

BIS

JOURNAL

ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ
БИЗНЕСА

№1 (52) 2024

**Александр
ШОЙТОВ**

Минцифры России
«Прорыв
требуется всей
экономике
данных» → 16



**Алексей
ЛУКАЦКИЙ**

«Так сошлись
звёзды —
я и Positive
Technologies...»
→ 124



ТЕМА НОМЕРА

Планирование цифровых прорывов

Максим КОРОЛЁВ

Segezha Group

ИБ в лесной
промышленности → 38

Юрий ШАБАЛИН

Swordfish Security

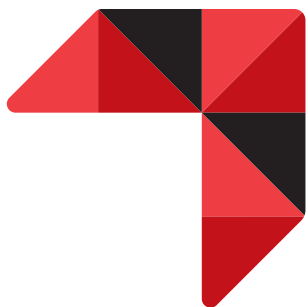
Безопасная разработка:
новая парадигма → 84

Андрей ЖАРКЕВИЧ

ООО «Антифишинг»

Security Champions.
Где они? → 90





АВАНГАРД



BIS JOURNAL



IB-BANK.RU



BIS TV

Медиа Группа «Авангард»

обеспечивает эффективную многоуровневую
бизнес-коммуникацию на рынке ИБ



проводит знаковые
деловые мероприятия
отрасли



предлагает самые
широкие возможности
медийного освещения



производит
видеоконтент



предоставляет
медиаресурсы
для решения ваших
маркетинговых задач



Воспользуйтесь уникальным
опытом и медийными площадками
«Авангарда» — с нами вы донесёте
информацию до аудитории
самым эффективным способом!



Игорь НЕКРАСОВ
главный редактор
BIS Journal

Технологический суверенитет экономики России — не просто большая комплексная задача. По сути, это вопрос выживания страны в агрессивной внешнеполитической среде.

Сегодня проблематику импортозамещения можно снимать с повестки дня — ее дискурс, построенный на точечном замещении одних конкретных технических решений, систем, услуг точно такими же, но созданными российскими руками, видоизменяется на достижение и последующее упрочение технологического суверенитета всех отраслей экономики большой страны. «Импортозамещение — это не панацея, — отметил, выступая на пленарном заседании ПМЭФ-2022, Президент РФ Владимир Путин. — Если мы будем повторять других, то рискуем оказаться в позиции догоняющего. Надо создавать свои конкурентные решения».

В русле этой идеи развитие отрасли высоких технологий можно сравнить с грандиозными проектами советского времени — атомным, космическим, — только еще более сложным, поскольку его задача не только в том, чтобы создать уникальные технологии и готовые решения, а «бесшовно» модернизировать на их базе всю российскую экономику.

«Невозможно обладать всеми научными решениями, — поясняет Владимир Путин. — Но нам надо иметь все критически важные технологии, чтобы при необходимости наладить в короткие сроки собственную продукцию».

Это состояние подразумевает технологический паритет с мировыми лидерами в области высоких технологий, продукцию которых можно встретить на всех предприятиях России. А такой паритет подпитывается только постоянным развитием научно-технической составляющей, обеспечивающей нужный уровень развития по всем перспективным направлениям «цифры»: от передовых математических методов обработки цифровых данных до реализации в «железе» новых технологий микроэлектроники. Иными словами, новые исследования и разработки в каждый момент времени должны отвечать на актуальные вызовы «расширяющейся цифровой вселенной».

BIS Journal начинает разговор на эту большую тему со своей стороны — стороны информационной безопасности.

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Батранков Д. В. — руководитель направления сетевой безопасности Positive Technologies
Былевский П. Г. — шеф-редактор, доцент департамента ИБ Финансового университета при Правительстве РФ, доцент кафедры международной ИБ МГЛУ, кандидат философских наук
Велигура А. Н. — председатель комитета по банковской безопасности Ассоциации российских банков, руководитель комитета по безопасности НП «НПС», CISA, кандидат физико-математических наук
Виноградов А. Ю. — старший научный сотрудник ФГУП «ЦНИИХМ»
Вихорев С. В. — советник генерального директора по информационной безопасности IT Expertise
Дзержинский Ф. Я. — независимый эксперт
Зубков А. Н. — генеральный директор ООО «Медиа Группа „Авангард“», директор Фонда содействия развитию безопасных информационных технологий (ФСРБИТ)
Калашиников А. И. — управляющий директор Центра информационной безопасности дочерних и зависимых обществ Газпромбанка (АО)
Курило А. П. — советник по вопросам ИБ ФБК и FBK CyberSecurity, кандидат технических наук
Левиев Д. О. — председатель Совета НП «Партнёрство специалистов по информационной безопасности»
Мельников С. Ю. — заместитель генерального директора ООО «Лингвистические и информационные технологии», доктор физико-математических наук
Некрасов И. В. — главный редактор журнала
Одувалов М. В. — директор службы Управления по обеспечению информационной безопасности ДБ Банка ВТБ (ПАО)
Окулесский В. А. — вице-президент по информационной безопасности ЦМРБбанка, кандидат технических наук
Пазизин С. В. — заместитель начальника Управления по обеспечению информационной безопасности ДБ Банка ВТБ (ПАО), кандидат физико-математических наук
Филипчук А. А. — технический директор ГК ЦРТ
Хайретдинов Р. Н. — заместитель генерального директора ГК «Гарда»
Шумский Л. С. — руководитель службы информационной безопасности Яндекс Банка
Янсон И. А. — бизнес-партнер по информационной безопасности, Департамент безопасности ПАО «Сбербанк России», кандидат физико-математических наук

РЕДАКЦИЯ ЖУРНАЛА

Главный редактор: **Некрасов И. В.**
 Директор по развитию: **Минаков А. В.**
 Арт-директор: **Мельников Н. С.**
 Руководитель интернет-проектов: **Воробьева А. А.**
 Обозреватели: **Бродская М. А.**, к. т. н., **Покатаева Е. Н.**
 Иллюстрация на обложке: **Виктор Миллер Гаусса**
 Фото в номере: **Freerik**
 Цветокорректор: **Наumenko М. В.**

УЧРЕДИТЕЛЬ-ИЗДАТЕЛЬ

ООО «Медиа Группа „Авангард“»
 Адрес: 127473, Россия, Москва, 3-й Самотечный переулок, д. 21
 Тел.: +7 495 921 42 44
 Интернет-версия: ib-bank.ru/bisjournal
 E-mail: bis@ib-bank.ru

Зарегистрирован 13 августа 2010 года Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) как «BIS Journal — Информационная безопасность банков».

Зарегистрирован 11 июля 2023 года Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) как «BIS Journal — Информационная безопасность бизнеса». Свидетельство ПИ № ФС77-85487 от 11.07.2023 г.

Все права на материалы, опубликованные в номере, принадлежат журналу «BIS Journal — Информационная безопасность бизнеса». Перепечатка и воспроизведение иными способами без разрешения редакции запрещаются. При использовании материалов ссылка на журнал обязательна. Мнение редакции может не совпадать с мнением авторов. Присланные материалы не рецензируются и не возвращаются. Возрастная категория 16+.

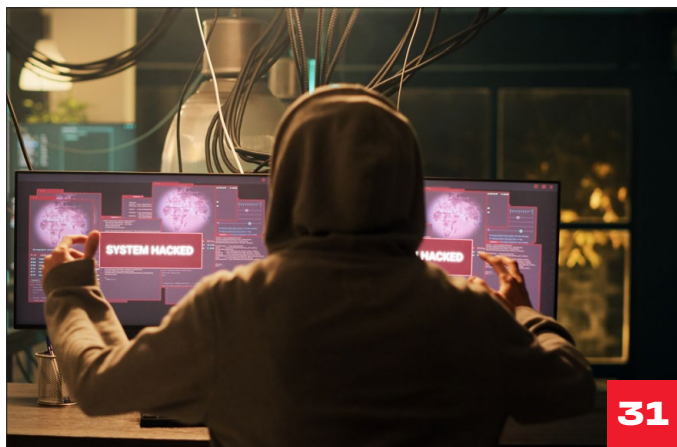
Подписан в печать 31.01.2024. Тираж 5000 экз. Заказ № 1182024.
 Цена договорная. Отпечатан в типографии «Московский Печатный Двор», 123298, г. Москва, 3-я Хорошевская 18, корп. 1, офис 201А

АКТУАЛЬНОЕ МНЕНИЕ

- 4 **Киберустойчивость**
Станислав Кузнецов (Сбербанк)
Фокус на проблемы ИБ
- 5 **Доверие**
Андрей Курило (ФБК)
А защищена ли ИС?
- 8 **КИИ**
Фёдор Музалевский (RTM Group)
Категорирование: что дальше?
- 10 **Большие перемены**
Рустам Гусейнов (РАД КОП)
Прямо сейчас...

НОВОСТИ

- 12 **Технологии, криминал, законодательство**



31

ТЕМА НОМЕРА: ПЛАНИРОВАНИЕ ЦИФРОВЫХ ПРОРЫВОВ

- 16 Александр Шойтов (Минцифры)
«Сегодня прорыв требуется всей национальной экономике данных»
- 24 Дмитрий Михеев, Константин Родин (АйТи Бастион)
Цифровизация – это не только внедрение инноваций

РЕГУЛЯТОРЫ

- 28 **От первого лица**
Василий Пискарев (Государственная Дума)
«Мы не сможем защитить свой суверенитет, не обеспечив технологическую самостоятельность страны»
- 31 **Есть вопрос!**
Александр Виноградов (ФГУП «ЦНИИХМ»),
Константин Грачёв (ООО «Максима»),
Анастасия Николаева (BIS Journal)
Тест на проникновение: чего-то не хватает...

ИБ В ОТРАСЛИ

- 38 **Лесная промышленность**
Максим Королев (Segezha Group)
Лес и цифра
- 42 **Банки**
Юрий Кардюков (eKassir),
Алексей Шарненков (МКБ)
Пример двустороннего движения
- 48 **Банки**
Ольга Горюкова (Свой Банк)
Запускаем умную антифрод-систему

УГРОЗЫ И РЕШЕНИЯ

- 52 **Экосистемы**
Анна Катанкина (BIS Journal)
Новая версия ОС
- 54 **HTTP/2 Rapid Reset**
Даниил Бобрышев (Servicepipe DosGate)
«Атаки с технологией HTTP/2 Rapid Reset проще детектируются...»
- 56 **Автоматизация**
Максим Пятаков (CtrlHack),
Виктор Сердюк (ДиалогНаука)
Автоматизация тестов на проникновение

УГРОЗЫ И РЕШЕНИЯ

- 59 **Персональные данные**
Александр Клевцов (InfoWatch)
Новая парадигма от InfoWatch
- 60 **Прогнозы**
Евгения Колодина, Василий
Окулесский, Илья Геймур (ЦИБИТ)
Кибербезопасность-2024

ИНФРАСТРУКТУРА

- 62 **Деловые мероприятия**
Марина Пересильд (BIS Journal)
SOC Tech 2023
- 66 **Деловые мероприятия**
Анна Катанкина (BIS Journal)
Антифрод Россия 2023
- 69 **Деловые мероприятия**
Марина Бродская (BIS Journal)
**Национальный проект
«Экономика данных»**
- 72 **Термины и понятия**
Денис Батранков (BIS Journal)
Новая технология удаленной работы
- 76 **Контейнеризация**
Никита Ладоскин (Positive Technologies)
**Контейнеры – наименее
безопасное окружение**
- 81 **Контейнеризация**
Тимофей Титков
(Лаборатория Касперского)
Безопасность изолированной среды

БЕЗОПАСНАЯ РАЗРАБОТКА

- 84 **Финансовый сектор**
Юрий Шабалин (Swordfish Security)
Безопасная разработка: виток развития
- 86 **Supply chain**
Мария Зубченко (Yandex Cloud)
Спасительный SLSA
- 90 **Организация труда**
Андрей Жаркевич (Антифишинг)
Security Champions

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

- 94 **Дейтинг**
Роман Журавлёв (VK)
Мошенничество на сайтах знакомств
- 98 **ИБ + МВД**
Василий Окулесский (ЦМРБанк)
По следам преступлений
- 100 **ИБ + МВД**
Сергей Вихорев (IT Expertise)
Преступление без наказания

ЗА РУБЕЖОМ

- 102 **Дайджест ИноСМИ**
Марина Бродская (BIS Journal)
Регуляторы всех стран, ужесточайтесь!
- 108 **Законодательство**
Александр Виноградов (ФГУП
«ЦНИИХМ»), Сергей Меньшиков
(Belarusian InfoSecurity Community),
Андрей Ситнов (независимый
эксперт), Валерий Соколенко (ICBC)
ОДКБ. Республика Казахстан

СУБЪЕКТЫ

- 113 **Большая теория**
Рустам Гусейнов (BIS Journal)
Вернём и вырастим ребёнка Энгельбарта!
- 116 **Новые книги**
Слово о кванте
- 118 **История**
Борис Столпаков (историк криптографии)
300 лет назад
- 124 **Лица ИБ**
Алексей Лукацкий (Positive Technologies)
**«Так сошлись звёзды –
я и Positive Technologies...»**
- 130 **Заметки безопасника**
Сергей Вихорев (IT Expertise)
Недекларированные подарки
- 132 **Заметки безопасника**
Александр Игонин (BIS Journal)
В жерновах процессов

ФОКУС НА ПРОБЛЕМЫ ИБ

О КЛЮЧЕВЫХ НАПРАВЛЕНИЯХ, ПО КОТОРЫМ
ОСУЩЕСТВЛЯЕТСЯ КИБЕРДАВЛЕНИЕ НА РОССИЮ



**Станислав
КУЗНЕЦОВ**
заместитель
Председателя
правления
Сбербанка

Станислав Кузнецов во время выступления на пленарной сессии «Устойчивость в BANI-мире: преграды, стратегии и возможности» на SOC-форуме наиболее просто и ясно сформулировал ситуацию в сфере информационной безопасности. Он рассказал, что постоянное и регулярное кибердавление на Россию осуществляется по четырём ключевым направлениям.

DDOS-АТАКИ

По мнению спикера, они направлены на то, чтобы остановить работу компаний. С начала специальной военной операции Сбер выдержал свыше 550 атак. Всего по стране таких атак было зафиксировано порядка 19 тыс. — и это только по официальным данным, ведь в реальности таких атак больше. В ноябре Сбер отразил сильнейшую в своей истории DDoS-атаку мощностью 1 млн запросов в секунду — в России такой атаки не было никогда. Важно понимать, что инструменты DDoS-атак в даркнете сегодня доступны всем.

КРАЖА ДАННЫХ

Сейчас в России насчитывается 1,5 млрд строк скомпрометированных персональных данных. Эти кражи стали более изощрёнными: пытаются украсть уже не просто номера телефонов, а государственные секреты. И проблема заключается в том, что большинство компаний и организаций не делятся информацией об утечках.

Станислав Кузнецов: «То, что компании не делятся информацией об утечках, — это проблема. И, может быть, нам об этой проблеме вместе с регуляторами стоит подумать. Мы не сможем оздоровить наше общество, если компании будут скрывать проблемы. Надо не штрафовать компании за то, что их атаквали, а придумать другую мотивацию, чтобы они делились этой информацией. Когда мы фиксируем атаки на некоторые компании, мы предлагаем мгновенную помощь. Но какую получаем реакцию? „У нас всё в порядке! Ничего не произошло“. Проходят сутки, двое... В этот же момент теми же инструментами могут атаковать других. Поэтому уровень культуры в профессиональном сообществе ИБ точно требует определённой корректировки».

ХИЩЕНИЕ СРЕДСТВ У ГРАЖДАН

С. Кузнецов отметил, что, по экспертным оценкам, объём похищенных у жителей России средств значительно выше, чем по официальным данным. Многие компании не раскрывают свои данные. В основном хищения происходят через телефонное мошенничество, которое постоянно эволюционирует. Преступники всё чаще заставляют своих жертв идти на террористические акты, в частности поджигать военкоматы, а также брать кредиты, чтобы отдать заёмные средства мошенникам. По данным Сбера, под давлением преступников россияне взяли кредитов на 200 млрд рублей.

ИНФОРМАЦИОННЫЕ ВОЙНЫ

Продолжается использование дипфейков для создания ложных новостей. Многие случаи сопровождаются информационными атаками. Сила информационных войн колоссальная, мы многое недооцениваем, заметил С. Кузнецов. Ущерб от кибератак растёт не только в России, но и по всему миру. От

действий киберпреступников в 2023 году пострадали такие известные компании, как Boeing, ICBC и другие.

Станислав Кузнецов: «Хорошая новость в том, что мы стали сильнее за последний год. Отдельное спасибо регуляторам за то, что у нас улучшилось регулирование, лучше стали работать правоохранительные органы. Они стали быстрее реагировать и результаты об этом свидетельствуют. У нас появились другие инструменты обмена информацией. Сформирован рынок кибербезопасности. Сегодня мы его можем очерчивать по границам и в цифрах. Появились разные инструменты координации профессионального сообщества».

По мнению спикера, осложняет борьбу с киберпреступностью отсутствие единого главного координатора от государства, единой общестрановой онлайн-платформы для обмена данными по киберугрозам в режиме онлайн, а также единых правил защиты для всех организаций и граждан. Ещё одна важная проблема — растущий кадровый дефицит в сфере ИБ. И, наконец, сложность, которая возникла относительно недавно в связи с импортозамещением: нередко отечественные решения стоят дороже, но менее качественны.

Как объяснил Станислав Кузнецов, фундамент совершенствования кибербезопасности должен состоять из четырёх основных кирпичиков. Это национальная платформа фрод-мониторинга, национальный аналитический центр киберугроз, координационный SOC и система профессионального обучения и сертификации, то есть подготовка кадров. Соответственно, именно на этих направлениях всему профессиональному сообществу, компаниям и государству необходимо фокусироваться в ближайшее время. Это нужно делать как можно быстрее и всем вместе.

А ЗАЩИЩЕНА ЛИ ИС?

К ВОПРОСУ О ДОВЕРИИ И ОЦЕНКЕ ЗАЩИЩЁННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ



Андрей КУРИЛО

советник вице-президента по вопросам ИТ-безопасности Услуги финансовым институтам (ФБК), советник по информационной безопасности ФБК CS, к.т. н., доцент

На фоне проблем, касающихся защищённости российских информационных систем, публично озвученных в последнее время, несколько на втором плане остаётся вопрос качества оценки защищённости этих систем, а ведь от этого зависит многое, в том числе и реальный общий уровень защищённости, и тот набивший оскомину вопрос о утечках больших объёмов персональных данных, и многое другое. Интуитивно сообщество специалистов по информационной безопасности чувствует, что те контроли защищённости, которые последовательно исторически возникали и широко применяются (аттестация, проверка, аудит, оценка соответствия), по-прежнему не дают ясного ответа на простой вопрос: а защищена ли система от актуальных и современных атак? Или, говоря более современным языком, неизвестно, какова величина остаточных рисков информационной безопасности системы? Да ещё и практика последних нескольких лет подбрасывает статистику результативных атак на российские информационные системы. Причём больше инцидентов возникает в организациях, напрямую не относящихся к оборонному комплексу или КИИ.

ДЕВЯТЬ ВИДОВ ПРОВЕРOK

Интуитивно сообщество реагирует на эти вызовы традиционным

запретительным способом, хорошо известным на Руси: увеличивает число разнообразных проверок, усиливает отчётность и повышает штрафы за очередные утечки данных, которые уже и так давно украли, потому что эти меры нужно было вводить лет 7 назад. А сейчас нужно думать о том, как защитить граждан от использования против них украденных данных, ибо огромные штрафы не дадут желаемого результата, но могут быть применены избирательно, хотя я рад был бы ошибиться.

А проверок мы насчитываем уже девять видов, и все они, похоже, нужны, но их девять — и каждая со своими затратами, отвлечением персонала от реальной работы, толстыми отчётами (средний «вес» отчёта по аудиту 500 листов) и с остаточной неопределённостью каждой проверки, ибо оценки интегральной защищённости объекта после этих проверок как не было, так и нет.

