИ принимает решения на основе общей базы знаний, накопленной путём сбора данных со множества устройств. Некоторые продукты данного типа используют технологии ИИ для разметки данных на конечных точках и дальнейшего контроля их перемещения, чтобы выявлять внутренние угрозы.

NDR (Network Detection and Response) — устройства и аналитические платформы, которые обнаруживают атаки на сетевом уровне и позволяют оперативно на них реагировать. Используя накопленную статистику и базу знаний об угрозах, продукты данного типа выявляют с помощью технологий ИИ угрозы в сетевом трафике и могут автоматически на них реагировать надлежащим образом, изменяя конфигурацию сетевых устройств и шлюзов. Часть продуктов данного типа специализируется на защите облачных провайдеров и их инфраструктуры. Дополнительный сценарий использования ИИ в сетевой защите — это анализ почтового трафика на предмет фишинга.

UEBA (User and Entity Behavior Analytics) — системы поведенческого анализа пользователей и информационных сущностей. Они обнаруживают случаи необычного поведения и используют их для детектирования внутренних и внешних угроз.Основной сценарий применения ИИ-технологий в продуктах типа UEBA — это автоматическое выявление аномалий в поведенческих моделях (отклонение от нормы или соответствие шаблону (паттерну) угрозы) для пользователей и различных сущностей информационных систем. Выявленные аномалии классифицируются с помощью ИИ как различные угрозы и риски для бизнеса. Аномальное поведение может выявляться в целях мониторинга и управления доступом, обнаружения мошенничества среди клиентов или сотрудников (антифрод), защиты конфиденциальных данных, проверки соблюдения тех или иных регламентов и нормативных актов.

TIP (Threat Intelligence Platform) —платформы раннего детектирования угроз и реагирования на них, действующие на основе большого количества различных данных (Data Lake) и индикаторов компрометации (IoC).Применение ИИ позволяет повысить эффективность выявления неизвестных угроз на ранних этапах; сценарий очень схож с работой SIEM-систем, но нацелен на внешние источники данных и внешние угрозы.

SIEM (Security Information and Event Management) — решения, которые осуществляют мониторинг информационных систем, в режиме реального времени анализируют события безопасности, поступающие от сетевых устройств, средств защиты информации, ИТ-сервисов, инфраструктуры систем и приложений, и помогают обнаружить инциденты ИБ. В системах такого класса накапливается огромное количество данных из различных источников, а применение технологий ИИ даёт возможность выявления аномалий эвристическими методами и сокращения ложных срабатываний при изменении паттернов и моделей данных. Применение ИИ в SIEM-системах позволяет достигнуть очень высокого уровня автоматизации.

SOAR (Security Orchestration and Automated Response) — системы, позволяющие выявлять угрозы информационной безопасности и автоматизировать реагирование на инциденты. В решениях данного типа, в отличие от SIEM-систем, ИИ помогает не только проводить анализ, но и автоматически реагировать надлежащим образом на выявленные угрозы.

Средства защиты приложений (Application Security) — системы, позволяющие определять угрозы безопасности прикладных приложений, управлять дальнейшим циклом мониторинга и устранения таких угроз. Основной сценарий применения технологий ИИ в системах защиты прикладных приложений — автоматический сбор информации об уязвимостях, атаках и заражениях, доступной в открытых источниках, и основанная на его результатах автоматизация защитных действий: сканирования на уязвимости, изменения правил защиты для веб-

приложений, выявления угроз и изменения рисковой модели.

Антифрод (Antifraud) — системы, позволяющие выявлять угрозы в бизнес-процессах и предотвращать мошеннические операции в режиме реального времени. В системах защиты от мошенничества технологии ИИ применяются для определения отклонений от установленных бизнес-процессов, тем самым помогая быстро реагировать на возможное финансовое преступление или уязвимость процессов. Применение ИИ в таких системах особенно актуально, так как позволяет быстро адаптироваться к изменению логики и различных метрик бизнес-процессов, а также использовать лучшие практики в индустрии.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Афанасьева, Д.В. Применение искусственного интеллекта в обеспечении безопасности данных // Известия ТулГУ. Технические науки. 2020. №2.