Да и доверять этим результатам, очевидно, нужно с осторожностью. Не зря Банк России говорит о «необходимости создания дополнительных правовых механизмов повышения качества оценки соответствия защиты информации в организациях кредитно-финансовой сферы и формировании требований к обеспечению достоверности результатов внешнего аудита»¹. Фактически речь

идёт о дефиците доверия к результатам оценки. Действительно, а можно ли верить результатам проверки, работа по которой выиграна кем-то в конкурсе на электронных торгах по цене 90 тысяч рублей при стартовой цене 2 миллиона? Ведь это не экономия, а профанация, оплатить работу специалиста этими средствами невозможно, потому что практически всё уходит на приобретение бумаги для отчёта и чернил.

А ЧТО ТАКОЕ ДОВЕРИЕ?

А что такое доверие? Мы широко пользуемся этим понятием в обиходе, оно попало в терминологию по информационной безопасности, например, широко используются понятия «доверенная среда», «доверенные АПК», «уровни доверия» и т.д. И базируется оно на уверенности в том, что объект, с которым мы работаем, «опираемся» на него, является надёжным, не подведёт, отвечает нашим ожиданиям, ему можно доверять, в него можно верить.

Но в сфере информационной безопасности полагаться на веру невозможно. Необходимы объективные подтверждения, основания для уверенности, поэтому доверие в этой сфере опирается на надёжную и объективную информацию о том, что объект, на который мы «опираемся», защищён.

Таким образом, применительно к проблематике информационной безопасности, доверие — это основание для уверенности в том, что конкретная реализация системы защиты адекватно удовлетворяет четырём свойствам безопасности (целостность, доступность, конфиденциальность и ответственность)². Причём выражение «адекватно удовлетворяет» однозначно указывает на связь понятия «доверие» с идеологией риск-менеджмента, о чём прямо

¹ Банк России. Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2023–2025 годов. Москва, 2023.

² NISTIR7298.

сказал Б. Шнайер: «Безопасность — это управление рисками, а процессы безопасности — это способ уменьшения рисков»³.

Результаты, обеспечивающие получение реальной информации о защищённости систем и существенно влияющие на повышение уровня доверия, могут быть получены только в результате квалифицированной проверки, проведённой оценщиком, который, в свою очередь, должен сам пользоваться достаточным доверием, а его квалификация и надёжность могут быть оценены, проверены и подтверждены. Это отдельная крайне важная задача.

ЧТО ОБЕСПЕЧИТ ДОВЕРИЕ?

Что может обеспечить доверие:

- ♦ построение системы защиты на основе адекватной модели угроз и политики безопасности, включая решение организационно-технических проблем и получение уверенности в том, что система построена правильно;

- ♦ доверие к оценщику, который должен зарекомендовать себя как квалифицированный, опытный субъект, имеющий практику проведения соответствующих работ и не замеченный ни в демпинге, ни в подтасовке результатов работы, ни в антиконкурентной деятельности;

- ♦ грамотный методический подход к оценке защищённости, в том числе на основе риск-менеджмента и зрелости процессов менеджмента;

- ♦ увязывание результатов деятельности по обеспечению информационной безопасности с результатом работы организации в целом как показателя качества и снижения рисков бизнес-процессов.

Задача эта не новая и не является исключительной для сферы ИБ, она давно исследована и проработана в рамках аналогичных исследований по повышению доверия к результатам финансового аудита и сформулирована в виде набора инструментов, приведённого в международных стандартах

ИСО/МЭК 17021-1:2015, ГОСТ Р ИСО/МЭК 27006-2020, ГОСТ Р ИСО/МЭК 17021-1-2017.

Но в нашем случае всё несколько сложнее.

Очевидны два аспекта:

- ♦ необходимо обеспечить точность оценки, обеспечивающую доверие и, главное, адекватную реалиям жизни в условиях интенсивных кибератак;

- ♦ результаты разных видов оценок должны быть интерпретированы в понятную и удобную форму, позволяющую делать адекватные выводы и принимать адекватные решения.

ТРИ УРОВНЯ

Что касается первой задачи, доверие к деятельности по обеспечению защищённости ИС обеспечивается на трёх уровнях (этапах).

1. Подготовительном (разработка методического аппарата и инструментария, используемого для оценки).

Понятно, что оцениваться должны важнейшие показатели, характеризующие защищённость системы или влияющие на неё.

На этом уровне необходимо добиться точности используемой методики оценки и правильно выбрать критерии оценки защищённости.

Тут нужно понять, что имеется в виду, когда мы говорим об оценке защищённости. В настоящее время одновременно присутствуют следующие идеологические концепции:

- ♦ все требования по защите должны быть выполнены в полном объёме, только в этом случае система считается защищённой;

- ♦ система считается защищённой, если она соответствует установленному протоколу соответствия, который характеризует достаточный уровень защищённости;

- ♦ система способна отражать атаки на самые ценные для неё ресурсы, чтобы не возникали недопустимые для неё события. Атаки второстепенного уровня допустимы;

- ♦ защищённость системы характеризуется отсутствием известных уязвимостей.

По каждому направлению существует своя методологическая база, стандарты, требования и т.д. Всё это

находится в различной стадии проработки и готовности. Например, в кредитно-финансовой сфере цель практически достигнута, и сейчас идёт совершенствование методического аппарата в направлении уточнения отдельных требований по защите и снижения трудоёмкости работ. Да и показывает себя система под кибератаками достаточно неплохо.

Сейчас становится понятно, что на стабильность уровня защищённости оказывают сильное влияние процессы менеджмента, а значит, нужно оценивать их уровень зрелости. Однако общей ясности нет.

Следует, однако, отметить, что есть ещё один не до конца прояснённый вопрос.

Совершенно непонятно, какова вероятность успешной атаки на информационную систему при установленном нормативном коэффициенте соответствия, характеризующем объём выполнения требований по защите. В документах Банка России, который продвинулся в этом вопросе существенно дальше других регуляторов, такой коэффициент установлен как 0,92 от общего объёма требований. А какова вероятность успешной атаки на защищаемый ресурс в этом случае? А какова будет эта вероятность при выполнении 100% требований по подходу ФСТЭК? И какая нас устроит: 10-1 или 10-5? Вопрос не исследован, ответа не существует. Но очевидно, этот параметр следует оценивать за достаточно большой период времени, 3-5 лет, и что вероятность успешной атаки будет разной для разных видов атак и зависит от частоты атак, их длительности и сложности. Можно предположить, что для атак типа DDoS оно должно находиться в пределах 10-5, а для АРТ-атак — в пределах 10-2. Именно такая информация гораздо понятнее владельцу системы, чем нынешние абстрактные показатели.

2. Этап собственно оценки.

Точность и достоверность результатов оценки определяются:

- а) качеством работы оценивающей команды, её способностью правильно сформулировать контекст оценки, умело применить методику

³ Секреты и ложь. Безопасность данных в цифровом мире / Б. Шнайер. — СПб.: Питер, 2003. — 368 с.: ил. — (Серия «Классика computer science»).

К фактору, затрудняющему процесс оценки, следует отнести отсутствие механизма приведения результатов различных видов проверок к интегральному показателю защищённости

оценки, точно и объективно оценить уровень защищённости проверяемой организации;

б) квалификацией привлекаемых экспертов. К сожалению, до сих пор отсутствует понятие «аудитор информационной безопасности», в отличие от финансового аудита, где оно чётко определено федеральным законом. В целом в данном вопросе царит анархия и к проверкам привлекаются организации и люди, подчас не имеющие необходимых статуса, подготовки и квалификации. Достаточно посмотреть на наборы квалификационных требований к экспертам, предъявляемые на электронных торговых площадках. Через раз — наличие квалификационных сертификатов (CompTIA, PenTest+, CEN, CPT, CEPT, CMWAPT, CRTOP, LPT, GIAC, OSCP, GPEN и т.д.), которые в нынешней ситуации вообще невозможно получить гражданину России. Значит, люди, имеющие такие сертификаты, обладают заведомыми конкурентными преимуществами. Какая тут честная конкуренция, на которую направлены механизмы торгов и соответствующие законы? Но регуляторы и ФАС в эту сторону даже не смотрят. Отмечу, что есть много вопросов к демпингу в ходе торгов, а также существенному влиянию на результат закупочных подразделений, приоритет которых — не качество работы, а экономия средств.

В целом в силу ряда причин субъективного характера на этом этапе результаты оценки в наибольшей степени подвержены искажению.

3. На этапе эксплуатации, в ходе практической деятельности по обе-

спечению информационной безопасности ИБ в организации, реальный уровень защищённости определяется прежде всего степенью зрелости процессов менеджмента информационной безопасности или модели возможностей процессов (в терминологии стандарта COBIT 5).

А степень зрелости процессов менеджмента прежде всего определяет:

- ♦ полноту покрытия «поверхности» защищаемой информационной системы требованиями по безопасности и защитными мерами;

- ♦ полноту и своевременность выполнения требований по безопасности и защитных мер самой организацией.

- ♦ способность организации сохранять достигнутый уровень безопасности (поддерживать измеренный в ходе оценки уровень защищённости) и противостоять факторам, приводящим к деградации процессов менеджмента и как следствие — деградации уровня защищённости.

Деградация зрелости процессов неминуемо приводит к снижению защищённости системы, как правило, это происходит незаметно и ненаблюдаемо (латентно) для руководства организации. Таким образом, формально и официально мы опираемся на результаты оценки, а реально уровень защиты может быть другой, гораздо ниже, чем мы думаем.

Итак, некачественная деятельность оценщиков и деградация процессов менеджмента и есть основные факторы увеличения как риска утраты доверия к их деятельности, так и риска снижения защищённости информационных систем. К фактору, затрудняющему процесс оценки, следует

отнести отсутствие механизма приведения результатов различных видов проверок к интегральному показателю защищённости.

Что касается вопроса интерпретации результатов разных видов оценок в понятную и удобную форму, позволяющую делать адекватные выводы и принимать адекватные решения, то речь идёт прежде всего об интеграции результатов проверок в рамках упомянутых идеологических концепций в общую систему оценки защищённости. При этом, похоже, в неё нужно включать ещё и оценку зрелости процессов менеджмента как основного фактора, влияющего на сохранение измеренного уровня защищённости в течение длительных сроков эксплуатации системы.

НЕГАТИВНЫЕ ФАКТОРЫ ВЛИЯНИЯ

Как повысить доверие к деятельности оценщика?

Это системная задача. И чем точнее и раньше будут идентифицированы негативные факторы влияния, тем лучше.

Попробуем их обозначить.

1. Отсутствие методологии расчёта интегральных показателей оценки защищённости.
2. Отсутствие понятия и статуса аудитора ИБ.
3. Отсутствие системы контроля качества выполненных работ по оценке защищённости.
4. Проблемы с подготовкой кадров, отсутствие системы профессиональной подготовки и квалификационных экзаменов для аудиторов (оценщиков, контролёров) ИБ.
5. Отсутствие антидемпингового механизма и механизма, обеспечивающего развитие конкуренции и качества выполняемых работ.

Это и есть перечень вопросов, которые необходимо разрабатывать с целью повышения доверия к деятельности в области аудита, оценки соответствия и консалтинга в сфере информационной безопасности.

КАТЕГОРИРОВАНИЕ: ЧТО ДАЛЬШЕ?

О ПЕРСПЕКТИВАХ РЕГУЛИРОВАНИЯ КИИ



Фёдор МУЗАЛЕВСКИЙ
директор
технического
департамента
RTM Group

В прошлом году исполнилось пять лет Постановлению Правительства РФ № 127, определяющему правила и порядок категорирования КИИ. Это не просто круглая дата – по замыслу регулятора, через пять лет субъекты КИИ (критической информационной инфраструктуры) уже должны провести эту процедуру повторно. Однако в этом направлении всё ещё много непонятного, начиная с того, какие организации считать объектами КИИ. Неудивительно поэтому, что некоторые из них до сих пор не провели категорирование даже однократно. Что всех их, а заодно и отрасль, ждёт дальше? Какие шаги предпримет регулятор? Разберёмся вместе.

КИИ ИЛИ НЕ КИИ?

ФСТЭК ещё в 2019 году заявлял о том, что общее число субъектов КИИ можно оценить примерно в 500 тысяч. При этом часть из них даже не догадывается о том, что должна следовать 187-ФЗ и, как следствие, проводить категорирование (не говоря уже о защите значимых объектов). Почему так? Прежде всего, из-за отсутствия чётких критериев принадлежности к КИИ. В упомянутом выше Постановлении есть единственная формулировка, но она может неоднозначно трактоваться, да ещё и содержит абсолютно нечёткие понятия,

такие как «функционирование в отрасли». В результате случаются казусы. К примеру, к функционирующим в горнодобывающей отрасли предприятиям ФСТЭК отнёс водоканал (!), а предприятие, не имеющее ничего общего с оборонзаказом, Минпромторг включил в перечень оборонно-промышленного комплекса (ОПК). Когда перечень предприятий ОПК оказался у ФСТЭК, его специалисты просто разослали по нему письма с требованием провести категорирование. При этом часть предприятий, получивших такие сообщения, ранее даже не была в курсе, что является частью ОПК нашей страны.

Несмотря на сложности на этом этапе, больше половины субъектов КИИ всё же сделали первые шаги к исполнению законодательства, проведя категорирование. У некоторых в результате был обнаружен значимый объект (или объекты), и мероприятия должны были продолжиться соответствующими манипуляциями по его защите. Другие, кто не обнаружил значимых объектов, расслабились и успокоились. Причём до сих пор пребывают в уверенности, что им делать ничего не нужно. Однако это не так: все субъекты КИИ должны выполнять повторное категорирование через пять лет, а также актуализировать данные в случае ввода или вывода из эксплуатации объектов КИИ, получения гособоронзаказа, изменения финансовых результатов и так далее. И эта задача гораздо масштабнее по числу вовлечённых субъектов, чем защита значимых объектов, которых всего несколько тысяч.

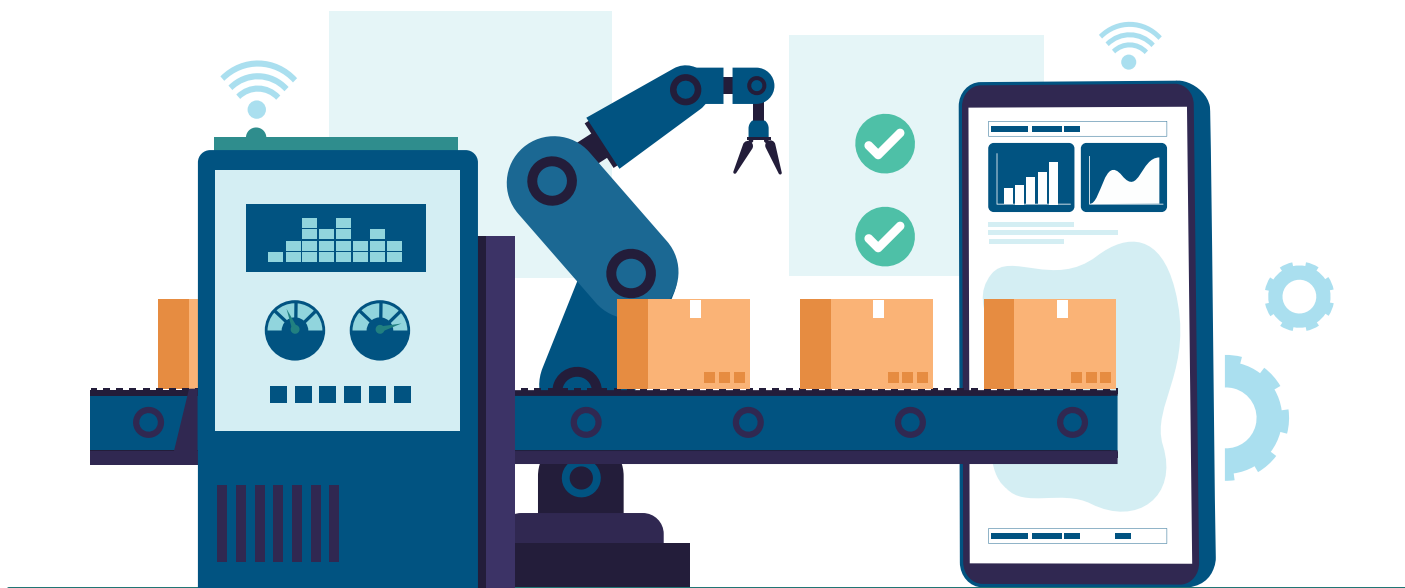
НО ЕСТЬ НЮАНСЫ

Само категорирование провести оказалось не так просто. Для начала ведь необходимо создать комиссию по категорированию, поняв, кого в неё можно включить (а это непросто). Да,

законодательство (например, пункт 11 Постановления Правительства) даёт на этот счёт пояснения, но они неактуальны для большей части субъектов (поскольку они не обрабатывают гостайну, не имеют подразделения гражданской обороны и так далее). А вот явно указать, что в комиссию должен входить бухгалтер или экономист, который владеет данными о налогах и сборах, законодатели по какой-то причине не захотели.

Конечно, в настоящее время ответы на распространённые вопросы по категорированию можно найти в сообществах, на информационных ресурсах и в системах автоматизации документов. В частности, могут помочь сервисы SECURITM, «АЛЬФА ДОК» и MEDOED. С помощью всего этого этапы работ, ранее у неподготовленного субъекта КИИ занимавшие недели, сейчас решаются за пару часов. Ну и справедливости ради следует отметить, что ФСТЭК крайне терпеливо реагирует на некорректные (по его мнению) документы, и о наказаниях субъектов, например, неправильно сформировавших комиссию, нам неизвестно. Но потраченное на согласование, создание неправильных документов и их переделку время этот факт, разумеется, не компенсирует.

Ещё один нюанс заключается в том, что все субъекты, независимо от значимости, подчиняются сразу двум регуляторам: ФСТЭК и тому, который соответствует их отрасли (Минпромторгу или Минтранспорту, например). Оба они могут проводить проверки, направленные (хотя бы теоретически) на повышение безопасности. Помимо этого, свой контроль осуществляет прокуратура. Заметно, что мощностей регуляторов не хватает: так, ФСТЭК провёл в 2023 году всего несколько десятков полноценных проверок (в основном по



ЗОКИИ) — капля в море. Объём проверок на 2024 год вряд ли заметно масштабнее: у регуляторов просто ограничены ресурсы в плане персонала.

Отраслевые регуляторы пошли чуть дальше — они создают отраслевые центры компетенции. Один из таких центров (НПП «Гамма» — центр компетенций Минпромторга) провёл в 2023 году уже несколько тысяч проверок подведомственных субъектов (в основном по корректности категорирования). При этом данная организация уделяет внимание не только формальному соответствию букве закона, но и фактической вовлечённости персонала в процесс работы с КИИ. Обычный устный опрос членов комиссии по категорированию весьма показателен. Реакция регулятора на результаты проверки пока отсутствует, но очевидно, что им придётся принимать меры.

К ЧЕМУ ГОТОВИТЬСЯ?

Что ещё ждём в ближайшее время, помимо усиления деятельности регуляторов по проверкам? Должны появиться также требования по самооценке либо независимому аудиту. Так, уже известно об инициативах по разработке стандартов оценки зрелости субъектов КИИ, и активно циркулируют слухи о создании отдельного управления в структуре ФСТЭК, которое будет заниматься проверками КИИ.

Также сам процесс контроля должен в перспективе наладиться, уйдут

несоответствия и вопросы, противоречия. Они иногда могут касаться неожиданных вещей. Обычно аудит (прокуратуры, ФСТЭК, центра компетенции) запрашивает различные бумажки. Так вот, есть случаи, когда прокурорская проверка требовала у ломбарда(!) результаты выполнения требований 187-ФЗ, ссылаясь на то, что эта организация работает в сфере финансового рынка. И формально прокуратура была права. Однако это противоречит реальности: суммарный оборот всех ломбардов, вместе взятых, вряд ли достигает нижней границы обороты значимых объектов КИИ, а их штат не позволяет компетентно проводить такие работы. Так что очевидно, что регуляторам необходимо поддерживать сведения в актуальном состоянии, да и просто не совершать противоречащих логике поступков.

Субъектам КИИ также необходимо заниматься комплаенсом, внимательно относиться к срокам и документам. Это довольно трудоёмкая задача, особенно с учётом меняющихся форм отчётности и даже состава показателей значимости. Для её решения можно привлекать аутсорс, содержать штат специалистов, а также использовать упомянутые уже средства автоматизации.