2. Козин, И.С. Метод обеспечения безопасности персональных данных при их обработке в информационной системе на основе анализа поведения пользователей // Информационно-управляющие системы. 2018. №3 (94).

3. Савенков, П.А. Использование методов и алгоритмов анализа данных в мобильной ueba/dss- системе для решения задач информационной безопасности // Известия ТулГУ. Технические науки. 2019.

4. Красов А.В., Петрив Р.Б., Сахаров Д.В., Сторожук Н.Л., Ушаков И.А. Масштабируемое Honeypot-решение для обеспечения безопасности в корпоративных сетях // Труды учебных заведений связи. 2019. Т. 5. № 3. С. 86–97.

5. Штеренберг С.И., Красов А.В., Цветков А.Ю. Компьютерные вирусы. Ч. 1. СПб.: СПбГУТ, 2015. 62 с.

6. Ковцур М. М., Герлинг Е. Ю., Коновалова В. В., Киструга А. Ю. Исследование способов удаленного перехвата трафика в корпоративных сетях // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 4. С. 68–75.

7. Ковцур М. М., Кистуга А. Ю., Петров В. А. Исследование методов дальнометрии в беспроводных сетях // REDS: Телекоммуникационные устройства и системы. 2021. Т. 11. № 4. С. 42–49.

8. Штеренберг С.И., Штеренберг И.Г. Вероятностные методы построения элементов самообучения адаптивных информационных систем: сб. науч. ст. Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2016 № 1 С. 53-56

9. Малюк, А. А. Защита информации в информационном обществе: Учебное пособие для вузов / А. А. Малюк - М.: Гор. линия-Телеком, 2015. - 230 с

10. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для бакалавриата и магистратуры / под ред. Т.А. Поляковой, А. А. Стрельцова. - М.: Издательство Юрайт, 2016. - 325 с.

Желобенко К.А.,
РТУ МИРЭА, Информационная безопасность автоматизированных систем, 5 курс,
jelobenko2014@yandex.ru
Научный руководитель:
Вершинин А.Н.,
РТУ МИРЭА, ст. преподаватель кафедры кб1 «Защита информации»,
ve.sa.2009@mail.ru

АВТОМАТИЗИРОВАННАЯ СИСТЕМА В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ ДЛЯ СОТРУДНИКОВ КОМПАНИИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Компьютерная безопасность это область знаний, охватывающая модели, методы, программные, аппаратно - программные средства, системы защиты информации при ее обработке, хранении и передаче с использованием информационных технологий. Компьютерная безопасность это защита информации на компьютере, на мобильных устройствах от различного рода случайных или умышленных её повреждений, удаления, а также защита персональных данных на компьютере от взлома и кражи. К задачам компьютерной безопасности относится стабильность работы программ, операционных систем, компьютерных сетей.

Безопасность информационных систем является частью более широкой проблемы: безопасность компьютерных систем или еще более общей проблемы информационной безопасности. В этой связи мы намерены обсудить некоторые общие подходы к безопасности, которые в значительной степени будут применимы и в отношении информационных систем.

Информации, как продукт, удовлетворяющий определенным потребностям

субъектов, который они получают посредством информационных систем, должна обладать следующими свойствами:

- Доступность информации – возможность за приемлемое время выполнить ту

или иную операцию над данными или получить нужную информацию. Заметим, что защита данных от повреждения является лишьчастным случаем защиты от нарушения доступностиинформации.

- Целостность информации это актуальность и непротиворечивость хранимой информации. Актуальность в данном случае следует понимать как оперативное отражение изменений, происходящих в предметной области, в информационной базе ИС. Непротиворечивость информации это соответствиесодержимого информационной базы логике предметной области.
- Конфиденциальность – защищенность информации от несанкционированного доступа.

Основой современных информационных технологий является автоматизированная компьютерная обработка данных. При создании распределенных систем управления информацией необходимо решать две довольно противоречивые задачи.

Первая из них состоит в том, чтобы создать систему с минимальной стоимостью. Стоимость создания подобных систем пропорциональна степени ис пользования коллективных ресурсов. Это означает, что в целях минимизации стоимости системы целесообразно создавать коллективный ресурс для всех ее пользователей, включая средства поддержки сохранения информации, программные и аппаратные средства ее обработки и доступа к другим средствам и системам. Удачно выбранные органи зация доступа и возможность коллективного ресур са значительно уменьшают стоимость создания и эксплуатации системы при реализации заданных требований к ее функционированию.

Обработка информации с использованием возмож ностей коллективного ресурса не означает, что каждому пользователю системы должны быть до ступны эти возможности. Доступность определяет ся правилами (требованиями), которые формули руются при создании системы. Именно соблюдение этих правил при делении пользователей системы на отдельные классы и предопределяет

необходимость решения второй задачи — организовать процесс передачи и обработки информации так, чтобы каждый пользователь получал только туинформа цию, которую ему разрешено получать.

Вашему вниманию предоставляю проект под названием “Создание и разработка безопасной системе в информационной структуре.”

Задача данного проекта создание защищённой изолированной системы, в ней будут использоваться различное программное обеспечение. Далее будет коротко описано каждое из них.

Удостоверяющий центр?

Чтобы получить неквалифицированный и квалифицированный сертификат электронной подписи, необходимо обратиться в один из удостоверяющих центров. Какие функции выполняют удостоверяющие центры и сколько времени займет получение сертификата?

Удостоверяющий центр (УЦ) – доверенная организация, которая имеет право выпускать сертификаты электронной

подписи юридическим и физическим лицам. Работа УЦ лежит на пересечении юриспруденции, информационной безопасности и IT-технологий.

В обязанности УЦ входят следующее:

- удостоверить личность человека, который обратился за сертификатом электронной подписи,
- изготовить и выдать сертификат, в который включены данные о владельце сертификата и его открытый ключ проверки,
- управлять жизненным циклом сертификата (выпуск, приостановление, возобновление, окончание срока действия).

Какие виды подписей выдает УЦ?

Законом «Об электронной подписи» определены три вида подписи:

- простая,
- усиленная неквалифицированная,
- усиленная квалифицированная. Получать в УЦ необходимо последние две:
- за квалифицированной подписью нужно обращаться только в аккредитованный Минкомсвязью РФ удостоверяющий центр.
- за неквалифицированной — в УЦ, который связан с той информационной системой, где планируется применять подпись. Например, выдавать неквалифицированные сертификаты для торгов могут только УЦ, аккредитованные

шестью федеральными электронными торговыми площадками. При этом УЦ может и не быть аккредитован в Минкомсвязи.

Настройте компьютер

Чтобы сертификат ФНС работал у вас на компьютере, нужно чтобы на нем была программа КриптоПро CSP и настроенный браузер. Лицензию на КриптоПро CSP налоговая включает в сертификат. Сертификат ФНС нельзя скопировать — налоговая устанавливает это ограничение для большей безопасности. Поэтому одновременно использовать его на двух компьютерах не получится. Всем сотрудникам, которые подписывают документы организации, понадобятся собственные сертификаты электронной подписи.и других порталах.

Законный представитель налогоплательщика:

руководитель организации-налогоплательщика;

индивидуальный предприниматель;

иное лицо, наделенное учредительными документами

организацииналогоплательщика.

2. Уполномоченный представитель налогоплательщика. организация или ИП, оказывающиеуслуги по подготовке и отправке отчетности (аудиторская фирма, пункт коллективного доступа, уполномоченная бухгалтерия и т.д.) сотрудник организации-налогоплательщика, не являющийся ее законным представителем (например бухгалтер);

наемный работник ИП. Уполномоченный представитель ВСЕГДА действует

на основании доверенности. Копия доверенности должна быть предоставлена в налоговый орган до начала отправки деклараций с подписью уполномоченного представителя.