Разумеется, основной контроль рано или поздно переместится на субъекты КИИ, которые владеют значимыми объектами, и акцент будет сделан на их защиту. Но в этой

части подводных камней пока не меньше — нет чёткого порядка согласования, шаблонов проектной документации, есть лишь скупые требования ФСТЭК с наборами мер и требований. Однако и здесь уже сформирована определённая практика, и она также нашла отражение в услугах аутсорсинга, профессиональных сообществах и средствах автоматизации.

Резюмируя всё вышесказанное, отметим, что КИИ идёт по пути плавного усиления контроля и ужесточения ответственности. Когда-то в сфере персональных данных даже после появления 152-ФЗ в течение нескольких лет практически не было наказаний, массовых проверок, а сейчас уже доросли до возможности отправить жалобу в РКН, появился проект закона об оборотных штрафах. Такая же судьба ждёт и КИИ. И меньше проблем будет (как и меньше расходов) у тех, кто начнёт раньше, — проект по категорированию, в 2018 году стоивший условные 100 рублей, в 2023-м стоит уже 350 тех же условных рублей. Сказывается и общее повышение цен, и уровень внимательности регулятора к результатам. Наступает время написания документации и превращения этой задачи в постоянный процесс.

ПРЯМО СЕЙЧАС...

О БЕЗОПАСНОСТИ ПРИЛОЖЕНИЙ И ИИ



**Рустам
ГУСЕЙНОВ**
председатель
кооператива
«РАД КОП»,
radcop.online

В непрерывном потоке новостей об очередных чудо-помощниках¹ или подборках GPT-агентов² можно не заметить самой важной проблемы, связанной с AI. Изначально проблематика DevSecOps и современного AppSec, встроенного в CI/CD, возникла из условий рыночной гонки компаний за клиентами. Когда перед организациями встала необходимость быстрее адаптировать приложения к потребностям пользователей и бороться за их внимание и деньги. Ускорять изменения. Обеспечивать сверхбыстрое масштабирование проектов без потери надёжности. Это, в свою очередь, породило потребности в новых инструментах и подходах к работе. Распространились контейнеры и их оркестраторы, набрали популярность low-code-платформы и облачные сервисы. И вот теперь в этой среде возникает всё более острая потребность в информационной безопасности — об этом свидетельствует огромное количество продуктов, решений и направлений услуг, связанных с тематикой безопасности приложений.

ПОПУЛИЗМ ИЛИ ОБЪЕКТИВНАЯ НЕОБХОДИМОСТЬ?

Но почему это происходит и о чём свидетельствует? По мнению автора,

главный фактор связан со стремительностью «прогресса», когда скорость «инноваций» достигает такого предела, за которым не успевают ни специалисты, ни технологии, ни консервативно выстроенные процессы. Всё более сложная экосистема сервисов, инструментов, утилит, фреймворков, стеков технологий порождает всё большее количество сбоев, инцидентов, ошибок, необходимости интеграций, настроек и... дефицит кадров, способных разбираться в этом хаосе.

В итоге дисциплина безопасности приложений и разработки превращается в разновидность «алхимии». Когда дефицитные «жрецы безопасного кода» ценятся так сильно, что джуниор с полугодовым опытом работы вполне может претендовать на вакансию 150 тысяч рублей на руки, иметь удалёнку из региона и считаться «выгодной корпоративной инвестицией». А грамотные инженеры со стажем 5+ лет годятся в «прожжённые ветераны» и ценятся как «крыло от самолёта».

И это не досужие домыслы, а суровые факты действительности, подтверждаемые статистикой. Например, созданный в 2010 году Consortium for Information & Software Quality (CISQ) оценивает ущерб от некачественного кода и недостатков процессов разработки в 2022 году в 2,41 триллиона долларов, а дефицит ИТ-кадров в 300 тысяч человек, и это только в США. Подробнее о результатах исследования можно почитать на сайте организации³. Но очевидно, что если в развитых с точки зрения ИТ-разработки США существуют такие проблемы, то аналогичная ситуация (или хуже) характерна для всего мира, особенно для развивающихся регионов вроде Африки⁴.

Казалось бы, отличные новости для профильных специалистов, у

которых впереди много работы! Но тут на сцену выходит ИИ, который может оказаться фактором существенных и достаточно быстрых изменений в индустрии (буквально на горизонте 3–5 лет). Что-то похожее происходило с классическими веб-дизайнерами, очень востребованными в конце нулевых, но существенно утратившими позиции после появления различных веб-конструкторов а-ля Figma. Аналогичный процесс наблюдался на примере консервативных сисадминов, оттесняемых на периферию облачными технологиями и виртуализацией. Конечно, это не означает, что веб-дизайнеры или сисадмины «вымерли». Среди них существуют и будут существовать отдельные супервостребованные гуру, у которых всё хорошо. Но важно понимать, что эти супергуру — разновидность «органических фермерских продуктов» — уникальных, нишевых товаров, которые не закрывают массовые потребности и существуют в своих трудно повторяемых нишах. Конечно, остаются и середняки. Но меняется степень их востребованности и падают заработные платы.

И если мы спроецируем тренды ИИ на отрасль безопасной разработки, то точно должны задуматься: а что будет дальше? Каким инструментарием необходимо овладеть, чтобы оставаться востребованными и соответствовать актуальному уровню компетенций?

НЕКОТОРЫЕ ПРИМЕРЫ И ВОЗМОЖНЫЙ ПЛАН ДЕЙСТВИЙ

Уже сейчас нейронные сети с различными специализациями, интегрированные в единое целое с помощью специальных оболочек, позволяющих использовать предустановленные промпты⁵, кажется, являются следующей вехой развития индустрии.

¹ <https://www.anthropic.com/product>

² <https://github.com/frogger/Awesome-GPT-Agents>

³ <https://www.it-cisq.org/the-cost-of-poor-quality-software-in-the-us-a-2022-report/>;

⁴ <https://www.youtube.com/watch?v=XWSrD-seKMaI>.

⁵ <https://www.techtartget.com/searchenterprise-ai/definition/AI-prompt>

Они не только помогают автоматизировать типовые задачи и встраиваются крупными корпорациями в свои сервисы и инструменты «из коробки». Но и снимают существенную часть аналитической нагрузки и рутины с опытных специалистов. Заменяя как отдельные роли и направления работы, так и толковых джунов, быстрее и точнее собирая необходимую информацию и чётко выполняя поставленные задачи.

Здесь очень характерно поведение Microsoft, которая после покупки GitHub начала интегрировать с ним всё больше интересных инструментов, связанных с безопасностью разработки. Например, уже в декабре на базе GitHub должен открыться (если ещё не открылся) чат со знаменитым Copilot⁶, который позволит в числе прочего следить за безопасностью создаваемого кода в режиме онлайн. А на недавней презентации CEO Microsoft продемонстрировал возможные интеграции этого инструмента с различными приложениями и внешними источниками данных, в рамках Office 365. Показал на примерах, как это позволит автоматизировать самые разные задачи, в том числе связанные с обработкой информации об инцидентах и уязвимостях кибербезопасности.

И это один продукт одной корпорации, не специализированной на информационной безопасности! Понятное дело, что любое новое решение может содержать какие-то недостатки, что адаптация к новым возможностям займёт какое-то время. Но кажется, для всех, кто хочет оставаться на плаву, наступает время готовиться к адаптации прямо сейчас. А для тех, кто любит неопределённость и риски, открываются возможности по развитию собственных стартапов в новых нишах. Например, почти наверняка потребуются консультанты по обучению команд AppSec и DevSecOps использованию и внедрению нового инструментария, возникнет потребность в защите API агентов GPT, встанут вопросы дообучения и тюнинга

⁶ <https://github.blog/2023-11-08-universe-2023-copilot-transforms-github-into-the-ai-powered-developer-platform/>

Адаптация к новым возможностям займёт какое-то время. Но кажется, для всех, кто хочет оставаться на плаву, наступает время готовиться к адаптации прямо сейчас

моделей, появятся истории про доверие и конфиденциальность вводимых данных, станет накапливаться ещё больше чисто юридических кейсов относительно прав собственности на «выделяемый AI продукт», потребуются стандарты и фреймворки безопасности ИИ и т.д. и т.п.

То есть, по существу, у нас на глазах возникает очередной фронт, и те, кто «поверит в него», получат шанс заскочить туда, если не в статусе крупнейших корпораций, создающих собственные модели и базовые инструменты, то по крайней мере в рамках разработчиков вспомогательных сервисов и нишевых инструментов или пользователей и инженеров, способных грамотно использовать новые возможности, повышающие продуктивность и результативность труда.

ЗАКЛЮЧЕНИЕ

Достаточно ли приведённых выше аргументов, чтобы запланировать изучение и внедрение новых инструментов или хотя бы сходить на курсы повышения квалификации? Ещё пару лет назад сам автор был скептичен к подобным инновациям, вспоминая

то популярность блокчейн-технологий и децентрализации вычислений, то радостный ажиотаж скорой колонизации Луны и Марса из более далёких времён. Но последние факты и то, что уже сейчас можно делать с помощью всё ещё несовершенного инструментария, убедили его в обратном.

Убедит ли это вас? Насколько у нас достаточно свидетельств для того, чтобы делать глобальные выводы? Автор не знает, но советует прочесть «ИИ-2041. Десять образов нашего будущего» Кай-Фу Ли и Чэнь Цюфань — достаточно взвешенную и многомерную аналитику профильного специалиста, переплетённую со сборником фантастических рассказов. И хотя футурология и прогнозы — дело неблагодарное, во многом потому, что технологии не существуют в вакууме и многое зависит от сил, занимающихся их внедрением, от заинтересованности субъектов, которые используют эти технологии, кажется, что ИИ не будет технологией-пустышкой и в ближайшую декаду мы увидим существенную трансформацию профессии, к которой можно и нужно готовиться прямо сейчас...

Подробнее о состоянии безопасности в развивающихся странах можно посмотреть в замечательном выступлении Евгения Соболева:



А всех желающих продолжить диалог автор приглашает в гости на свой канал в «Телеграме» (t.me/sec_devops):



РОССИЯ — БЕЛАРУСЬ: ЦИФРОВАЯ СУДЬБА

24 января делегация Министерства связи и информатизации Республики Беларусь посетила с визитом Минцифры РФ.

На этой встрече топ-менеджеры РУП «Центр цифрового развития» (Беларусь) и ПАО «Ростелеком» (РФ) подписали меморандум о взаимодействии и сотрудничестве в сфере цифровой трансформации государственного управления обеих стран.

Основные векторы такого сотрудничества — внедрение и развитие платформенных решений и систем управления государственными данными, реализация общих целей по созданию единого цифрового пространства и обеспечению цифровой независимости, создание и развитие интегрированных информсистем и цифровых сервисов Союзного государства.



В КОСМОС!

Компания «Бюро 1440», входящая в «Икс холдинг», планирует запустить коммерческий спутниковый широкополосный интернет в 2027 году.

На первом этапе для базового покрытия будут запущены 250 спутников. С ростом абонентов их число вырастет примерно до 700. Потенциальная аудитория спутникового интернета в РФ составляет 1,5–2 млн человек.

Однако, есть и мнение, что у компании могут возникнуть трудности — запуски ракет расписаны на несколько лет вперед. Известно, что Starlink Илона Маска столкнулся с той же проблемой.

Летом «Бюро 1440» запустило на орбиту три спутника «Рассвет-1» и протестировала связь, достигнув скорости 12 Мбит/с с задержкой 41 мс.

ПРЕЗИДЕНТ ДАЛ ПОРУЧЕНИЯ В СФЕРЕ ИИ

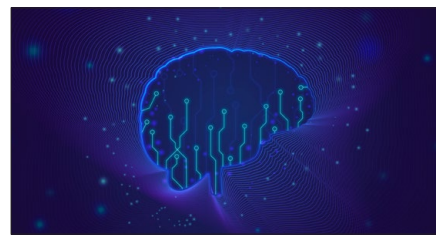
Владимир Путин утвердил перечень поручений по итогам конференции «Путешествие в мир искусственного интеллекта». Предложено рассмотреть дополнительное финансирование в области генеративного ИИ, а также создание инфраструктуры и поддержку развития больших генеративных моделей.

Также поручено провести анализ потребностей работодателей в ИИ-специалистах и внести изменения в профстандарты и образовательные программы в целях подготовки новых кадров.

Правительству РФ поручено обеспечить привилегированный доступ российских профильных исследователей и студентов к вычислительной инфраструктуре суперкомпьютеров. Будет проведена и разработка Кодекса этики в сфере ИИ.

Совместно с Госдумой Правительство РФ будет работать над изменениями в законодательство, чтобы упростить доступ к экспериментальным правовым режимам в цифровых инновациях и принять меры по ответственности за возможный вред, причиненный использованием ИИ.

В рамках усиления международного сотрудничества будет рассмотрена возможность взаимодействия российских и зарубежных разработчиков ПО в области ИИ, а также порядок доступа разработчиков из других стран к российским генеративным моделям.



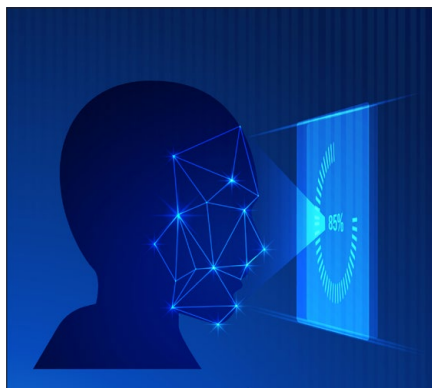
ДИПФЕЙКИ — УГРОЗА ДЛЯ ВСЕХ!

По результатам стратегической сессии, посвященной национальному проекту «Экономика данных», Михаил Мишустин, глава правительства РФ, поручил Минцифры разработать методы для обнаружения недостоверных данных, созданных с помощью ИИ. Это решение было принято в рамках Национальной стратегии развития ИИ до 2030 года и проекта «Искусственный интеллект» на период 2025–2030 годы.

Дипфейки, то есть поддельные данные, созданные с использованием ИИ, представляют серьезные риски, особенно для КИИ и органов власти. В США и Великобритании уже существуют регуляции в области ИИ, и Россия следует этому глобальному тренду.

Скорость создания и распространения дипфейков превосходит возможности СМИ. Это представляет угрозу для государства, общества и граждан. Технологии ИИ — машинное обучение, компьютерное зрение, обработка языка и т.д. — могут привести к сбору огромного объема ПД, распространению ложной информации и ошибочным действиям. В критически важных отраслях это может иметь непоправимые последствия.

Распространение дипфейков становится все более упрощенным и доступным благодаря совершенствованию алгоритмов и технологий. Чтобы с ними бороться, необходимы новые подходы и решения.



ГЕРОЙ НАШЕГО ВРЕМЕНИ

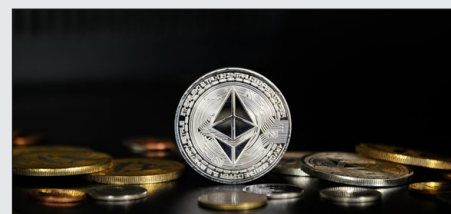
В США суд приговорил инженера облачных сервисов Миклоса Броуди к двум годам тюремного заключения и выплате компенсации 529 тыс. долл. за уничтожение репозитория кода своего бывшего работодателя — коммерческого банка First Republic Bank. Также после освобождения фигурант будет три года находиться под надзором.

По информации Минюста США, Броуди был уволен весной 2020 года из отделения FRB в Сан-Франциско за то, что нарушил политику компании, подключив USB-накопитель с порнографией к компьютерам банка. Уточняется, что после увольнения он отказался сдать рабочий ноутбук, а после использовал свою корпоративную учётную запись для доступа к компьютерной сети банка и причинения ущерба в 220 тыс. долл.

До того, как инженера отключили от системы, он успел не только удалить репозитории кодов, но так-

же запустить вредоносный скрипт для уничтожения серверов и удаления журналов банка, оставить в коде оскорбительные комментарии в адрес бывших коллег, а также выдать себя за других сотрудников, чтобы войти в сеть организации от их имени и внести изменения в конфигурацию.

Сначала Броуди утверждал, что корпоративный ноутбук у него украли из машины, но в итоге признал вину. First Republic Bank же закрылся и был продан JPMorgan Chase.



НАШЕЛ РАБОТУ...

Неназванный хакер вернул криптобирже HTX ранее похищенные им 5 тыс. ETH (примерно 8,1 млн долл.), за что получил вознаграждение в размере 250 ETH (примерно 405 тыс. долларов) и предложение о работе.

Советник площадки Джастин Сан рассказал, что взломщик украл коины 25 сентября. Тогда биржа покрыла убытки пострадавших держателей криптовалюты и предложила хакеру вернуть «монеты» за выплату в размере 5 % от объёма похищенного и должность советника по безопасности.

На выполнение требования дали неделю — в случае отказа компания передала бы все данные в полицию, но хакер согласился.



АССОЦИАЦИЯ
БАНКОВ
РОССИИ

Ежегодная встреча кредитных организаций с руководством Банка России

Целью ежегодно проводимых встреч является обсуждение в прямом диалоге с Банком России актуальных вопросов надзора и регулирования деятельности кредитных организаций, новых законодательных и нормативных документов, а также ключевых вызовов, стоящих перед банковским сообществом.

Во встрече традиционно принимают участие Председатель Банка России, заместители Председателя, руководители департаментов и служб Банка России, представители федеральных министерств и ведомств, Госдумы, Совета Федерации, институтов развития.

29 февраля—1 марта 2024 года

Московская область, кампус СберУниверситета

Контакты: +7 (495) 785-29-93, +7 (495) 785-29-88
event@asros.ru, <https://asros.ru>

Подробная
информация

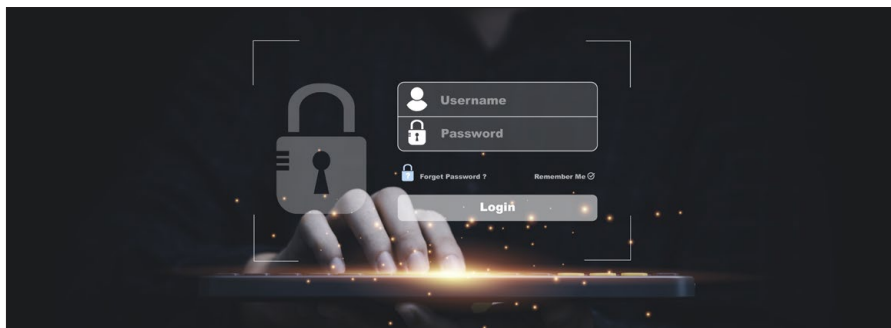


«ПРОШЕЛСЯ» ПО АККАУНТАМ

Джозеф Гаррисон, 19-летний подросток из США, признал вину в организации масштабной атаки на букмекерский сервис DraftKings. Ранее он методом Credential Stuffing взломал 60 тыс. аккаунтов пользователей этого ресурса.

Гаррисон с сообщниками привязывали в личном кабинете новый платёжный метод, вносили на счёт пять долларов для верификации, а затем выводили с него все имеющиеся средства. Так им удалось похитить около 600 тыс. долларов с более чем полутора тысяч аккаунтов.

При инспекции компьютера обвиняемого полиция обнаружила около 40 млн строк учётных данных, которые могли использоваться в атаках методом подбора. А в телефоне Гаррисона нашлась переписка между ним и остальными фигурантами, где они обсуждали способы взлома букмекерского сайта и возможную монетизацию данной схемы.



МОШЕННИК БРАЛ МИКРОКРЕДИТЫ

Полиция задержала петербуржца, создававшего фишинговые сайты для сбора персональных данных граждан. Они копировали официальные страницы различных госорганов.

При попытках воспользоваться сервисами жертвы привычно вводили данные своих аккаунтов, зарегистрированных на Едином портале государственных и муниципальных услуг, предоставляя таким образом преступнику доступ к размещённым в учётных записях сведениям.

Мошенник в свою очередь менял пароли и подавал через угнанные аккаунты заявки в микрокредитные организации, а после выводил средства через анонимные электронные кошельки. Когда лимит на получение кредита исчерпывался, учётная запись удалялась вместе со всей информацией об её использовании.