Протоколы

Протокол связи — набор определённых правил или соглашений интерфейса *логического уровня*, который определяет обмен данными между различными программами. Эти правила задают единообразный способ передачи сообщений и обработки ошибок.

Сигнальный протокол используется для управления соединением — например, установки, переадресации, разрыва связи. Примеры протоколов: RTSP, SIP. Для передачи данных используются такие протоколы как RTP.

Сетевой протокол — набор правил и действий (очерёдности действий), позволяющий осуществлять соединение и обмен данными между двумя и более включёнными в сеть устройствами.

Модель OSI — 7-уровневая логическая модель работы сети. Реализуется группой протоколов и правил связи, организованных в несколько уровней:

- на физическом уровне определяются физические (механические, электрические, оптические) характеристики линий связи;
- на канальном уровне определяются правила использования физического

уровня узлами сети;

- сетевой уровень отвечает за адресацию и доставку сообщений;
- транспортный уровень контролирует очерёдность прохождения компонентов сообщения;
- сеансовый уровень координирует связь между двумя прикладными программами, работающими на разных рабочих станциях;
- уровень представления служит для преобразования данных из внутреннего формата компьютера в формат передачи;
- прикладной уровень является пограничным между прикладной программой и другими уровнями, обеспечивая удобный интерфейс связи для сетевых программ пользователя.

Протоколов большое множество.

IP — Internet Protocol

Протокол передачи, который первым объединил отдельные компьютеры в единую сеть. Самый примитивный в этом списке. Он является ненадёжным.

TCP/IP — Transmission Control Protocol/Internet Protocol

Это стек протоколов TCP и IP. Первый обеспечивает и контролирует надёжную передачу данных . Второй же отвечает за маршрутизацию для отправки данных.

UDP — User Datagram Protocol

Протокол, обеспечивающий передачу данных без предварительного создания соединения между ними. Этот протокол является ненадёжным. В нём пакеты могут не только не дойти, но и прийти не по порядку или вовсе продублироваться.

FTP — File Transfer Protocol

Протокол передачи файлов. Его использовали ещё в 1971 году — задолго до появления протокола IP. На текущий момент этим протоколом пользуются при удалённом доступе к хостингам. FTP является надёжным протоколом, поэтому гарантирует передачу данных.

DNS

Это не только система доменных имён (Domain Name System), но и протокол, без которого эта система не смогла бы работать.

HTTP — HyperText Transfer Protocol

Изначально протокол передачи HTML-документов. Сейчас же он используется для передачи произвольных данных в интернете. Он является протоколом клиент-серверного взаимодействия без сохранения промежуточного состояния.

NTP — Network Time Protocol

Не все протоколы передачи нужны для обмена классического вида информацией. NTP — протокол для синхронизации локальных часов устройства со временем в сети. Он использует алгоритм Марзулло. Благодарянему протокол

выбирает более точный источник времени.**SSH — Secure SHell**

Этапы создания ИТ-инфраструктуры компании:

Разработка и утверждение технического задания. Техническое задание (ТЗ) – является документом, который включает в себя все требования заказчика к создаваемой информационной системе.

Разработка проекта. После утверждения технического задания разрабатывается рабочий проект – документ, содержащий техническое описание

реализации требований, указанных в техническом задании.

Создание исполнительной документации. Завершающим этапом создания ИТ-инфраструктуры является создание исполнительной документации.

Аппаратная часть.

Аппаратное обеспечение — это физическая часть всей платформы. Помимо серверов, компьютеров или маршрутизаторов, сюда входят и те элементы, которые помогают поддерживать функционирование машин и устройств. К таким элементам можно отнести элементы питания, охлаждения, коммутации, а также помещения, которые под них выделены. Основным элементом является сервер.