Правоохранителями возбуждено уголовное дело по ст. 272 УК РФ («Неправомерный доступ к компьютерной информации»). По данным следствия, жертвами киберпреступника стали более 130 граждан.

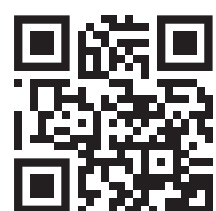


17-й Межотраслевой форум директоров
по информационной безопасности

CISO-FORUM 2024



17 ЛЕТ МЫ СОБИРАЕМ ЛУЧШИХ CISO,
РУКОВОДИТЕЛЕЙ ИБ И ЭКСПЕРТОВ В ОБЛАСТИ
КИБЕРБЕЗОПАСНОСТИ ИЗ КЛЮЧЕВЫХ ОТРАСЛЕЙ
ЭКОНОМИКИ



12
апреля

Loft Hall
Москва

10 ЛЕТ! ЗА ЧТО?

Законопроектом, подготовленным с участием Банка России, предлагается на десять лет отстранять от работы топ-менеджеров финучреждений за неоднократную утечку данных.

Документ предусматривает, в частности, повышение персональной ответственности замглавы банка по ИБ за нарушения требований по защите информации, приведших к утечке ПД или банковской тайны. Инициатива касается также стра-



ховых компаний, пенсионных фондов и МФО.

Практически это требование вводит десятилетний запрет на занятие должности за сам факт наступления определенных событий, говорится в отзыве на законопроект Национального совета финансового рынка (НСФР). По мнению главы НСФР А. Емелина, в нынешней версии законопроекта не прописана связь непосредственной деятельности человека и его дисквалификации. Например, если базу данных слил подчиненный-инсайдер, то его руководителя автоматически дисквалифицируют на десять лет, даже если он не причастен к происшествию.

В НСФР полагают, что такой запрет несопоставим даже с наказаниями за более серьезные нарушения, несоразмерен, несправедлив и объективно избыточен. Эта мера может усугубить и без того сложную ситуацию с нехваткой профильных специалистов.

ДОРАБОТАЮТ ИЛИ НЕТ?

АРПП «Отечественный софт» и АПКИТ во второй раз предложили депутатам доработать законопроект «О внесении изменений в отдельные законодательные акты РФ» в части правовых основ для аутсорсинга ИТ и использования облачных услуг.

Текст принятого в первом чтении документа предусматривает включение в профильное финансовое законодательство понятий «услуги аутсорсинга информационных технологий» и «облачные услуги». И под «аутсорсингом» здесь можно понять практически любую ИТ-деятельность в случае, если её потребителем является финучреждение.

В связи с этим авторы послания попросили законодателей уточнить предмет регулирования законопроекта. Отраслевые эксперты в свою очередь рекомендуют при доработке законопроекта использовать подход, нацеленный на регулирование правил автоматизированной обработки и (или) хранения

информации, обладателем которой является субъект финансового рынка, при привлечении им сторонней организации.

Специалисты уверены, что эти предложения соответствуют целям законопроекта: регулировать не деятельность в области ИТ в отдельном секторе, а порядок обращения финорганизаций со сведениями, составляющими банковскую и иные виды тайн.



ЕС ВЗЯЛСЯ ЗА КРИПТОСЕКТОР

Совет ЕС и Европарламент достигли соглашения по ужесточению правил борьбы с отмыванием денег, которые обяжут операторов криптовалют проверять и информировать власти о сделках своих клиентов.

В заявлении Совета ЕС подчеркивается, что «финансовые учреждения, банки, агентства недвижимости, службы управления активами, казино, торговые предприятия играют центральную роль в качестве посредников в системе борьбы с отмыванием денег и противодействия финансированию терроризма, поскольку они имеют привилегированное положение для обнаружения подозрительной деятельности».

В соответствии с соглашением все поставщики услуг криптоактивов (CASP) должны будут проводить комплексную проверку своих клиентов при осуществлении транзакций на сумму от одной тысячи евро.

ПРО БАНКОВСКУЮ ТАЙНУ

Совет директоров Банка России утвердил перечень информации, которую банки будут вправе не раскрывать в 2024 году.

Например, финансовые организации могут не публиковать информацию о лицах, под контролем (либо значительным влиянием) которых они находятся, о членах органов управления и иных должностных лицах, о фактах, затрагивающих деятельность учреждения, реорганизуемого в форме слияния, присоединения и преобразования и т.д.

Некоторые данные в 2024-м не будет раскрывать и сам Центральный банк. Конфиденциальной останется информация о лицах, контролируемых кредитными и страховыми организациями, а также негосударственные пенсионные фонды. Сведения о структуре и составе акционеров и членах советов директоров также будет закрыта.



Александр ШОЙТОВ
заместитель министра
цифрового развития, связи
и массовых коммуникаций
Российской Федерации

«СЕГОДНЯ ПРОРЫВ ТРЕБУЕТСЯ ВСЕЙ НАЦИОНАЛЬНОЙ ЭКОНОМИКЕ ДАННЫХ»

Цифровизация в нашей стране наступает широким фронтом, охватывает все сферы экономики, государства, общества. При этом традиционное противостояние щита и меча приобретает новые фор-

мы. О том, какие задачи сегодня стоят перед отраслью информационной безопасности в контексте намеченного государством перехода к национальной «Экономике данных», BIS Journal беседует с Александром Шойтовым.

– Александр Михайлович, параллельно с нарастанием процессов цифровизации новое содержание приобретают вопросы информационной безопасности. Не случайно в этой сфере действует четыре регулятора: Минцифры, ФСБ, ФСТЭК, Банк России. Как распределяются роли в этом квартете?

– На самом деле базовых регуляторов, которые определяют требования информационной безопасности (ИБ), два: ФСБ РФ и ФСТЭК России. Каждый из них отвечает за требования ИБ в своей части: ФСТЭК – с точки зрения систем защиты государственной информации, ФСБ занимается вопросами криптографии и мониторинга реагирования на компьютерные атаки. Банк России – это регулятор сферы ИБ в части, касающейся кредитно-финансовой сферы. А Минцифры является, с одной стороны, регулятором в сфере обеспечения безопасности персональных данных, а с другой стороны, мы более плотно работаем с отраслью, чем коллеги, которые занимаются определением самих требований информационной безопасности и следят за их выполнением.

Под более плотным взаимодействием с отраслью ИБ понимается, в частности, организация перспективных направлений исследований, а также запуск государственных программ для массового сектора цифровой экономики в части государственных информационных систем (ГИС), систем обработки персональных данных. Мы это делаем в рамках действующих госпрограмм, в первую очередь это программа «Цифровая экономика», а также перспективных программ, например «Национальная экономика данных», которая должна стартовать в 2025 г. Здесь мы являемся главным распорядителем бюджетных средств. Но конечно, эту систему мы выстраиваем во взаимодействии с коллегами по цеху. У нас со всеми выстроена правильная полноценная кооперация, мы хорошо дополняем друг друга.

ИБ И ТЕХНОЛОГИЧЕСКИЙ СУВЕРЕНИТЕТ

– На уровне государства сегодня поставлена цель – обеспечение технологического суверенитета российской экономики. Эта цель предъявляет какие-либо новые требования к реализации систем информационной безопасности на российских предприятиях?

– В целом нужно рассматривать два больших сегмента: сами информационные

системы и профильные средства защиты информации, которые обеспечивают информационную безопасность информационных систем компаний с учётом требований технологической независимости. Для самих технических средств, предназначенных для того, чтобы гарантировать и обеспечивать информационную безопасность, есть системы сертификации ФСТЭК и ФСБ. Соответственно, степень их доверенности и качество реализации проверяется с помощью этих систем сертификации. Но состояние информационной безопасности на предприятии существенно зависит от самих средств и систем ИТ – программного обеспечения, программно-аппаратных комплексов, телекоммуникационного оборудования и т.д., от того, насколько правильно они построены с учётом доверия, являются ли они доверенными российскими системами.

В этой части в первую очередь для наиболее значимых объектов, для критической информационной инфраструктуры сейчас идут процессы определения критериев доверия, с учётом импортозамещения и технологической независимости. Насколько российскими являются реализованные ИТ-решения, насколько они качественные и надёжные.

Конечно, технологии информационной безопасности должны пронизывать всю многоуровневую цифровую структуру предприятий, например, для промышленности: от уровня технологических установок и агрегатов и до самого верхнего уровня управления самим предприятием. Поэтому правильный путь – такой, когда все эти вопросы решаются изначально при построении самих систем.

– Secure by design?

– Да, в широком смысле этих слов. Конечно, чем мы глубже погружены внутрь происходящих процессов, тем лучше сможем их защитить, и в конечном счёте это будет дешевле по сравнению с другими способами, например наложенными средствами ИБ. Но эти возможности очень сильно связаны с тем, каким образом мы владеем самой информационной технологией, которую мы защищаем. Если она российская или она плод международной разработки, но мы её полностью понимаем и можем вносить нужные коррективы на уровне ядра информационной системы, то, конечно, нам существенно проще обеспечить её информационную безопасность. К этому мы стремимся. Но надо понимать, что в разных аспектах цифровых систем у нас разный уровень зрелости и знания

Если искусственный интеллект работает в КИИ, то меры обеспечения безопасности тоже должны быть очень серьёзными

самой технологии. Эти параметры зависят и от того, каким образом наша страна владеет конкретной технологией, и от степени её зрелости на мировом уровне.

— Можете привести примеры?

— Один пример — облачные технологии, которые помогают создавать облака. Сегодня одно из перспективных направлений развития российских информационных систем — это их размещение в больших правильно защищённых облаках. Соответствующие отечественные технологии хорошо развиты. В том числе мы их сильно подтянули на уровень лучших международных решений, когда создавали систему «Гостех». Тут точно можно сказать, что мы глубоко погружены в эти технологии, и необходимые меры и средства обеспечения ИБ реализованы внутри этих технологий.

Другой пример — Интернет вещей. Там есть общее понимание проблематики в целом и понятны отдельные направления, по которым уже идёт ряд работ.

И третий пример — это искусственный интеллект. Здесь наиболее сложная ситуация. Сама технология ещё недостаточно изучена, с точки зрения информационной безопасности и надёжности. Причём такая ситуация наблюдается во всём мире. Отдельные направления у нас прорабатываются на очень хорошем уровне, но тему искусственного интеллекта надо развивать активно и глубоко.

ИБ И ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ

— А какая активность наблюдается у нас в вопросах безопасности интеллектуальных систем?

— С точки зрения рисков ИБ, надо разделять два вопроса, хотя они и связаны между собой: защита интеллектуальной системы от внешней атаки, обеспечение её надёжной работы и использование ИИ в системах информационной безопасности. По второму направлению — умное противодействие

компьютерным атакам и прочее — у нас разработок достаточно много, в целом мы здесь идём примерно на мировом уровне. Но нужно прилагать усилия для максимально быстрого развития и энергичного дальнейшего движения вперёд.

А вот по первому направлению перед нами стоят такие же сложные задачи, как и перед всеми технологически развитыми странами мира. Что у нас делается в этом направлении?

В мае 2023 г. года при поддержке Минцифры прошёл форум «Цифровая экономика: технологии доверенного искусственного интеллекта», организованный АНО «Национальный технологический центр цифровой криптографии» (НТЦ ЦК), Академией криптографии РФ, Институтом системного программирования им. В. П. Иванникова РАН. На этот форум мы собрали наиболее активных участников процессов в области доверенного и безопасного искусственного интеллекта, включая разработчиков ИИ-систем, например, из ВТБ, Сбера.

Институт системного программирования РАН, а это, напомню, опорный центр доверенного искусственного интеллекта, в рамках нацпроекта «Искусственный интеллект» сейчас занимается исследованиями популярных нейросетевых моделей, которые чаще всего применяют наши компании в своих проектах. На старте проекта в списке было порядка 60–70 моделей, но благодаря импортозамещению этот список корректируется. Но в топе самых популярных моделей остаются такие зарубежные разработки, как TensorFlow и PyTorch. Где-то они используются как полностью свободное ПО, где-то как частично открытое ПО open source. В каждом случае надо понимать, насколько можно верить этим моделям. Исследователи проводят глубокий анализ ядра модели и выдают вариант, подходящий для дальнейшего использования в реальных проектах.

В Академии криптографии, которую я по совместительству возглавляю, также идут научно-исследовательские работы по информационной безопасности самого искусственного интеллекта в рамках нацпроекта «Цифровая экономика». В 2024 г. мы должны выдать проект требований по информационной безопасности к продуктам искусственного интеллекта в целом.

— Автономным интеллектом специалисты тоже занимаются?

— Конечно. В целом сложность изучения проблем безопасности ИИ существенно

зависит от уровня критичности применения искусственного интеллекта. Так, есть большой пласт задач, в которых искусственный интеллект выступает в роли помощника человека, даёт подсказки решения на основе некоторой аналитики, но окончательное решение принимает сам человек. Здесь уровень критичности не так высок, как, скажем, для ВАС с пятым уровнем автономности.

Одно дело, когда внутри автомобиля сидит оператор, который может вмешаться в управление транспортным средством. Или этот оператор может находиться в некотором удалённом центре управления, откуда может управлять целой группой автомобилей, но всё равно у него остаётся возможность перехватить управление. А вот когда человек устраняется из этого процесса и полностью передаёт управление искусственному интеллекту, это уже критическое применение. Здесь, конечно, нужно обеспечить повышенные меры надёжности и безопасности.

Другое направление — медицина. Подсказки врачу тоже должны соответствовать некоторым протоколам, потому что нельзя допустить, чтобы доктор принимал рекомендацию ИТ-системы за непосредственное указание к действию. Он должен обязательно сделать несколько шагов, чтобы оценить предложения ИТ-системы и принять самостоятельное решение.

Если искусственный интеллект работает в критической информационной инфраструктуре, то меры обеспечения безопасности тоже должны быть очень серьёзными.

И в области обработки данных есть отдельное направление, которым мы тоже занимаемся, — обезличивание персональных данных. Это ещё одна сфера ИТ, до конца не отрегулированная нигде во всём мире. Есть отдельные практические рекомендации, которые приняты в США и других странах. Но таких методов, которые могли бы гарантировать надёжное и эффективное обезличивание персональных данных: образно говоря, поставщик данных где-то их выложил и кто угодно может ими пользоваться совершенно безопасно для граждан, — на настоящий момент не существует нигде в мире. И регулирования такого уровня тоже нигде в мире нет. Есть конкретные практические подходы, но решения задачи в общем случае нет.

Мы тоже в этом направлении работаем. Эффективное решение задачи обезличивания персональных данных — одно из важнейших направлений госпрограммы «Национальная экономика данных», рассчитанной на 2025–

2030 гг., которая придёт на смену «Цифровой экономике». И в 2024 г. все соответствующие мероприятия будут сформированы и заложены в новый нацпроект. С этой целью мы рассчитываем на полноценное взаимодействие с разработчиками. На всех форумах, где мы выступаем, во всех документах, которые мы готовим, призываем: каждый разработчик перспективных ИТ-решений, особенно если это крупная компания, должен прямо сейчас начать заниматься вопросами безопасности ИИ.

О ЗАКОНОДАТЕЛЬСТВЕ В СФЕРЕ ПД

— Достаточно давно в кулуарах Госдумы ходит проект федерального закона по обезличиванию персональных данных. В настоящее время он на какой стадии?

— Рассмотрение этого законопроекта во втором чтении планируется на начало 2024 г. Надеюсь, что в ближайшее время данный законопроект удастся принять. И сразу будет возможно получить серьёзное продвижение в вопросе обезличивания данных.

Дело в том, что технологически мы практически готовы к началу действия закона в том виде, в котором это описывается в законопроекте. Речь идёт о том, что обезличивание или обучение системы искусственного интеллекта на обезличенных данных будет проводиться некоторой государственной информационной системой, замкнутой в специальной «песочнице». И вот там можно будет продемонстрировать всем — и бизнесу, и регуляторам в области ИБ — все существующие на данный момент методы, показать, что они позволяют гарантированно проводить обезличивание и что это совсем не сложно для использования в бизнес-системах. Далее пойдёт практика апробации методов и решений, параллельно будут совершенствоваться технологии, но это уже вопрос перспективного развития.

Эффективное решение задачи обезличивания персональных данных — одно из важнейших направлений госпрограммы «Национальная экономика данных»

На практическом уровне уже создан макет центра обезличивания, который позволяет проводить эксперименты и исследования. Но в окончательном виде он должен быть погружён в некоторую конкретную государственную информационную систему, с ней должен быть обеспечен правильный интерфейс, и вокруг действующего макета должна быть выстроена вся система защиты «песочницы». В нынешнем варианте он демонстрирует эффективность отдельных методов или методик обезличивания, их эффективность в части защиты данных, а также то, что эти данные будут надёжно сохраняться для последующего применения той или иной системой искусственного интеллекта. Фактически это хорошо проработанная заготовка. Принятие федерального закона и дальнейшее построение полной системы на основании принятого закона позволит запустить процесс загрузки данных и наблюдения за тем, чтобы все внутренние механизмы правильно заработали.

О СОРЕВНОВАНИИ С МИРОВЫМИ ЛИДЕРАМИ

— **Вы постоянно говорите о новых разработках, которые нельзя скопировать у мировых лидеров, потому что они сами ещё проходят исследовательский путь проб и ошибок. Значит, термин «импортозамещение» тесноват для задач, стоящих перед отраслью ИБ?**

— Этот этап, когда нужно было «взять западный образец и быстро повторить», мы в основном прошли. Выстояли. Все информационные системы в стране работают, все отрасли продолжают функционировать, более того, наращивают обороты.

То, что западные вендоры ИБ ушли с нашего рынка, — это только одна сторона вопроса. Другая сторона — позиция наших регуляторов, которые чётко указали: к 2025 году необходимо уйти с западных продуктов, по крайней мере в КИИ. Поэтому сфера отечественных разработок начала существенно расширяться. Здесь важно не только то, что российские вендоры неплохо закрывают различные ниши ИБ и только в некоторых узких классах решений типа интеллектуальных высоконагруженных межсетевых экранов следующего поколения (NGFW) остаётся некоторое отставание. Главное — мы нацелены «догнать и перегнать», причём в точке, которая расположена дальше на «стреле» технологического развития.

Образно говоря, наша задача — не догнать западных лидеров в той точке, где они находятся сегодня, а, пройдя своим путём развития, перегнать их в той точке, которую они только планируют достичь. Да, в какой-то момент с кем-то из них мы сравняемся в развитии, но не это наша главная задача, наша задача — быстрее идти вперёд. Именно такая задача стоит перед отраслью ИБ, да и ИТ в целом. Но конечно, если иметь в виду весь ландшафт отечественной техники ИТ, то в разных сегментах эта задача выглядит очень по-разному.

О РОССИЙСКОЙ КРИПТОГРАФИИ

— **Расскажите, пожалуйста, как сегодня развивается суверенная российская отрасль передовых продуктов криптографической защиты данных?**

— Базовая криптография, по сути, обеспечивает всю информационную безопасность начиная с 50-х годов прошлого века в виде защиты канала передачи информации с помощью двух шифраторов. И в этой части у нас были кардинальные достижения, которые признавал весь мир. Американцы прямо говорили, что успехи советской криптографии соизмеримы с успехами Советского Союза в космосе. Это были те две сферы деятельности учёных и конструкторов, где мы были глобальными лидерами. И это преимущество удалось сохранить, невзирая даже на распад Советского Союза в 90-е годы. Как раз тогда, в 1992 г., была создана Академия криптографии, которую я возглавляю с 2017 г. В частности, её усилиями удалось сохранить научную составляющую отечественной криптографии, и во всём мире по-прежнему есть два основных «идеолога» в данной сфере со своими стандартами и алгоритмами — США и Россия. И мы здесь нигде не отстаём. Конечно, это всегда был и остаётся динамичный паритет — то один, то другой участник соревнования криптографов чуть вырывается вперёд в конкретных аспектах, а второй быстро навёрстывает разрыв.

ОБ УГРОЗАХ КВАНТОВОГО КОМПЬЮТЕРА

— **А к приходу CRQC (Cryptographically Relevant Quantum Computer), криптографически релевантного квантового компьютера, наши предприятия успеют подготовиться?**

— Что касается квантовой угрозы, то она есть и действительно угрожает всему миру. Однако замечу, что не для всех алгоритмов

она одинаково опасна. Скажем, для алгоритмов симметричного шифрования квантовые компьютеры даже менее опасны, чем обычные. А вот для алгоритмов асимметричного шифрования — да, угроза реальная. Но это всё же дело более-менее отдалённой перспективы. Чтобы вскрывать системы шифрования RSA с длиной ключа шифрования 2048 бит, нужен квантовый компьютер на 3000–5000 кубитов. То есть эта опасность не сегодняшнего дня, но, конечно, работать в этом направлении надо.

Работа сложная. Так, в США соответствующий конкурс NIST в области постквантовой криптографии начался в 2016 г. и проходит с большими трудностями. Правительство США планировало в конце 2023 г. завершить фазу первичного накопления и анализа различных методов, подходов, алгоритмов, практических решений постквантовой криптографии и в 2024 г. приступить к формированию стандартов криптографии силами NIST.

Мы планируем совместно с НТЦ ЦК в 2024 г. провести свой конкурс. В целом для противодействия угрозам квантового компьютера мы действуем по трём направлениям: применение алгоритмов постквантового шифрования, переход с асимметричного шифрования на симметричную криптографию там, где это оправдано, и использование шифрования с квантовым распределением ключей на аппаратном уровне.

Следует отметить, что в нашей стране системы, в которых обрабатывается государственная тайна, не используют алгоритмы с открытым ключом. Поэтому квантовые угрозы наиболее существенны для областей, где массово применяются алгоритмы шифрования с открытым ключом, например, банковской сферы. Там в перспективе надо эту проблему решать. Подходящие научные и технологические подходы есть, наша наука в этом плане хорошо работает. Возможно, мы радикально не обгоняем наших заокеанских коллег, но точно и не отстаём.

Например, наши стандартизованные симметричные алгоритмы шифрования ГОСТ построены на основе математики эллиптических кривых, а американский стандарт симметричного блочного шифрования AES основан на разложении чисел на простые сомножители. Иными словами, наш математический подход появился чуть позже, но он лучше работает. Мы сравнивали стандартизованные алгоритмы и видим, что в некоторых технических аспектах наши существенно выигрывают у главных конкурентов.



Александр Шойтов на форуме «Цифровая экономика: технологии доверенного искусственного интеллекта»

О НЕОБХОДИМОСТИ ТЕХНОЛОГИЧЕСКОГО ПРОРЫВА

— Если у нашего государства есть «госзаказ» на создание новых нетривиальных решений, которые идут впереди в глобальном масштабе, то от наших разработчиков и от компаний-заказчиков тоже требуется некий технологический прорыв в области ИБ?

— Здесь есть два соображения. Во-первых, в целом отрасль хорошо развита. А во-вторых, сегодня прорыв требуется всей национальной экономике данных. Вообще, четвёртый технологический уклад подразумевает: тот, кто победит в технологиях, тот сможет диктовать свои условия миру. И нам нужно для каждого вида ИТ сделать отличное высокоэффективное решение лучшего мирового уровня.

ОБ ОРГАНИЗАЦИИ ПРОРЫВОВ

— Для этого нужна какая-то методология планирования, организации работ?

— Очевидно, что в данном случае нужна хорошая кооперация, в первую очередь науки с государством и бизнесом. Именно в русле этой идеи год назад была создана некоммерческая организация АНО «Национальный технологический центр цифровой криптографии».

АНО «Национальный технологический центр цифровой криптографии» станет серьёзной платформой для координации работы в области криптографии и смежных вопросов

В настоящее время она полноценно функционирует, у неё есть научно-технический совет, правда, пока небольшой. Сейчас её научно-исследовательские мощности наращиваются, и к концу 2024 г. планируется завершить создание инфраструктуры: появятся новые лаборатории, и НТЦ ЦК станет серьёзной платформой для координации работы в области криптографии и смежных вопросов. Причём это будет такая единая площадка, куда смогут приходить заказчики со своими проблемами, в поисках того или иного продукта или системы, с просьбой создать определённый макет.

И это не обращение в коммерческую фирму с просьбой реализовать более или менее традиционное решение, которыми обычно занимаются разработчики коммерческих продуктов. Здесь речь идёт о решении тех задач, для которых в стране ещё нет готовых рыночных компетенций. Поэтому важная роль на этой площадке принадлежит университетской, вузовской науке.

— **Площадки такого типа не новинка...**

— Совершенно верно. Таких площадок узкоспециализированной направленности действительно немало. Есть, например, центры безопасной разработки, Технологический центр исследования безопасности ядра Linux, где строится доверенное программное обеспечение. Это тоже мероприятие программы «Цифровая экономика», и там также создана определённая кооперация на базе Института системного программирования РАН с головной организацией — ФСТЭК России. Цель — исследование ядра Linux с последующей передачей безопасного ПО бизнесу.

Почему сегодня актуален именно такой вид кооперации? Речь идёт о таких системах, где наиболее сложные и длительные исследования проводит государство, конечно, во

взаимодействии с бизнесом, а полученные результаты дальше масштабируются, внедряются. Скажем прямо, не все задачи такого рода мы научились решать. Например, ещё не построили кооперацию для высокопроизводительных NGFW, необходимых для обеспечения взаимодействия между ЦОДами, для банковских систем, крупных корпораций. За эту задачу сразу взялось много компаний, на рынке появляется много решений, но нет значительного рывка вперёд. Нужно, чтобы все эти участники рынка объединили свои усилия и в единой кооперации решили системные проблемы: от создания соответствующей аппаратной базы до программной части.

Кооперацию такого типа мы сейчас и стараемся построить. Она станет составной частью госпрограммы «Национальная экономика данных», которая сейчас проектируется. И естественно, будет связана со специальными направлениями госпрограммы, в частности, с программой развития микроэлектронной продукции. Думаю, что в ходе подготовительных работ проявятся новые аспекты кооперации науки, государства и бизнеса.

О ДВИЖУЩИХ СИЛАХ

— **В новой кооперации с наукой и государством компании-разработчики должны научиться работать по-новому. Как вы полагаете, с этой задачей справятся нынешние игроки или должны появиться компании-стартапы нового типа?**

— Я лично считаю, что сфере информационной безопасности нужен приток новых стартапов. Но есть нюансы. Во-первых, область ИБ сильно регулируется, требуются лицензии на осуществление деятельности в этой сфере. Во-вторых, на рынке наблюдается процесс укрупнения компаний, специализирующихся в области кибербезопасности, как ответ на запрос обеспечения комплексной информационной безопасности заказчиков. В-третьих, заказчики заинтересованы в привлечении лучших игроков ИБ-рынка, которые могут гарантировать высокое качество внедряемых решений в нынешних условиях, когда информационная безопасность находится в фокусе внимания. Понятно, что в таких условиях молодой, пусть и амбициозной, компании работать на рынке сложно.

Однако, если этого не будет, отрасль рискует превратиться в конгломерат «удельных княжеств» из 4–5 крупных компаний, которым, как, кстати, глобальным вендорам на локальном рынке, отдельные мелкие задачи

могут показаться неинтересными: раз прибыль небольшая, нет смысла тратить ресурсы.

Поэтому должна реализоваться история с притоком стартапов, но при поддержке государства и при участии крупных игроков рынка. Как это может выглядеть на практике?

Есть место — площадка кооперации, где консолидируются нетривиальные запросы заказчиков. Там может появиться стартап, который заявляет о том, что знает решение проблемы. Его инициативу подхватывают, и дальше он сам во взаимодействии с какой-либо крупной компанией демонстрирует работоспособное решение. Вполне возможно, что он будет поглощён крупным игроком, но это не страшно, потому что и задача заказчика будет решена, и плодотворная оригинальная идея стартапа получит «путёвку в жизнь».

В целом идея не принципиально новая. Нечто подобное делает, например, «Сколково». Но описанный механизм обязательно должен быть реализован, иначе мы рискуем остаться Ахиллесом, который никак не может догнать черепаху...

КЛЮЧЕВЫЕ ЗАДАЧИ 2024 ГОДА

— Какие у вас главные ожидания от 2024 года?

— Запуск «Национальной экономики данных» — это 2025 год, и в течение 2024 года её нужно будет активно отстраивать. Понятно, что будет проходить красной нитью через всю госпрограмму — Secure-by-design, обеспечение информационной безопасности на самой ранней стадии. Это направление было задано Указом Президента Российской Федерации № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» от 30.03.2022.

Это большое направление, по которому работает много рабочих групп. И в среде специалистов по ИБ уже есть понимание, как правильно строить цепочку действий в разработке того или иного средства защиты. Теперь это понимание нужно нести всем — и заказчикам, и коллегам из смежных ИТ-сегментов. Думаю, что 2024-й будет годом активного погружения всех в детали практической реализации концепции Secure-by-design, переходом от призыва «Так надо!» к её системной реализации на практике. И далее в ходе реализации планов «Национальной экономики данных» в 2025–2030 гг., как я рассчитываю, все будем работать по-новому. В том числе подоспеет отечественная микроэлектроника.

ПРО МАГНИТКУ

— В феврале состоится конференция «Цифровая устойчивость и информационная безопасность России» — продолжение легендарной «Магнитки», где Минцифры выступает организатором. Какие цели и задачи ставите, чего ожидаете?

— Для организации любой конференции самое важное — понять, кто, что и кому рассказывает. Эта конференция — отраслевая, здесь компании ИБ взаимодействуют с отраслями: энергетика, финансовая сфера, транспорт и т.д. Специалисты по ИБ расскажут о тех методах и технологиях защиты, которыми они владеют, а коллеги из отраслей подскажут, какие специфические особенности необходимо учитывать, помогут поставщикам продуктов дорабатывать узкопрофильные вещи. Ведь даже риски ИБ у отраслей существенно разнятся. Если для банков особо важными являются риски мошенничества, кражи данных, то у энергетиков — это компьютерные атаки, которые могут вывести из строя оборудование, критически важное для жизнеобеспечения города или даже региона.

И решения одного класса могут сильно различаться по технической реализации в разных областях. Скажем, для решения Интернета вещей в транспортной сфере важна поддержка передачи данных в движении, а для энергетики — абсолютная достоверность показаний датчика, передающего данные о состоянии критически важных параметров производственной установки.

Мы ожидаем, что результатом конференции станет налаживание полноценного взаимодействия отрасли ИБ с различными отраслями экономики страны. Как строить отраслевые центры обеспечения безопасности? Как обеспечить взаимодействие отрасли с ними, с системой ГосСОПКА? Как наладить эффективное взаимодействие отраслевого бизнеса с государством, в том числе с регуляторами в сфере ИБ?

Координация совместных усилий по ускоренному движению в сторону технологического суверенитета — вот чего хочется достичь в ходе конференции. А дальше начнётся предметная работа по тонкой настройке продуктов и решений информационной безопасности на специфические потребности конкретных отраслей и максимально быстрые проекты их внедрения на предприятиях разных отраслей.

Беседовала
Елена Покатаева

ЦИФРОВИЗАЦИЯ — ЭТО НЕ ТОЛЬКО ВНЕДРЕНИЕ ИННОВАЦИЙ

ЭТО И «УМНОЕ» РАЗВИТИЕ И ИЗМЕНЕНИЕ ПОДХОДА К БИЗНЕСУ



Дмитрий МИХЕЕВ
технический директор,
«АйТи Бастион»



Константин РОДИН
руководитель отдела развития
продуктов, «АйТи Бастион»

На фоне развития технологий понятие «цифровая трансформация» становится ключевым для успешного функционирования бизнеса. Этот процесс определяет будущее предприятий и является базой для их конкурентоспособности и устойчивости.

Цифровизация в широком смысле — стратегический подход к использованию современных технологий для изменения бизнес-моделей и процессов компании. Очевидно, в его основе лежит применение цифровых технологий: искусственного интеллекта, аналитики данных и других инновационных решений и подходов. О том, как правильно это трансформировать в бизнесе, рассказывают эксперты компании «АйТи Бастион».

Цифровая трансформация направлена на повышение эффективности процессов, потому как сконцентрирована на их автоматизации и оптимизации, ведущих к повышению операционной эффективности бизнеса. Она улучшает клиентский опыт: позволяет создавать более точечные решения. Дает возможность предприятиям адаптироваться под рынок: быть более гибкими в момент его изменений.

Внедрение и использование инноваций открывает бизнесу новые возможности для развития. Анализ больших данных позволяет

принимать решения, основанные на текущей повестке, что становится преимуществом в конкурентной борьбе. Автоматизация облегчает совершение рутинных операций, что повышает эффективность бизнеса и высвобождает его ресурсы для реализации более стратегических задач.

Цифровизация — это синергия взаимодействия процессов, технологий и людей. От того, как оно будет выстроено, зависит конечный эффект: будет ли это прорыв с ростом важных бизнес-показателей, топтание на месте или тупик, который ни к чему не приведет, а обернется финансовыми издержками и репутационной несостоятельностью.

«Там, где есть бизнес-процессы и технологии, там есть и потенциальные риски. Ведь цифровая трансформация затрагивает информационные системы предприятий, изменение их технических характеристик, конфигураций, функционала, структуры, доработки системы в целом или отдельных ее сегментов. И главное здесь — уметь правильно управлять такими изменениями, чтобы они не нанесли ущерб бизнесу. Важно исключить или минимизировать ИБ-риски. И в первую очередь те, которые можно отнести к человеческому фактору. Нужно контролировать права пользователей, как правило, привилегированных, но не ограничиваясь этим, сегментировать их действия в рамках определенных бизнес-функций, следуя концепции «нулевого доверия» (Zero



Trust) — доверять, но проверять. И это уже не прихоть, а норма и даже необходимость», — комментирует **Константин Родин**.

РАЗНЫЕ СТОРОНЫ МЕДАЛИ

Следуя тренду на цифровизацию, предприятия повсеместно внедряют передовые технологии. С одной стороны, они получают возможности для увеличения скорости, эффективности работы и мониторинга всех процессов, а с другой — становятся мишенью для кибератак из-за появления новых точек уязвимости: ими могут быть и технические несовершенства в развертывании цифровых решений, и человеческий фактор. Очевидно, нужно контролировать ИТ-системы, иначе киберриски будут расти.

Существует много инструментов, которые помогают контролировать бизнес-процессы, связанные с действиями пользователей, отслеживать утечки и проводить анализ легитимности использования доступа в системы. Одни из заметных решений на сегодня — решения класса PAM (Privileged Access Management), например, «СКДПУ ИТ», применяемые в бизнесе для обеспечения

комплексной ИБ-защиты удаленного доступа в ИТ-инфраструктуру. Система контролирует внедрение, настройку и обслуживание нового программного обеспечения, мониторит уже существующие системы во избежание утечек и нарушения работоспособности периметра.

«Это особенно важно в ситуациях, когда много процессов на крупных предприятиях, например, промышленного, добывающего или финансового сектора, происходят без участия человека. Если в их работе будет малейший сбой, это приведет к остановке всего бизнеса, а, возможно, и к глобальным катастрофам. А также в ситуациях, когда функционирование ИТ-периметра контролируется живым человеком и он лично отвечает за обеспечение корректности работы и бесперебойности конкретных бизнес-процессов. Именно поэтому необходимо принимать меры для всестороннего контроля, который обеспечивают PAM-системы», — отмечает **Дмитрий Михеев**.

КЛЮЧ К ДОСТИЖЕНИЮ ЦЕЛЕЙ

Но контроль пользователей — это не «волшебная пиллюля» от всех потенциальных

кибербед. Важно подходить к проблеме комплексно и выстраивать многоуровневую цепочку защиты ИТ-структуры. А когда дело касается передачи информации — уделять этому особое внимание, и для эффективности мер — разграничивать зоны ответственности. Работать не вместо человека, а ему в помощь, автоматизировать «с умом». Потому что любая автоматизация должна быть связана на контролируемой связи объектов, контролируемом доступе и разделении зон и ответственности между ними.

Такой подход развернут в системе «Синоникс», программно-аппаратном шлюзе безопасного объединения сетей, предназначенном для использования в автоматизированных информационных системах для обработки данных. Решение позволяет организовать безопасный обмен информацией между разными сетями или узлами одной сети в режиме передачи данных с контролем направления, предотвращая распространение киберугроз и потенциально возможного вредоносного взаимодействия между сетями. Изолированными получаются не только сегменты данных, но и возможности пользователей, ответственных за работоспособность инфраструктуры. Тем самым происходит автоматизация процессов в рамках строго определенных оцифрованных бизнес-задач с минимизацией рисков безопасности со стороны человека.

«Система применима для решения конкретных бизнес-сценариев, например, для передачи телеметрии, информации с конечных объектов, которые обладают фактурой, но не обладают нужной для бизнеса аналитикой. «Синоникс» обеспечивает встречный контроль правил обмена данными, результат которого основывается на согласованном решении конкретных людей. Дает возможность быстро отключить и подключить доступ на физическом и логическом уровнях. Позволяет автоматизировать задачи по передаче крупных объемов информации, включая файловый обмен, не раскрывая при этом особенности стыкуемых архитектур друг другу, и снизить риски полной компрометации узла объединения», — добавляет **Дмитрий Михеев**.

РАЗДЕЛЕНИЕ ПОЛНОМОЧИЙ И ОТВЕТСТВЕННОСТИ

Период «единых систем для всего на свете» сменяется процессно-ориентированным подходом, а полная физическая изоляции сетей и сегментов уступает решениям, способным организовать связь между ними под точечную задачу. В общем виде, это можно выразить словами «только требуемый доступ, только определенные системы, только заданные права доступа». Нужно действовать в разрезе концепции минимально доступных полномочий. Когда выдан доступ к ИТ-системе, но только строго в рамках прав, которые нужны конкретным людям для реализации процессов.

То есть комплексами решений — от МЭ и систем обнаружения вторжений до РАМ и систем объединения изолированных систем — разделять полномочия и создавать цельные системы управления с привилегированным, критически важным доступом за счет применения разных ИБ-технологий: изоляции, сегментации, контроля и пр.

«Здесь идет речь про возможности построения конкретных бизнес-ориентированных систем по обеспечению информационной безопасности. Не про слепое следование регуляторной практике или полного ограничения всех возможных прав в надежде, что это спасет предприятие от взломов, утечек и компрометаций. Да, системы такой подход, возможно, и спасет, но бизнес в целом — скорее нет. Не спасет он и цифровую трансформацию от необходимости применения единого, эффективного, а лучше сказать «умного» управления каждым отдельным сегментом, объектом и элементом системы», — отмечает **Константин Родин**.

Инновации не всегда подразумевают новые технологии. Зачастую это про новый взгляд на ранее решенные проблемы под новым углом и с новыми возможностями. И потому цифровизация — это не просто внедрение новых технологий. Это изменение подхода к бизнесу в целом по всем направлениям.



ОТ РЕДАКЦИИ

Дорогие читатели, тема номера «Планирование цифровых прорывов» собрала сумму противоречивых мнений со стороны экспертов ИТ и ИБ разных уровней. Получилась очень объемная дискуссия. Но по техническим причинам мы не успеваем опубликовать ее в этом номере и вынуждены перенести в следующий. Приносим свои извинения и заверяем: игра стоит свеч, вы не будете разочарованы. До встречи в следующем номере!