Программная часть

В программное обеспечение входят все приложения, которые используются для внутренних целей и для предоставления услуг клиентам. ПО необходимо для работы аппаратного части

и управления ей. Операционные, CMS и CRM-системы, веб-серверы,почтовые клиенты относятся к программному обеспечению.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - М.: РиС, 2014. - 586 с.

2. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - М.: ГЛТ, 2016. - 586 с.

3. Бутакова, Н.Г. Криптографическая защита информации / Н.Г. Бутакова, В.А. Семененко, Н.В. Федоров. - М.: МГИУ, 2010. - 316 с.

4. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. - Ст. Оскол: ТНТ, 2010. - 384 с.

5. Деднев, М.А. Защита информации в банковском деле и электронном бизнесе /

М.А. Деднев. - М.: Кудиц-образ, 2004. - 512 с.

6. Емельянова, Н.З. Защита информации в персональном компьютере: Учебное пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. - М.: Форум, 2013. - 368 с.

7. Жук, А.П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - М.: ИЦ РИОР, НИЦ ИНФРА- М, 2013. - 392 с.

8. Игнатьев, В.А. Защита информации в корпоративных информационно-вычислительных сетях: Монография / В.А. Игнатьев. -Ст. Оскол: ТНТ, 2005. - 552 с.

9. Ищейнов, В.Я. Защита конфиденциальной информации: Учебноепособие / В.Я. Ищейнов, М.В. Мецатунян. - М.: Форум, 2013. - 256 с.

10. Кондратьев, А.В. Организация и содержание работ по выявлению и оценке основных видов ТКУИ, защита информации от утечки: Справочное пособие / А.В. Кондратьев. - М.: МАСКОМ, 2011. - 256 с.

Новиченко А.В.
акционерное общество «Перспективный мониторинг»,
старший аналитик
Aleksandr.Novichenko@amonitoring.ru
Хромова А.В.
акционерное общество «Перспективный мониторинг»,
системный аналитик
Anna.Khromova@amonitoring.ru

«МИКРОЦИКЛЫ» В РАБОТЕ АНАЛИТИКА

Не секрет, что весь цикл получения информации давно сведен к так называемому «разведывательному циклу». Если коротко, то это бесконечный круг, состоящий из постановки задачи, сбора сведений, их обработки, оценки и распространения (Рис. 5) [5] . Нежданов И.Ю. отметил, что на каждом этапе разведывательного цикла ценность информации повышается, т.к. информация структурируется, очищается аналитиком и приобретает уникальную форму знаний [11].

Рисунок 5 – Схема разведывательного цикла

В классическом понимании процесса информационной работы, аналитик получает задачу, собирает сведения по интересующему вопросу, обрабатывает и анализирует их. Превращенные в «разведданные» сведения оцениваются и распространяются среди заинтересованных лиц, например, докладываются инициатору. После осуществления мероприятий, для которых требовались сведения, аналитик уточняет задачу исходя из полученных данных, собирает новые сведения, обрабатывает (анализирует) их, предоставляет результат заинтересованным лицам и так вплоть до выполнения основной задачи.

На практике исполнителю иногда приходится возвращаться на один, а то и несколько этапов назад, иногда уже на этапе составления результирующего документа приходилось собирать недостающие данные и анализировать их с учетов новой информации.

В случае нехватки информации об объекте, найденной в открытых источниках, на помощь аналитику приходит поисковый синтаксис Google, поисковые операторы которого, вкупе с различными комбинациями искомых слов иногда приносят неожиданные результаты. Применяя так называемые «дорки» аналитик может получить намного больше информации, чем при простых запросах в поисковые системы.

Дорки, Google Dork или Google Dork Queries (GDQ) — это набор запросов к поисковым системам для нахождения информации на различных сайтах, всего, что должным образом не спрятано от поисковых роботов. О необходимости применения dorks и поискового синтаксиса поисковых систем Google и Яндекс постоянно напоминает один из практиков конкурентной разведки, Андрей Масалович [12].