КОНФЕРЕНЦИЯ РУСКРИПТО '2024

КРИПТОГРАФИЯ КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА
ЗАЩИТЫ ИНФОРМАЦИИ РОССИЙСКАЯ КРИПТОГ
РАФИЯ ОТЕЧЕСТВЕННЫЕ ОПЕРАЦИОННЫЕ СИСТЕ
МЫ ЭЛЕКТРОННАЯ ПОДПИСЬ ЭЛЕКТРОННЫЙ ДОКУ
МЕНТ ОБОРОТ КРИПТОГРАФИЯ В ФИНАНСОВОЙ
СФЕРЕ ЦИФРОВАЯ КРИМИНАЛИСТИКА СУДЕБНАЯ
ЭКСПЕРТИЗА КВАНТОВАЯ КРИПТОГРАФИЯ КВАНТ
ОВЫЕ КОММУНИКАЦИИ БЕЗЛИЧивАНИЕ ДАННЫХ М
АШИ ННОЕ ОБУЧЕНИЕ НИЗКОРЕСУРСНАЯ КРИПТО
ГРАФИЯ ИНТЕРНЕТА ВЕЩЕЙ ТЕХНОЛОГИИ ИНФОР
МАЦИОННОЙ БЕЗОПАСНОСТИ В КИИ ОТРАСЛЕВЫ
Е ОСОБЕННОСТИ ПРИМЕНЕНИЯ СКЗИ ДОВЕРЕННЫ
Е ИНФОРМАЦИОННЫЕ СИСТЕМЫ ТЕОРЕТИЧЕСКАЯ
И ПРИКЛАДНАЯ КРИПТОЛОГИЯ СТЕГАНОГРАФИЯ
РЕВЕРС ИНЖИНИРИНГ ЗАЩИТА ОТ НЕСАНКЦИОНИ
РОВАННОГО ДОСТУПА ЗАЩИТА ПРОГРАММНОГО
ОБЕСПЕЧЕНИЯ БЕЗОПАСНАЯ ЦИФРОВАЯ СРЕДА

26 конференция | 700+ участников | 75+ докладов

Международная научно-практическая конференция РусКрипто — это теория и практика, презентации новых технологий, обмен мнениями и опытом специалистов в области криптографии и защиты информации

Организаторы: Академия Информационных Систем и Ассоциация РусКрипто

19 - 22
марта 2024



«МЫ НЕ СМОЖЕМ ЗАЩИТИТЬ СВОЙ СУВЕРЕНИТЕТ, НЕ ОБЕСПЕЧИВ ТЕХНОЛОГИЧЕСКУЮ САМОСТОЯТЕЛЬНОСТЬ СТРАНЫ»

VIS JOURNAL ПОПРОСИЛ ВАСИЛИЯ ПИСКАРЕВА ПОДВЕСТИ ИТОГИ ГОДА И РАССКАЗАТЬ О ПОЕЗДКЕ В КИТАЙ



Василий ПИСКАРЕВ
председатель Комитета
Государственной Думы
по безопасности и противодействию
коррупции

Наш Президент Владимир Владимирович Путин в ходе прямой линии с гражданами в качестве приоритетной задачи назвал укрепление суверенитета. Он подчеркнул, что «для такой страны, как Россия, просто существование без суверенитета невозможно, её просто не будет». Президент уточнил, что речь идёт и об укреплении обороноспособности, и об обеспечении прав и свобод граждан, и о финансово-экономическом и технологическом суверенитете страны.

В связи с этим хотел бы поделиться впечатлениями от недавней поездки в Китай. Я побывал там в конце ноября в составе представительной делегации Государственной Думы во главе с Вячеславом Викторовичем Володиным. В Пекине мы встретились с Председателем КНР Си Цзиньпином, провели переговоры в парламенте, познакомились с опытом развития экономики и образования в Поднебесной.

Для меня это было не первое пребывание в Китае. Мы регулярно встречаемся с коллегами и даже в период антикоронавирусных ограничений общение не прерывали, связывались в видеорежиме. И знаете, каждую поездку в Китай удивляет то, как сочетается в этой стране верность традициям, своему прошлому с технологическим прорывом. Китай сегодня всё увереннее занимает лидирующие позиции в мире, и союзнические отношения для наших стран очень важны. Убеждён, по многим направлениям, где наши страны добились наибольших успехов, мы будем взаимодополнять друг друга.

Не случайно на этот раз Китай посетила представительная делегация Госдумы. Она включала и глав комитетов, и руководителей фракций. Сегодня Россия и Китай

сталкиваются с жёстким давлением извне, попытками расшатать наши государства изнутри, затормозить экономическое развитие. И конечно, обмен законодательным опытом, в том числе в сфере защиты суверенитета, для нас очень важен. Мы стремимся выстроить ещё более тесное сотрудничество с китайскими коллегами для решения задач, которые стоят перед нашими странами, в том числе в сфере безопасности и противодействия иностранному вмешательству.

Признаюсь, мы с интересом познакомились с тем, как построена система образования в Китае. Посетили и университет, и начальную школу «Шицзя» в Пекине. Там младшеклассники, помимо основных традиционных школьных дисциплин, изучают основы спутниковой связи, создания электросхем, моделирования и управления дронами. Очень правильный подход. Это и профессиональная ориентация с ранних лет, и обретение полезных навыков. В конце прошлого года Государственная Дума приняла решение о возвращении уроков труда в школу, и я понимаю, что речь должна идти не только о том, чтобы научить детей мастерить и готовить, что, конечно, важно, но и о том, чтобы познакомить их с современными технологиями.

Почему я на этом акцентирую внимание? Наши соседи неслучайно доверяют малышам паять микросхемы. Это стратегия привлечения в передовые отрасли молодой смены. Не все сразу заинтересуются, но, возможно, многие выберут перспективную специальность. А микроэлектроника — это одна из составляющих государственного суверенитета любой страны.

Сегодня перед нами стоит задача достичь технологического суверенитета, освоив те технологии, которые мы ранее завозили из-за рубежа, и те, которыми мы когда-то владели, а в период безвременья утратили. Когда-то Советский Союз помог Китаю создать собственную промышленность, в том числе автомобильную. С тех пор прошло много лет, наши соседи сначала копировали самые передовые образцы, потом уже развивали своё, и сегодня мы видим успехи китайского автопрома на наших улицах. Надо делать выводы.

Стоит сказать, что Россия всегда была богата самородками, и мы должны создавать условия для того, чтобы наши таланты могли реализовать свой потенциал. Думаю,



Делегация Государственной Думы в Китае. В центре — Председатель Государственной Думы Вячеслав Володин и Председатель КНР Си Цзиньпин, крайний справа — Председатель Комитета Государственной Думы по безопасности и противодействию коррупции Василий Пискарев

сегодня уже всем понятно: прозвучавшая некогда фраза, что советская школа растила творцов, а нам нужно готовить квалифицированных потребителей, давала ошибочный вектор развития, и пора нам его выправлять.

Сегодня всё больше стран задумываются о собственном суверенитете, хотя бы избавиться от диктата США, который не ослабевает, а усиливается, хотя США уже не те, какими были 50 и даже 30 лет назад. И эта борьба будет нарастать. А технологический суверенитет будет приобретать всё большее значение. Не случайно Соединённые Штаты запрещают поставлять самые современные чипы даже в Турцию, ОАЭ и Саудовскую Аравию. В Вашингтоне понимают, что с позиции силы могут разговаривать только со слабыми государствами, которые находятся от них в технологической и экономической зависимости. Сегодня мы видим разрушение их монополии, и простыми запретами на поставки тех или иных товаров им этого не остановить.

В связи с этим я бы выделил ещё одну составляющую суверенитета — информационный суверенитет. Соединённые Штаты рекламировали интернет как открытое общее пространство. Они очень шумно всегда протестуют, когда мы пытаемся ограничить распространение деструктивной информации в нашем сегменте интернета, будь то пропаганда наркотиков, распространение порнографии или рецептов изготовления боеприпасов. Но за показной открытостью американский интернет очень жёстко контролируется, и они без всяких



Делегация Государственной Думы в начальной школе «Шицзя» в Пекине

лишних разговоров заблокировали у себя все наши СМИ и телеканалы, когда им понадобилось демонизировать нашу страну, а правда о происходящем в России оказалась невыгодна.

Показательный момент. Газета «Файненшиал Таймс» в одной из недавних публикаций помогла вскрыть методику Евросоюза, которая применяется с целью вмешательства во внутренние дела нашей страны накануне выборов Президента России. По данным газеты, высокопоставленные еврочиновники оказывают давление на медиагигантов с целью обеспечить преференции для ряда СМИ, работающих в информационном пространстве России.

В частности, Еврокомиссия настоятельно рекомендует продвигать на лидирующие позиции в новостных агрегаторах материалы так называемых российских независимых изданий, а также монетизировать их русскоязычный



Председатель Комитета Государственной Думы по безопасности и противодействию коррупции Василий Пискарев на трибуне Государственной Думы

контент, размещённый на видеохостинге. Судя по всему, речь идёт о СМИ-иноагентах.

Всё это наглядно показывает важность и правильность принятия в нашей стране пакета законов, направленных на обеспечение открытости и финансовой прозрачности в деятельности зависимых от иностранного заказчика СМИ и физических лиц. А ещё напоминает о том, что, как бы ни было сложно конкурировать с западными медиагигантами, мы обязательно должны иметь отечественное программное обеспечение и свои видеохостинги, новостные агрегаторы и другие медиаресурсы, которые предлагают нашим пользователям не деструктивный контент, а объективную и полезную для развития информацию. И в этом плане появление в нашем интернет-пространстве онлайн-энциклопедии «Рувики» (отечественного аналога Википедии) — позитивный шаг вперёд.

Что же касается законодательной поддержки, в том числе регулирующего характера, мы её уже оказываем. Среди последних инициатив — законопроект, в разработке которого я принимал участие, об ответственности за ведение так называемых треш-стримов — онлайн-трансляций со сценами совершения противоправных действий с особой жестокостью, садизмом и унижением. Этому явлению мы должны создать надёжный барьер.

Ещё один наш законопроект, который сейчас находится на рассмотрении в Государственной Думе, появился как реакция, в частности, на пропаганду так называемого массшутинга — массовых убийств в учебных заведениях и детских садах. Оправдание подобных страшных преступлений и попытка представить их «модными» в молодёжной среде через интернет и соцсети — крайне опасная тенденция. Поэтому мы предложили внести изменения в статью 280 УК РФ («Публичные призывы к

осуществлению экстремистской деятельности»). В случае принятия законопроекта Государственной Думой ответственность будет грозить также за публичное оправдание или пропаганду экстремизма наравне с ответственностью за призывы к осуществлению экстремистской деятельности. Наказание по этой статье предусмотрено от штрафа до 300 тысяч рублей и вплоть до пяти лет лишения свободы. Этому явлению, пришедшему к нам с Запада, — и оно намеренно навязывается и пропагандируется внешними силами в нашем информационном пространстве, — мы также должны решительно противостоять. Считаем, что принятие наших поправок будет важной профилактической мерой, направленной в первую очередь на защиту детей и молодёжи от деструктивного влияния экстремистской идеологии и попыток вовлечь их в противоправную, опасную деятельность.

В заключение отмечу, что в отношении информационного суверенитета позиции России и Китая во многом совпадают, и это зафиксировано в документах ШОС, где особое внимание уделено ответственному поведению государств в информационном пространстве и обеспечению равных для всех стран прав на управление своим национальным сегментом в сети. Китай выстроил свою жёсткую систему регулирования в интернете, мы решаем проблемы немного по-другому, но мы сходимся в главном — в информационном пространстве должны соблюдаться принципы взаимного уважения государств и невмешательства во внутренние дела. Сотрудничество в этой сфере мы обязательно продолжим.

ТЕСТ НА ПРОНИКНОВЕНИЕ: ЧЕГО-ТО НЕ ХВАТАЕТ...

ЗАКОН ЕСТЬ, НО КАК ЕГО ВЫПОЛНЯТЬ?



**Александр
ВИНОГРАДОВ**
ФГУП
«ЦНИИХМ»



**Константин
ГРАЧЁВ**
ООО «Максима»



**Анастасия
НИКОЛАЕВА**
BIS Journal

В 2017 г. в России был принят Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», исходя из которого отраслевому регулятору вменялось разработать комплекс мер, направленных на проведение аудита состояния информационной безопасности объектов КИИ и обеспечения её защищённости. В результате была разработана и принята нормативная база, включающая как одну из мер аудита тест на проникновение.

Банк России включил данную меру аудита в подзаконные акты — Положения Банка России № 683-П, № 719-П. Другие регуляторы включили соответствующие положения в другие нормативные документы:

- ♦ Распоряжение Правительства РФ от 28-08-2019 г. № 1911-р;
 - ♦ Приказ Минфина от 01-06-2023 г. № 80н;
 - ♦ Приказ Минцифры России от 28.02.2022 № 143;
 - ♦ Приказ ФСТЭК России от 25.12.2017 № 239;
 - ♦ Приказ Минцифры России от 11.05.2023 № 449;
 - ♦ Приказ Минкомсвязи России от 30.01.2019 № 22
- ...и это не полный список.

ПОСТАНОВКА ПРОБЛЕМЫ

Тестирование на проникновение (от англ. pentest, сокр. от penetration test) — метод оценки степени защищённости компьютерных систем или сетей средствами моделирования сценария атак злоумышленника. Анализ системы безопасности ведётся с позиции потенциального атакующего и может включать в себя активное использование уязвимостей системы. Результатом работы является отчёт, содержащий в себе найденные уязвимости, а также рекомендации по их устранению. Цель испытаний на проникновение — оценить возможность его осуществления в различных сценариях проведения атак на информационные ресурсы.

Проанализировав нормативную базу Законодательства РФ, мы не смогли найти полноценной

методики проведения теста на проникновения. Были несколько попыток создать что-то единое, но они остались только в проектах.

В то же время в международной практике проведение тестов на проникновение регламентируется стандартами и методиками, которые регламентируют этапы тестирования, порядок испытаний тестируемых объектов, порядок взаимодействия аудитора с заказчиком и т.д.

К широко распространённым зарубежным стандартам и методикам относятся:

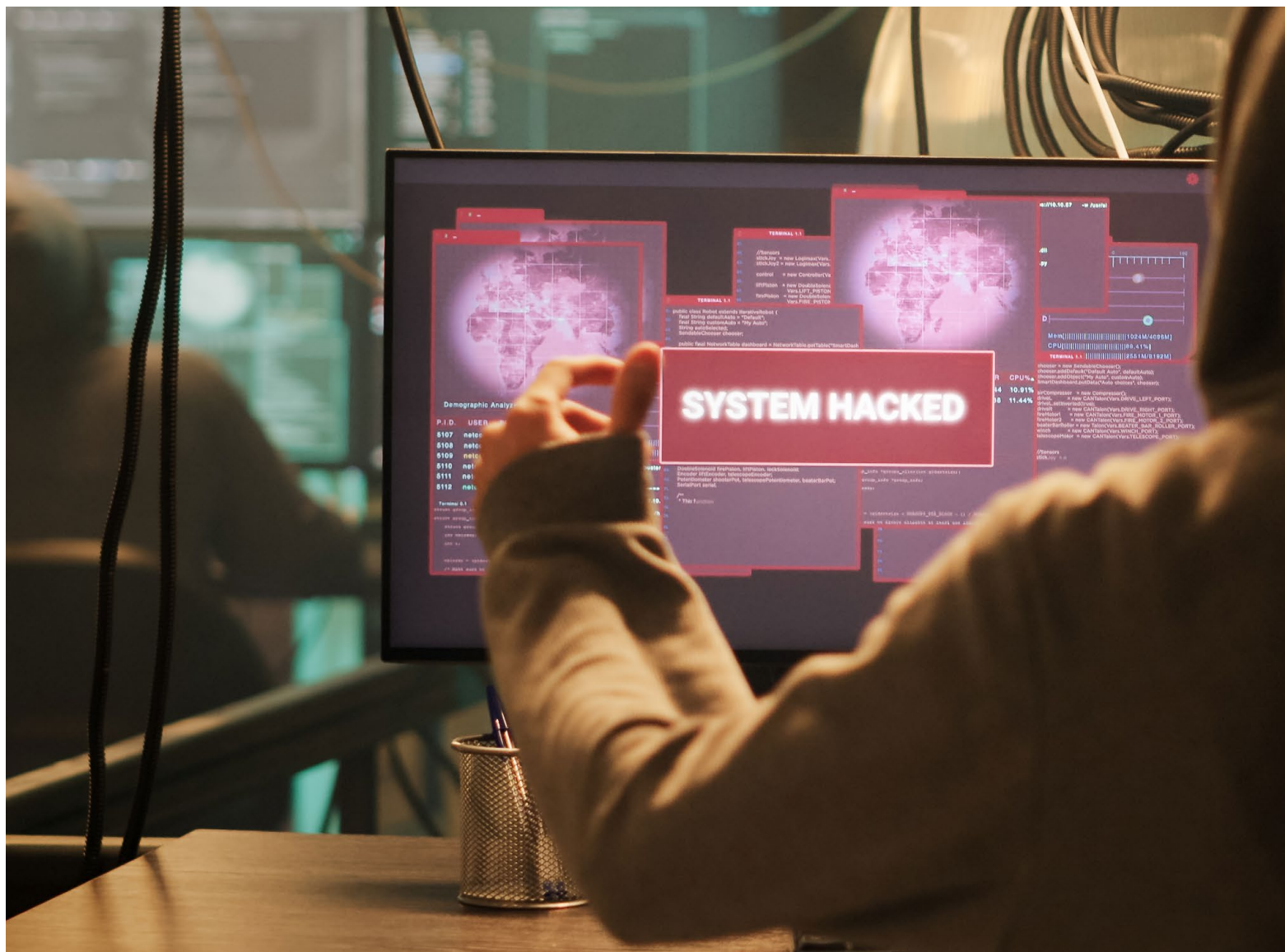
- ♦ методика OSSTMM — The Open Source Security Testing Methodology Manual;
- ♦ методика ISSAF — Information System Security Assessment Framework;
- ♦ методика OWASP — Open Web Application Security Project;
- ♦ стандарт PTES — Penetration Testing Execution Standard;
- ♦ стандарт NIST SP 800-115 — Technical Guide to Information Security Testing and Assessment;
- ♦ методика BSI — Study a Penetration Testing Model;
- ♦ методика PETA — Methodology of Information Systems Security Penetration Testing;
- ♦ методика PTF — Penetration Testing Framework.

Среди отечественных практик можно упомянуть ГОСТ Р 58143-2018 «Методы и средства обеспечения безопасности. Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045. Часть 2. Тестирование проникновения».

Рассмотрим более подробно некоторые из представленных выше методик.

МЕТОДИКА OSSTMM

OSSTMM — это универсальный, базовый стандарт при тестировании на проникновение, благодаря которому можно выстроить чёткий план, шкалу оценивания уровня безопасности. Благодаря данному способу этот метод имеет возможность индивидуально оценить уровень



безопасности, учитывая при этом и отраслевые, и технологические характеристики компании. Руководство по методологии тестирования безопасности — с открытым исходным кодом.

Методика OSSTMM является в высокой степени формализованным и хорошо структурированным документом, регламентирующим практически все аспекты тестирования на проникновение, ориентирована на тестирование преимущественно компьютерных сетей. Методика обновляется с завидной периодичностью.

Методика OSSTMM содержит следующие разделы:

- ◆ информационная безопасность;
- ◆ тестирование процесса безопасности;
- ◆ тестирование безопасности интернет-технологий;
- ◆ тестирование безопасности каналов связи;
- ◆ тестирование безопасности беспроводных технологий;
- ◆ тестирование физической безопасности.