В деятельности аналитика очень помогает то, что можно назвать «микроциклами»: в рамках одного, «первичного» разведывательного цикла, по каждому из имеющихся или найденных объектов проводится миниатюрное расследование с применением всего имеющегося в распоряжении аналитика

инструментария. В ходе такого «микрорасследования» можно найти другие «сущности», которые, в свою очередь, становятся объектами расследования.

В ходе постановки задачи саму себе, аналитик примерно представляет себе набор инструментария, список ресурсов, которые будут применены к тому или иному виду объектов.

В ходе проведения расследования аналитику приходится применять весь спектр доступных ему инструментов. В данной статье ссылки на официальные ресурсы, полукриминальные агрегаторы компромата и откровенно «мутные» боты приведены не будут, все это находится самостоятельно, если не с первого, то со второго запроса в поисковые системы, в т.ч. специализированные.

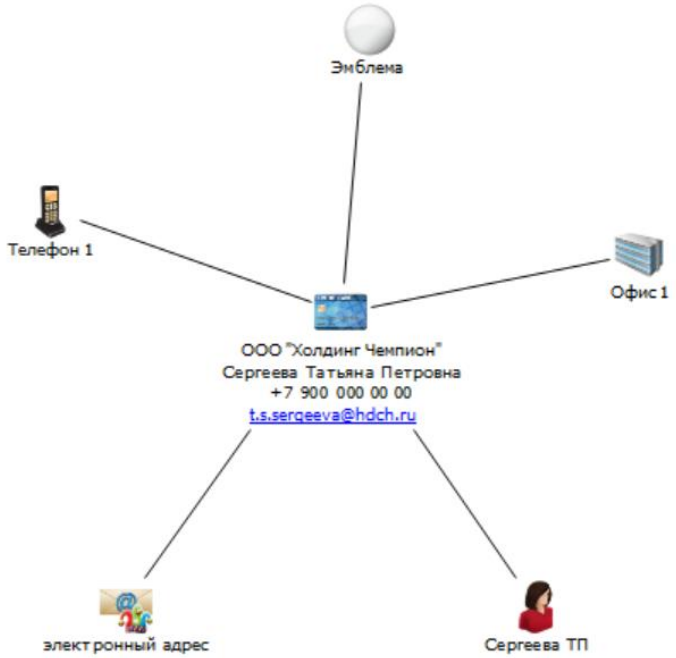
Приведем пример одного такого расследования:

Постановка задачи аналитику выглядит очень по-разному. Чаще всего это устный разговор, иногда - выписка из ЕГРЮЛ, а когда и просто ссылка на текст в Сети. В практике автора самая экзотичная постановка задачи выглядела в виде визитки. С компанией, которую представляла указанная на визитке женщина, предполагалось сотрудничество и нужно было выяснить его целесообразность.

На визитке была указана следующая информация:

– ФИО – Сергеева Татьяна Петровна.
– Название компании – ООО «Холдинг Чемпион».
– Телефон - +7 900 000 00 00
– Адрес электронной почты – t.s.sergeeva@hdch.ru.
– Эмблема компании.

Все объекты, с визитной карточки, были визуализированы на графе (Рис. 2)



.

Рисунок 6 – Визуализация исходной информации

Были поставлены следующие промежуточные задачи:

– Идентификация юридического лица, включая идентификационные данные, руководство и учредители, а также историю смены руководства и состав учредителей.

– Идентификация физического лица, установление связи с юридическими лицами, в т.ч. иностранными, а также круга рабочих и личных связей.

– Получение информации, влияющих на принятие решения о целесообразности сотрудничества в Ф.И.О. и представляемой ей компании.

Ход расследования

Ф.И.О. из-за большого количества однофамильцев информативным не оказалось. Такую задачу так просто не решить и было принято решение о проведении «микрорасследований» о каждом объекте и их сочетаниях.