Как таковой классификации уязвимостей в этой методике нет. Понятие «уязвимость» в методике вводится как ограничение безопасности — это дефект или ошибка,

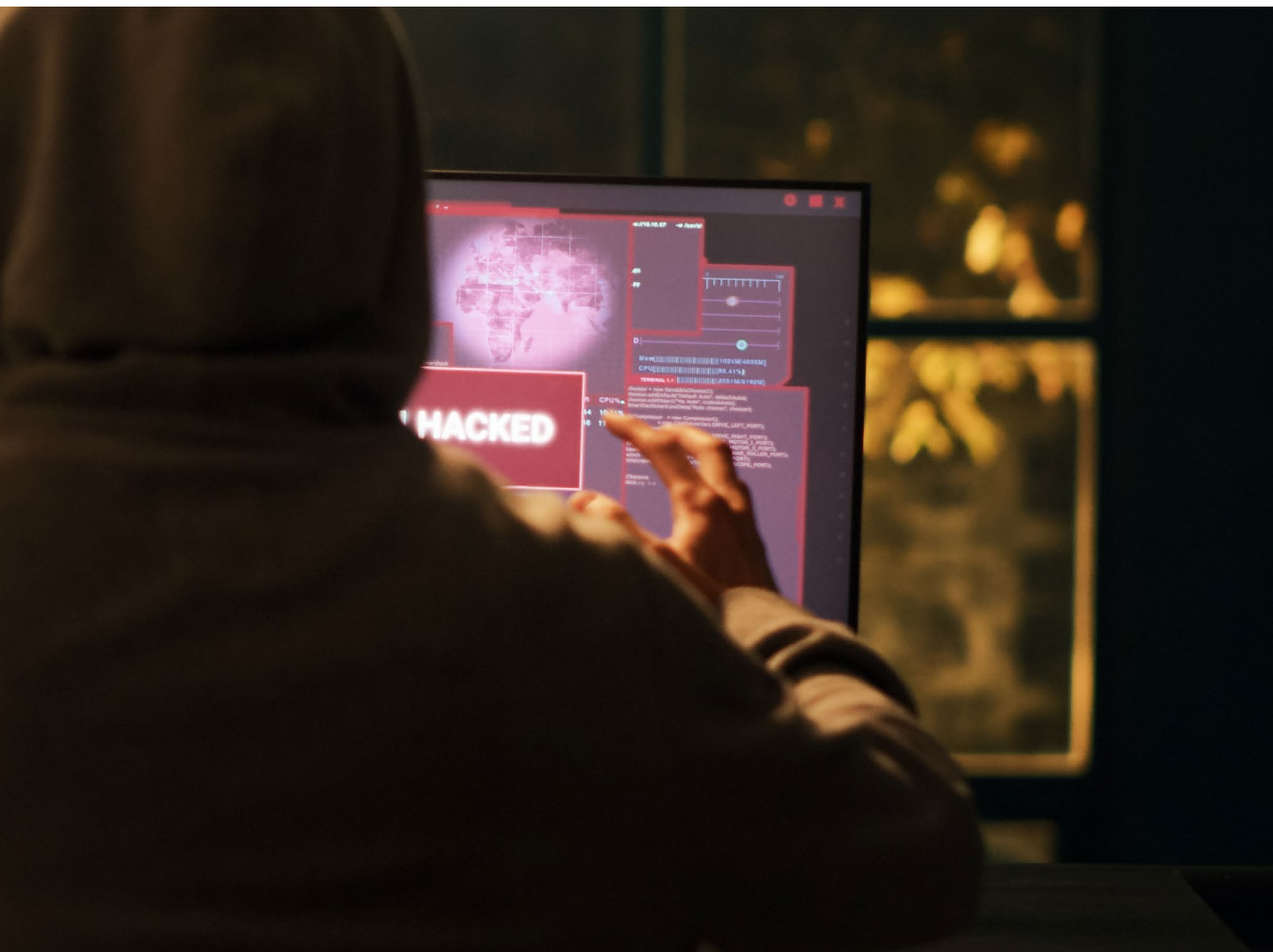
которая запрещает доступ авторизованным пользователям или процессам к информационным ресурсам или позволяет несанкционированный доступ (НСД) неавторизованных пользователей или процессов к ресурсам.

Итог: данную методику можно использовать как на этапе предварительной оценки защищённости объектов, так и на этапе разработки объектов. Из недостатков стоит отметить малое количество информации по практическим действиям и инструментарию тестирования, а также отсутствие полного описания процесса проведения тестирования отдельных модулей информационной системы.

МЕТОДИКА ISSAF

Метод ISSAF разработан OISSG (Open Information Systems Security Group) для внутренних контрольных проверок.

Документ охватывает огромное количество вопросов, связанных с информационной безопасностью. Присутствуют главы, описывающие оценку безопасности межсетевых экранов, маршрутизаторов, антивирусных систем и многого другого.



Данный метод включает три этапа:

а) планирование и подготовка — получение начальной информации, планирование и подготовка к тестам, заключение договора, определение сроков, объектов и методов тестирования;

б) оценка — выполнение тестирования на проникновение;

в) отчётность — разработка отчёта о тестировании.

Итог: ISSAF — один из самых сложных, но в то же время популярных способов.

МЕТОДИКА OWASP

OWASP — международное открытое сообщество, нацеленное на улучшение безопасности программного обеспечения. Каждый имеет право участвовать в OWASP, и все их материалы свободно распространяемы. OWASP Testing Guide представляет собой более широкую методологию по сравнению с другими, так как даёт указания не только по тестам на проникновение, но и по анализу веб-приложений в целом (к примеру — исходного кода), поскольку эта методика фокусирует

своё внимание именно на обнаружениях уязвимостей веб-приложений.

Эксперты организации каждые 3–4 года обновляют OWASP Top Ten — список критических уязвимостей веб-приложений. Он помогает разработчикам и специалистам по информационной безопасности создавать и поддерживать безопасные сайты и приложения.

В последней редакции OWASP Top Ten названы следующие уязвимости на 2021 г.:

A01:2021 — нарушение контроля доступа;

A02:2021 — криптографические сбои;

A03:2021 — инъекции;

A04:2021 — небезопасный дизайн;

A05:2021 — неправильная конфигурация безопасности;

A06:2021 — уязвимые и устаревшие компоненты;

A07:2021 — ошибки идентификации и аутентификации;

A08:2021 — нарушения целостности программного обеспечения и данных;

A09:2021 — ошибки ведения журнала и мониторинга безопасности;

A10:2021 — подделка запросов на стороне сервера.

СТАНДАРТ PTES

Стандарт, разработанный для объединения как бизнес-требований, так и возможностей служб информационной безопасности и масштабирования тестов на проникновение. На первом подготовительном этапе подробно рассматриваются устанавливаемые каналы коммуникаций, правила взаимодействия и контроля, конкретные способы реагирования и мониторинга инцидентов. Далее выделены следующие этапы:

- ◆ сбор информации;
- ◆ моделирование угроз;
- ◆ методы анализа уязвимостей;
- ◆ эксплуатация — обеспечение обхода контрмер и обнаружение наилучшего пути атаки;
- ◆ постэксплуатация — анализ инфраструктуры, последующее проникновение в инфраструктуру, зачистка и живучесть.

СТАНДАРТ NIST SP 800-115

Создан и поддерживается подразделением NIST — CSRC, центром по компьютерной безопасности, объединяющим специалистов федеральных служб, университетов, крупнейших ИТ-компаний США.

Методика NIST была изначально предназначена для государственных организаций, но в ней также рассматривается возможность использования и негосударственными организациями. Она не предназначена для проведения комплексного тестирования уровня информационной безопасности, поскольку содержит лишь ключевые элементы технического тестирования и оценки безопасности. В методике NIST основной упор делается на теоретическое обоснование того, как эти техники могут быть применены. В ней не содержится информации о том, какие техники должны быть применены и при каких обстоятельствах. Таким образом, пентестерам предоставляется гибкость в определении техник, которые более всего подходят в их ситуации.

Особенности методики NIST:

- ◆ подготовлена для оценки безопасности в государственных организациях;
- ◆ детально описывает ключевые элементы технического тестирования;
- ◆ предоставляет гибкость при выборе подходов к тестированию (внешнее или внутреннее; скрытое или открытое);
- ◆ описывает уровень подготовки, необходимый для проведения тестирования;
- ◆ содержит расширенное описание методов социальной инженерии.

Недостатки NIST:

- ◆ не содержит конкретных примеров тестирования;
- ◆ не описывает механизмы защиты от уязвимостей.

МЕТОДИКА BSI

Разработана немецким подразделением Federal Office for Information Security. В методике описывается проведение корректных испытаний системы на устойчивость. Подробно описываются не только сама методология

тестов, но и необходимые требования, правовые аспекты применения методологии и процедуры, которые необходимо выполнить для успешного проведения тестов. В приложениях содержится описание ПО, которое можно использовать для тестирования объектов, описанных в методике.

Согласно методике BSI, выделяется три основных типа воздействий:

- 1) информационно-техническое воздействие через сеть;
- 2) тестовые информационно-психологические воздействия и социальная инженерия;
- 3) обход физических мер безопасности.

Данную методику рекомендуется использовать для тестирования конечного продукта. Методика BSI является достаточно подробной, а её разработчики старались предусмотреть все аспекты тестирования на проникновение: технические, организационные, правовые.

МЕТОДИКА PETA

Методика PETA — пример проектного подхода к организации тестирования информационных систем. Данная методика предлагает следующую последовательность этапов тестирования на проникновение:

- 1) планирование;
- 2) тестирование;
- 3) формирование отчёта.

Вышеуказанные этапы в данной методике формализованы в виде процессной модели, которая, однако, описана не очень подробно. Методика является достаточно обзорной и определяет только самые общие подходы к проведению тестирования на проникновение, оставляя выбор конкретных целей тестирования, используемых в тестах на информационно-техническое воздействие, и прочие параметры тестирования на усмотрение заказчика и аудитора.

МЕТОДИКА PTF

Методика PTF — детальное техническое руководство по проведению тестирования на проникновение в технической части. Данное руководство не содержит общетеоретической информации, подобно методикам OSSTMM или ISSAF, однако предоставляет практически исчерпывающий перечень уязвимостей объекта, подлежащих проверке, в некоторых случаях с указанием рекомендуемого порядка проведения тестирования и инструментария для него.

Необходимо отметить, что методика PTF фактически является частным проектом специалиста по ИБ К. Оггеу. Вместе с тем данная методика получила большое число положительных отзывов специалистов по тестированию на проникновение, которые использовали данную методику как первооснову для разработки своего варианта тестирования.

ГОСТ Р 58143-2018

На основе ГОСТ Р 58143-2018 можно проводить разработку тестов на проникновения на основе иденти-

фикационных шаблонов атак, а также с использованием метода гипотез (предположений) о недостатках тестируемой системы. Используя результаты определения шаблонов атак и идентификации соответствующих уязвимостей и недостатков, эксперт разрабатывает план тестирования проникновения, определяя соответствующий шаблон атаки, порядок выполнения атаки, условия проведения атаки, порядок тестирования и ожидаемые результаты.

Данный стандарт содержит детализацию рекомендаций по планированию, выполнению и составлению отчётности тестирования проникновения объекта оценки.

ИТОГО

Многие организации в России проводят данный тест, но по утверждённым в своих локальных актах программам, которые согласуются с заказчиком.



Александр МОИСЕЕВ

ведущий консультант
по информационной безопасности
AKTIVCONSULTING

В действительности ситуация имеет следующий вид: для каких-то отраслей установлены требования по проведению теста на проникновение в явном виде, для каких-то даётся только рекомендация по применению меры. Например, в финансовой отрасли пентесты обязательны, а в МЭК 63096 по безопасности объектов атомной энергетики рекомендательны. Для их проведения существует большое количество общих верхнеуровневых фреймворков, которые позволяют оптимально выстроить процесс, но в то же время отсутствуют те самые детальные методические рекомендации, которые определяют последовательные шаги при тестировании на проникновение, а также требования к формированию отчёта.

В первую очередь эта ситуация обусловлена тем, что такие рекомендации на данный момент описаны только коммерческими организациями, оказывающими услуги по проведению пентестов. Но эта детализированная техническая информация является проприетарной, то есть имеет высокую коммерческую ценность для этих компаний. Раскрыть её — всё равно что разгласить коммерческую тайну или собственное ноу-хау. Задача по формированию общей методологии под силу скорее государственным ведомствам и органам власти.

В большинстве случаев проведение тестов на проникновение внешними подрядчиками (исполнителями работ) охватывает и внутренний, и внешний аудит.

Анализ защищённости внешнего периметра включает в себя:

- ♦ полную проверку доступных ресурсов;
- ♦ поиск уязвимостей операционной системы и сетевой инфраструктуры;
- ♦ сбор общедоступной информации о внешних ресурсах;
- ♦ сбор данных об инфраструктуре;
- ♦ поиск уязвимостей с использованием сканеров защищённости и специализированного ПО;
- ♦ тестирование выявленных уязвимостей.

При анализе защищённости внутренней сети проводится:

- ♦ сканирование сетевых портов объектов тестирования;
- ♦ анализ сетевого взаимодействия;
- ♦ сбор данных о сетевых сервисах заказчика;

BIS-КОММЕНТАРИЙ

Второй момент связан с многообразием применяемого стека IT/OT, описать особенности которого в рамках одной методологии — задача не из лёгких. Можно представить, что в идеале это должна быть информационная система или веб-ресурс, в котором на лету конфигурируется методика для конкретного проекта в зависимости от архитектурной особенности и технологического стека.

Третий момент: не всегда при проведении пентеста возможно поэксплуатировать уязвимость, так как к ней может не быть опубликованного PoC (Proof of Concept), а также попытка эксплуатации имеет риск нарушения нормального функционирования объектов ИТ-инфраструктуры. Неслучайно в том же МЭК 63096 при тестировании на проникновение какого-либо технологического оборудования, влияющего на атомную безопасность, рекомендуют его проводить на стендовой инфраструктуре (макете), а на реальном оборудовании только во время проведения планово-предупредительных работ.

Четвёртое: любой тест на проникновение показывает результаты на текущий момент времени. В организации постоянно происходят изменения — добавление и/или обновление аппаратного и программного обеспечения. При этом сами банки данных угроз и уязвимостей, будь то БДУ ФСТЭК или NVD от NIST, постоянно обновляются новыми опубликованными уязвимостями, рекомендациями вендоров и сообщениями об опубликованных PoC. Все эти факторы заставляют нас проводить непрерывные пентесты (Continuous Penetration Testing) и периодические red team.

В текущей ситуации экспертному сообществу необходимо объединиться и через ассоциации и технические комитеты предложить регуляторам концепцию методологии, которая, в частности, классифицирует виды тестов на проникновения и опишет подходы, учитывающие различные объекты и сценарии тестирования.

- ♦ определение типов и версий сетевых сервисов и приложений;
- ♦ выявление уязвимостей с использованием универсальных сканеров защищённости;
- ♦ ручная проверка уязвимостей в обнаруженных сервисах заказчика;
- ♦ моделирование атак на уровне сетевых сервисов и приложений;
- ♦ использование обнаруженных уязвимостей, чтобы оценить возможности получения доступа к защищаемой информации и объектам тестирования.

В настоящее время для отечественных инструментов, позволяющих проводить данный тип анализа защищённости, методические документы и рекомендации отсутствуют.



Антон ОСТРОКОНСКИЙ
руководитель отдела пентеста,
Deiteriy Lab

На данный момент действительно отсутствует методика, по которой необходимо проводить пентест в соответствии с требованиями 187-ФЗ.

В статье рассмотрены различные международные стандарты, но хотелось бы обратить внимание на ещё один документ. У совета PCI SSC есть PCI DSS Pentest Guidance. Это хороший пример документа, который описывает «правила игры» и отвечает на следующие вопросы: «какой должен быть пентест?», «какие доступы и какую информацию необходимо предоставить пентестеру?», «что является целью пентеста?»

Это очень важный момент, который позволит исключить разногласия у клиентов и исполнителей. Так как на данный момент, когда требования к пентесту не сформированы, можно столкнуться с ситуацией, в которой клиент говорит: «Тестируйте систему, но доступ к ней мы не дадим».

Очевидно, что пентестеры достучаться до системы не смогут и будут вынуждены сформировать отчёт без уязвимостей и ценность такой работы будет нулевой. При этом сослаться на какой-либо нормативный документ и запросить адекватные доступы, как это происходит в случае с PCI DSS, у пентестеров возможности нет.

Именно поэтому в методике должны быть требования к информации, которую необходимо предоставить

Большинство отчётов инструментов ИБ по анализу защищённости разбиваются в практической части их применения — не доказано, что уязвимость действительно может быть проэксплуатирована.

Часть работ приходится проводить вручную в том же Metasploit или Empire ещё и потому, что после ухода с рынка ПО многих зарубежных вендоров, таких как Rapid 7, мы остались без инструментов полного цикла. Именно полного цикла для проведения тестов на проникновение.

Ещё хорошее новшество, которое мы могли бы перенять от зарубежных инструментов, — это предоставление в динамике общей сводной информации по отчётам от инструментов не только по CVE (база данных общеизвестных уязвимостей информационной безопасности), но

исполнителю. Например, если речь идёт о внешнем и внутреннем пентесте, то это совершенно точно должен быть перечень IP-адресов систем, которые входят в область аудита.

Методика также должна включать описание модели нарушителя, которую необходимо использовать при проведении пентеста.

Если в область аудита входят приложения, то нужно договориться о минимальных привилегиях учётной записи, которая будет предоставлена пентестеру. Ведь если в область аудита входит приложение со сложной бизнес-логикой, а клиент просит протестировать его только «чёрным ящиком», толку от такой работы будет немного.

Если речь идёт о внутреннем пентесте, то нужно указать, что необходимо предоставить пентестеру сетевой доступ во внутреннюю сеть, а также, например, учётную запись в Active Directory или на терминальном сервере с привилегиями обычного пользователя.

Кроме того, методика должна содержать верхнеуровневое описание шагов, которые необходимо выполнить пентестеру.

Например, необходимо провести сбор информации, выполнить сканирование на предмет открытых портов, определить сервисы, доступные на выявленных портах, и так далее.

Пентестер должен иметь свободу в выборе конкретных инструментов и способов выполнения шагов, предусмотренных методикой.

Более того, описать универсальную последовательность действий с командами и инструментами не получится для всего пентеста, так как каждый шаг зависит от множества факторов. Эту последовательность можно описать только для нескольких первых этапов, включающих разведку и сбор информации.

На последующих этапах техника пентеста будет зависеть от результатов первых этапов сбора информации: какой фреймворк используют разработчики, какие сервисы были найдены на внешнем периметре или

и детально по CWE (Перечень общих слабостей — это система категорий слабых мест и уязвимостей аппаратного и программного обеспечения). Сейчас многие отечественные инструменты ИБ содержат в себе выборку, в том числе из базы уязвимостей bdu.fstek.ru (ФСТЭК России).

Для примера, если взять систему AOSC DefectDojo (opensource продукт), то она содержит в себе возможность сбора и анализа соответствия информационной системы комплаенсу того же OWASP 4.1. Конечно, многие скажут: а зачем нам зарубежный стандарт, если у нас и так признано, что оценка соответствия по ОУД4 как часть работ для многих аккредитованных компаний проводится регулярно. А по факту — не отражает действительных угроз из-за статичности показателей самого процесса оценки. Вот если бы существовали

требования и методика, которая отражает показатели на том же bdu.fstek.ru (ФСТЭК России), и показатели менялись под реалии новых угроз в соответствии с трендом Top 10 РФ, а не Top 10 OWASP, то все специалисты вздохнули бы свободно.

Сейчас достаточно много компаний проводят тесты на проникновение в отраслях промышленности, и каждый из отчётов, включённых в общий аудиторский отчёт, по идее должен быть стандартизирован и структурирован. А этого не происходит по причине отсутствия единой методики проведения тестов на проникновение.

BIS-КОММЕНТАРИЙ

во внутренней корпоративной сети. Также стоит учесть, что технологии меняются быстро, постоянно появляются новые уязвимости и атаки. Поэтому настолько детализированную методику сделать невозможно, если не заниматься её постоянным обновлением.

В этом же разделе стоит подсветить информацию о включении адресов пентестеров в белые списки на системах WAF, IDS, IPS. Это важный момент, так как срок проведения пентеста ограничен и у специалистов по тестированию нет задачи действовать скрытно и сильно уменьшать рейтинги сканирования. Это неминуемо приводит к блокировкам, что мешает проведению тестирования на проникновение. При выявлении уязвимостей, обнаруженных с IP-адреса, добавленного в белые списки, рекомендуется перепроверить, возможна ли эксплуатация данной уязвимости с другого IP-адреса. Это необходимо для того, чтобы понять, могут ли средства защиты помочь закрыть данную уязвимость. Информацию об этом стоит добавить в отчёт о тестировании на проникновение.

Также методика должна содержать требования к квалификации пентестеров. О квалификации можно косвенно судить по опыту выполнения аналогичных проектов, наличию профильных сертификатов, признанных международным сообществом, лицензий, наличию публикаций и докладов на конференциях. Также стоит обратить внимание на участие в CTF и наличие зарегистрированных CVE.

Ещё один важный момент, который стоит описать в методике, — структура отчёта. Необходимо описать основные разделы, например:

- ♦ резюме — краткое описание проводимой работы и её результатов;
- ♦ описание области тестирования;
- ♦ описание методики;
- ♦ описание ограничений, с которыми могли столкнуться пентестеры, например, отсутствие сетевого доступа до целевой системы или неработающие методы API;

♦ описание выявленных уязвимостей и рекомендаций по их устранению;

♦ описание вектора атаки.