В одной из поисковых систем нашлось одно фото, но оно было настолько низкого качества, что разобрать на нем черты лица было очень сложно. Однако, выкрутив все настройки графического редактора на максимум и отправив фото в Яндекс.Картинки, нашлось фото искомой женщины и незнакомого мужчины, а также упоминание, о том, что на фото «Татьяна и Иван» и у «Ивана» был указана фамилия (Сидоров). Эти данные также были перенесены на граф.

Компания ООО «Холдинг Чемпион» оказалась очень молодая, никаких активов, долгов и истории у нее не нашлось, кроме адреса регистрации, совпадающего с тем, что указан на визитке. Проведя «микрорасследование» вокруг сущности «Адрес» и применив к объекту все возможные методы, количество информации не увеличилось.

Исследовав окрестности адреса при помощи Яндекс.Панорамы, было обнаружено, что у машин, стоящих довольно далеко от точки съемки, номерные знаки не «замылены» и, скачав картинку в максимальном разрешении, номера вполне можно прочитать. Предположив, что автомобили находились на парковке, предназначенной для сотрудников, не составило труда найти данные их владельцев. Было найдено совпадение: владелец одного из автомобилей являлся полным однофамильцем Сергеевой.

Упоминание Ивана Сидорова нашлось на полупустом сайте-визитке, на котором он был указан как сотрудник с громкой, но малозначащей должностью. Однако упоминалась компания «ООО «Холдинг Чемпион», а она была указана на визитной карточке, ставшей поводом к расследованию.

Сочетание «ООО «Холдинг Чемпион» и Сидорова выдало сайт дизайнерской компании, на которых лежали макеты визиток и Ивана и Татьяны. На визитках было указано название фирмы - «Холдинг Чемпион». Также установлено, что Иван, а также некая Мария, которая, судя по всему, является дочерью Татьяны, были учредителями различных предприятий с участием иностранных граждан. Компании

декларировали участие в громких проектах с привлечением государственного и иностранных капиталов, но, судя по всему, проекты так и остались проектами.

При поиске по изображению «эмблемы» найдено, что она практически копирует другой логотип до «степени смешения». А оригинальный логотип принадлежит очень крупному холдингу из обрабатывающей отрасли и название его очень похож на название искомой компании, опять же, до «степени смешения», т.е. название ООО «Холдинг Чемпион» было очень прхоже на ООО «Компания «Холдинг Чемпион».

Представившись журналистом из несуществующей газеты «Оймяконская зарница», я позвонил по указанному номеру. Взявшая трубку женщина хоть и отозвалась на Татьяну Петровну, но была совершенно сбита с толку вопросами «корреспондента» про производство и переработку очень специфического сырья, а в Википедии расписаны подробности процесса. Таким образом подозрения о готовящемся мошенничестве окрепли. Необходимо отметить, что перед проведением мероприятий по «социальной инженерии» аналитику необходимо хотя бы поверхностно ознакомиться с вопросом, чтобы иметь хотя бы начальные знания.

Процесс поиска информации дошел до того, что в начале-середине двухтысячных годов Петрова со коллегами дружили с фальшивыми генералами, якобы войск ООН (Рисунок 33) из Средней Азии, где занимались торговлей подложными номерами ООН. Правда, информации об уголовном преследовании кого-либо за это, найдено не было.

Рисунок 3 - Фотография с «генералами» ООН

Вся полученная в ходе расследования информация была перенесена на граф (**Error! Reference source not found.**4) для наглядного отображения результатов расследования и установления ранее неизвестных связей.

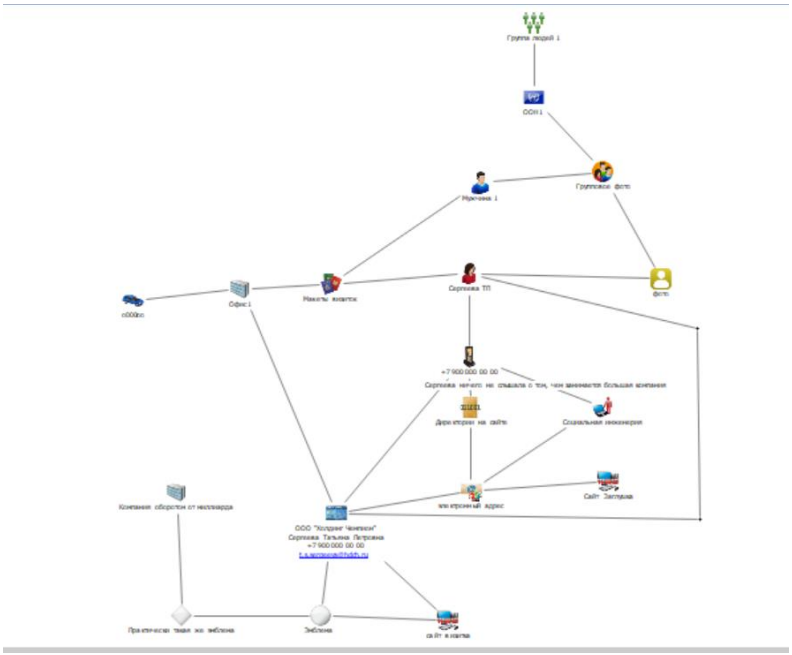


Рисунок 4 – Полученные в ходе расследования результаты

Заключение

Таким образом, проведенное расследование не ограничилось только применением методов и ресурсов к имеющимся данным, а по каждому имеющемуся объекту был применен весь спектр имеющихся возможностей, повлекших получение, на первый взгляд, мало значащих данных, но способствовавших получение информации, являющейся довольно ценной.

Физическое и юридические лица были однозначно идентифицированы, установлен круг рабочих и личный связей, получен информация негативного характера

Руководителю предоставлена справка, в которой отражены результаты работы и рекомендации аналитика.

СПИСОК ЛИТЕРАТУРЫ

1. Плэтт В. Информационная работа стратегической разведки. Основные принципы. / Пер. с английского Е. Б. Пескова. Под ред. А. Ф. Федорова— М.: Издательство иностранной литературы, 1958. – 338 с.

2. Ромачев Р.В., Нежданов И.Ю. Конкурентная разведка. — М.: Ось-89, 2007. 272 с.

3. Ющук Е.Л., Пелевина Н.А., Сергеев К.В., Ющук В.Е. Конкурентная разведка: маркетинг рисков и возможностей. – 3-е изд., доп. И переработ. – Екатеринбург: ПервоГрад, 2019. – 264с.

4. 42 оператора расширенного поиска Google (полный список).ф [Электронный ресурс] https://habr.com/ru/post/437618. – URL: (дата обращения: 14.09.2022).

5. Военная разведка П. Робинсона и Р. Н. Пухова. — М.: Центр анализа стратегий и технологий, 2021. — 376 с.

6. Блог Андрей Масалович [Электронный ресурс]. – URL: http://iam.ru/world (дата обращения: 29.10.2020).

7. Блог о конкурентной разведке [Электронный ресурс]. – URL: https://nejdanov.livejournal.com (дата обращения: 14.09.2022).

8. Ronald V. Clarke, John E.Eck. Crime Analysis for problem solvers in 60 small Steps. Office of Community Oriented Policing Services, U.S. Department of Justice 2005.

9. Бурьяк А.В. Аналитическая разведка. URL: http://analytical.narod.ru/Index.htm (дата обращения: 11.09.2022).

10. Додонов А.Г., Ландэ Д.В., Прищепа В.В., Путятин В.Г. Конкурентная разведка в компьютерных сетях. – К.: ИПРИ НАН Украины, 2013. 248 с.

11. Нежданов И.Ю. Аналитическая разведка для бизнеса. М.: Ось-89, 2012. – 336 с.

12. Андрей Масалович. Жизнь после Сноудена. Современный инструментарий интернет-разведки URL: https://www.youtube.com/watch?v=TdTq6ug8yIY (дата обращения: 14.09.2022).