Авторы статьи указали и на проблемы, связанные с отсутствием инструментов полного цикла. Тут нужно отметить важный момент: сканирование уязвимостей и тестирование на проникновение очень сильно отличаются. Пентестеры редко используют коммерческие инструменты полного цикла. В основном они используют open-source-решения, инструменты, разработанные компаниями и собственные разработки. Поэтому данная проблема переоценена.

Что касается определения критичности выявленных уязвимостей, то данный момент тоже довольно сложно стандартизовать, так как критичность одной и той же уязвимости в разных информационных инфраструктурах может отличаться. Более того, она может быть разной в той же самой информационной инфраструктуре, но при проведении разных пентестов. Например, при проведении тестирования на проникновение в соответствии с требованиями PCI DSS самым критичным активом являются данные держателей карт. Соответственно, уязвимость, которая позволяет их получить, например XSS на платёжной странице, является критичной. В пентесте, не связанном с PCI DSS, критичность у такой уязвимости может быть ниже.

В заключительной части статьи авторы говорят о том, что необходимо разработать собственный OWASP TOP 10. Я не могу с этим согласиться, так как считаю, что не нужно отгораживаться от международного опыта. OWASP TOP 10 не имеет какой-либо привязки к локации и включает в себя самые популярные уязвимости, встречаемые в мире в целом. Но и у OWASP TOP 10 есть недостаток, связанный с тем, что он не учитывает специфику индустрии. Было бы полезно разработать подобные списки для разных сфер: финансовая сфера, энергетика, здравоохранение и так далее, согласно перечню отраслей КИИ.

ЛЕС И ЦИФРА

ОПЫТ ВНЕДРЕНИЯ SOC В ДЕРЕВООБРАБАТЫВАЮЩЕЙ ОТРАСЛИ



Максим КОРОЛЕВ
директор
по информационной
безопасности
Segezha Group

В IS Journal попросил директора по информационной безопасности Segezha Group рассказать, зачем, как и с каким результатом происходило подключение к удаленному SOC в одном из крупнейших в отечественной лесной промышленности холдинге.

ДИСПОЗИЦИЯ

Segezha Group — ведущий российский лесопромышленный холдинг с полным циклом собственной лесозаготовки, деревообработки и выпуска широкой линейки продукции, представленной на рынках более 80 стран мира. Особенность компании в ее географической распределенности — десятки предприятий и офисов разбросаны по всей стране от Карелии до Иркутской области. Больше 20 тыс. сотрудников в десяти регионах в разных часовых поясах. Но проблема не только в разнице во времени, а в том, что каждое предприятие холдинга — самостоятельная бизнес-единица. Активы присоединялись в разное время, у каждого из них свой уровень зрелости IT-инфраструктуры и, соответственно, информационной безопасности.

Сервисы в холдинге централизованы, поэтому каждое новое предприятие, в первую очередь, интегрируется в единую сеть, после чего начинается плановая модернизация всех систем и приведение их к единой политике. Риски очевидны: в активах компании есть как современные технологичные производства с хорошим оборудованием, так и далекие лесосеки с очень старыми уязвимыми системами. Часто отказаться от устаревших систем враз невозможно, но обеспечить их безопасность — необходимо.

В целом архитектура компании адаптирована к таким условиям. Работает распределенная сеть межсетевых экранов, размещенных на границах каждого подразделения. Централизованные сервисы развиваются давно, и уровень их защищенности как правило не вызывает больших опасений. Защита внешнего периметра тоже на уровне.

ПОЧЕМУ МЫ ВЫБРАЛИ ВНЕШНИЙ SOC

Итак, задача максимального закрытия рисков очевидна. У нас была своя SIEM-система для оперативного управления информацией о текущем состоянии безопасности и управления инцидентами. Но с учетом стоящих перед холдингом бизнес-задач она требовала срочной модернизации. Во-первых, её настройка находилась в зачаточном состоянии. Какие-то правила были предустановлены вендором, какие-то интегратором, что-то пытались настраивать наши предшественники. Это была огромная база данных, генерировавшая более 10 тыс. событий в сутки. Необходима была основательная настройка и общая оптимизация работы.

Решили обратиться к аутсорсерам. Мы сформулировали свои требования. Во-первых, это должен быть надежный SOC с полной поддержкой, так как нам не нужен вариант еще одной громоздкой системы, где постоянно приходится что-то доводить до ума. Соответственно, предполагается не только развертывание, но и дальнейшая поддержка и развитие. Во-вторых, необходима высокая скорость подключения, что взять все под контроль как можно быстрее. Третье требование — гибкие условия тарификации. Тут понятно: деньги нужно тратить с умом, поэтому чем более гибкие условия нам предложат, тем лучше. Четвёртое — дополнительная финансовая выгода. Экономия на штате специалистов и мощностях должна перенаправить освободившиеся ресурсы на развитие ИБ. Специалистов мало, а систем, требующих внимания и сопровождения с каждым годом всё больше. Необходимо высвободить как человеческие, так и вычислительные ресурсы.

И последнее. В холдинге есть объекты КИИ, к ним особое отношение, а взаимодействие с НКЦКИ жестко регламентировано и требует специфических навыков. То есть нам нужна была помощь в организации и упрощении такого взаимодействия.

Главными критериями при выборе поставщика сервисов SOC для нас было наличие успешного опыта защиты больших территориально распределенных инфраструктур, скорость подключения и экспертиза команды.

Я уже упоминал, что нам необходимо было выполнить требования законодательства и взаимодействие с регулятором, поэтому наличие необходимых сертификатов, лицензий, и, главное, опыта организации такого взаимодействия было тоже важно.

КАК МЫ ПОДКЛЮЧАЛИСЬ

Инженеры внешнего SOC оперативно проанализировали нашу инфраструктуру и подготовили схему развертывания. Поскольку проект масштабный, для нас было важно, чтобы участие наших сотрудников не стало узким местом, но подключение сервисов прошло очень быстро и безболезненно. По результатам анализа определились с количеством необходимых ресурсов внутри периметра. Ресурсов требовалось меньше, чем для работы имеющейся системы, поэтому уже на этом этапе мы достигли части планируемых результатов.

Первым делом было принято решение подключать журналы безопасности с рабочих станций и серверов. Настроили политики перенаправления журналов, серверы сбора журналов, нормализации и по защищенному каналу отправили весь этот поток данных в SOC.

Но самое интересное было дальше.

ЧТО МЫ ПОЛУЧИЛИ СРАЗУ

Итак, что мы получили сразу после подключения к внешнему SOC? Инциденты. Не десятки тысяч неструктурированных данных, а настоящие инциденты, обработанные и подготовленные к реагированию. Правила корреляции событий позволяли объединять данные из разных источников в цельную картину. В этих инцидентах содержалась исчерпывающая информация и о задействованных хостах, и пользователей, и потенциальных рисках, и рекомендации по дальнейшим действиям.

Что касается выявления вредоносной активности, то после подключения к SOC мы стали более быстро понимать, что происходит

в нашей инфраструктуре — все проблемы предстали как на ладони.

С внешним периметром немного другая история. Как я уже говорил, на границах стоят межсетевые экраны, публикация централизованных сервисов в Интернет осуществляется через них. Но, во-первых, благодаря анализу и корреляции событий, мы смогли более точно настраивать защиту внешнего периметра. А во-вторых, мы одновременно охватили картину по другим предприятиям, у которых были собственные каналы в Интернет. И наконец-то появилась возможность эффективно закрывать слепые зоны.

Здесь хотелось бы объединить пару пунктов — помощь в расследовании и ретроспективный анализ. Что было особенно важно, мы могли запрашивать дополнительную информацию у дежурного инженера, если нам не хватало каких-то данных для принятия решения по дальнейшим шагам. Тикеты закрываются вручную после подтверждения с нашей стороны. Вся история хранится в SOC, и, если появлялся похожий или связанный инцидент, нас об этом информировали. Плюс часто в рамках расследований нам требовалось получить какие-либо данные для обогащения инцидентов, и эту потребность также закрывал SOC. То есть мы получили действующую систему управления инцидентами. Про круглосуточный режим работы, учитывающий нашу географию, думаю, говорить нет смысла. Это само собой.

Отдельно отмечу отчеты и регулярные рассылки, в том числе от НКЦКИ и ФСТЭК. По новым уязвимостям получаем дополнительную информацию от коллег — они оперативно подсвечивают критичные моменты. Ну и последнее в списке, но не по значимости, — передача информации в координационный центр. Нас так же успешно подключили к ГосСОПКА, теперь нам не надо переживать о соблюдении всех требований регулятора.

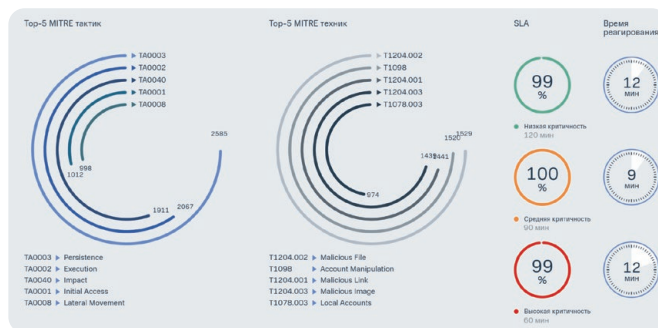
КАК МЫ РАЗВИЛИ СЕРВИС ЗА ПЕРВЫЙ ГОД

Что было дальше? Подключение к SOC дало свои результаты, и нам захотелось большего. На основе анализа инцидентов коллеги предлагали свои варианты кастомизации правил таким образом, чтобы установка была максимально адаптирована к нашим условиям. Например, интерактивный вход под локальной учетной записью, добавление пользователей в критичные

SEGEZHA GROUP

А оно «вам» надо?

Инцидентов в сутки



50%

зарегистрированных
инцидентов имеют высокий
уровень критичности

~14 мин.

Средняя скорость
информирования
с соблюдением SLA

Рисунок 1. Какими ресурсами должно обладать ИБ-подразделение компании, чтобы справиться с таким количеством работы?

группы active directory, «срок действия пароля не ограничен», информирование о состоянии жесткого диска и т.д. Трудно было не согласиться. Теперь отслеживание инцидентов помогает более эффективно упреждать возможное негативное развитие событий — мы отсекаем риски на более раннем этапе и не позволяем им развиваться до критического уровня.

Мы постоянно внедряем в компании новые системы ИБ, одной из них стала система анализа трафика и обнаружения атак. Тестирование показало её полезность, поэтому данные с неё было необходимо тоже включить в обработку. Так, шаг за шагом, мы обогащали нашу инсталляцию новыми источниками и делали её всё более эффективной.

Отдельная большая работа была проделана в части интеграции с нашей SOAR системой R-Vision. Внешний SOC предоставляет нам личный кабинет, в котором можно управлять инцидентами, но у нас уже существовала собственная локальная система управления инцидентами. В неё были заведены наши активы, сотрудники по ИБ, были прописаны плейбуки для некоторых типов инцидентов. И обрабатывать инциденты нам хотелось именно в ней. Были некоторые технические ограничения со стороны R-Vision, поэтому интеграцию пришлось придумывать

совместно с коллегами из SOC. Выбрали вариант почтовой интеграции с тэгируемыми ключевыми полями. Добавлю, что эта работа не останавливается и по сей день — всегда есть куда расти, мы продолжаем развивать и расширять интеграцию.

Кроме того, большая работа была проделана в части фильтрации поступающих событий. Данных должно быть необходимое и достаточное количество, чтобы не перегружать ресурсы и каналы и в то же время не рисковать потерей важных событий. Тут я снова хочу отметить экспертизу инженеров SOC, совместно с которыми настраивались все подписки. Без их опыта это был бы либо огромный поток данных (как с нашей собственной SIEM), либо бесполезный поток.

ПОДВЕДЕНИЕ ИТОГОВ

Правильно ли мы сделали, когда отказались от идеи развития собственных систем и обратились к сервисам внешнего SOC? На слайде всё очевидно (рис. 1). Чтобы эффективно обрабатывать такой поток событий, необходимо большое количество ресурсов. И речь даже не столько о вычислительных ресурсах, это решаемый вопрос, сколько о человеческих. Чтобы настроить, поддерживать и развивать собственную систему

SEGEZHA GROUP

Что сейчас?

Интеграция систем обеспечения ИБ АСУ ТП (в первую очередь КИИ) в процесс управления инцидентами

Подключение к SOC приобретаемых активов

Подключение к SOC дополнительных источников (Linux, логи с оборудования и т.д.)

Постоянная разработка новых правил корреляции

Постоянная доработка плейбуков IRP (разбивка на подтипы, подключение новых СЗИ к IRP, усложнение логики)



7000+

рабочих станций
сотрудников и серверов

Рисунок 2. Удаленный SOC меньше чем за год стал неотъемлемой частью ИБ холдинга Segezha Group

требуется много специалистов. Найти и удержать их весьма проблематично. В нашем случае наиболее оптимальным и эффективным решением стало подключение к внешнему SOC.

Кроме того, в истории нашего взаимодействия с SOC уже существует целый ряд критичных инцидентов, риск развития которых мог бы стать катастрофическим. После каждого из них мы понимаем, что сделали правильный выбор. Какие это были инциденты? Например, детектирование сигнатуры ETHERNALBLUE с компьютера администратора, работающего через VPN. Максимальный приоритет инциденту, оповещение от дежурного, сбор данных о затронутых хостах — и угроза остановлена. Появление в сети недоменных устройств и детектирование вирусной активности с них. Так была обнаружена нелегитимно установленная wifi-точка на отдаленном предприятии, через которую сотрудники сидели с личных устройств в интернете. Кроме того, у нас в компании на регулярной основе проводятся пентесты, по результатам которых SOC не пропускает ни одного критичного инцидента.

ЧТО СЕЙЧАС?

Как я говорил вначале, для нас было критически важно не получить мертвым грузом

неподдерживаемую статичную систему. Поэтому развитие взаимодействия с SOC успешно продолжается. Холдинг не стоит на месте, а вместе с ней развивается и ИБ. Тот факт, что при приобретении новых активов в первую очередь ставится задача на подключение новых источников к SOC, по-моему, говорит сам за себя. Нам стало гораздо проще и безопаснее интегрировать неизвестную инфраструктуру в корпоративную сеть и оперативно закрывать уязвимые места. Обычно такая работа предполагает долгий подготовительный этап изучения, сканирования, подготовки и длительного ограничения функциональности. С внешним SOC этот процесс ускорился в разы.

Я уже упоминал про постоянную работу над правилами корреляции, развитием интеграции и подключением новых систем как источников данных. Эта работа не останавливается, при внедрении новых систем одна из первоочередных задач — подключение их к SOC. К этому добавляются новые задачи по настройке и интеграции со специализированными системами безопасности АСУ ТП. В связи с определенными трудностями в приобретении современного телекоммуникационного оборудования, добавляются задачи по получению данных со всё более широкого спектра устройств (рис.2).

ПРИМЕР ДВУСТОРОННЕГО ДВИЖЕНИЯ

КАК ИДЁТ ЦИФРОВИЗАЦИЯ НА ОСНОВЕ ОТКРЫТЫХ ФИНАНСОВ



Юрий КАРДЮКОВ

руководитель направления Identity и Open API, компания eKassir



Алексей ШАРНЕНКОВ

руководитель направления Центра компетенций интеграционных решений, МКБ

В ноябре 2022 года Банк России опубликовал объёмный стратегический документ, посвящённый развёртыванию на российском финансовом рынке технологии передачи данных на основе открытых программных интерфейсов. Сейчас Концепция внедрения Открытых API носит рекомендательный характер, но со временем их использование может стать обязательным. Это запустит последовательный переход рынка к модели Открытых финансов (Open Finance).

В рамках этой модели между собой взаимодействуют участники рынка (банки, страховые и инвестиционные компании, МФО и проч.), а также поставщики и рядовые потребители финансовых услуг. Информационный обмен между ними осуществляется при помощи универсального языка, которым являются Открытые API (Open API).

Внедрение стандартизированных программных интерфейсов создаёт преимущества для всех участников этого обмена.

Преимущества банков:

- ♦ точка входа на новые площадки для продаж;
- ♦ гарантированная безопасная и надёжная передача данных;

- ♦ повышение лояльности клиентов.

Преимущества для финтехтов:

- ♦ доступ к банковским данным клиентов;
- ♦ сокращение времени вывода продукта на рынок;

- ♦ отсутствие необходимости настраивать сервисы под каждого партнёра.

Преимущества для пользователей:

- ♦ доступ к новым сервисам и предложениям;
- ♦ прозрачное управление персональными финансовыми продуктами;
- ♦ возможность управлять согласием на доступ к своим данным;
- ♦ высокий уровень защиты информационного обмена между участниками.

Основными выгодоприобретателями от перехода участников рынка финансовых услуг к модели передачи данных на основе Открытых API станут рядовые пользователи (рис. 1).

Демонстрация доступа к информации о счетах и продуктах банковских клиентов развязывает руки поставщикам услуг и финтехам, позволяя им предлагать более смелые пользовательские приложения.

Выбор клиента более не ограничен одним-двумя решениями: в парадигме обслуживания Open Finance он получает новые



Рисунок 1. Преимущества цифровизации на основе модели Открытых финансов

возможности для управления персональными продуктами, альтернативные платёжные методы, широкий список адресатов денежных переводов и сопутствующие финансовые опции (например, приложения для ведения бюджета, повышения финансовой грамотности и т.п.).

УПРАВЛЕНИЕ ПЕРСОНАЛЬНЫМИ ФИНАНСОВЫМИ ДАННЫМИ — ПРАВО САМОГО ПОЛЬЗОВАТЕЛЯ

Другая проблема, которую решают Открытые API, связана с правом пользователя на его личные данные, точнее — с отсутствием подобного права в современной парадигме финансового обслуживания.

Рассмотрим стандартную ситуацию: покупатель приобретает товар через приложение маркетплейса и хочет получить кешбэк за транзакцию. Поскольку финансовое сообщение, составляющее суть платёжной операции, содержит данные покупателя о счёте, его личные реквизиты и т.п., логично предположить, что он ими владеет. Тем не менее это не так — поделиться информацией с кешбэк-сервисом он не может.

Так происходит потому, что в классической модели обслуживания пользователь, формально являясь владельцем счёта, фактически не может самостоятельно предоставить доступ к нему стороннему поставщику финансовых сервисов. Ему позволено взаимодействовать со счётом только из приложения

банка — то есть именно банку принадлежит абсолютное право распоряжаться ресурсами пользователя.

Модель обслуживания, опирающаяся на Открытые API, делегирует это право пользователю, который может напрямую через приложение стороннего поставщика услуг передать тому данные о счёте и согласие на их хранение и обработку.

Возрастает безопасность транзакций. Благодаря строгим стандартам API сторонние поставщики финансовых услуг получают доступ к пользовательским ресурсам непосредственно от первоисточника. Контроль регулятора за единообразием взаимодействия внутри доверенной среды гарантирует, что информационный обмен между её участниками надёжно защищён от компрометации, более вероятной при использовании различных частных API.

Защита интересов полноценного участника информационного обмена, которым является потребитель финансовых услуг, — одна из ключевых целей, которую преследует Банк России, стимулируя рынок к переходу на использование Открытых API.

Движение к новой модели финансового обслуживания отчасти напоминает сценарий внедрения на российский рынок сотовой связи MNP-технологии (Mobile Number Portability), позволяющей абонентам переходить к другому оператору с сохранением телефонного номера. Реализация этой меры не была простой и заняла немало времени,

Долгий путь к Открытым финансам

1) Самостоятельное изучение Стандарта безопасности ФАПИ.СЕК («СТО БР ФАПИ. СЕК-1.6–2020. Безопасность финансовых (банковских) операций. Прикладные программные интерфейсы обеспечения безопасности финансовых сервисов на основе протокола OpenID. Требования»), а также прикладных стандартов Банка России по Открытым API

2) Самостоятельная реализация поддержки Стандарта безопасности СТО БР ФАПИ. СЕК-1.6–2020

3) Самостоятельная реализация функций сервера авторизации и шифрования/дешифрования, а также поддержки прикладных стандартов Банка России по Открытым API: «Инициирование перевода денежных средств клиента третьей стороной в валюте Российской Федерации» и «Получение информации о счёте клиента третьей стороной».

4) Подать заявку оператору доверенной среды Открытых API (Ассоциация ФинТех)

5) Успешно отработать позитивные/негативные сценарии на сертификационном стенде Открытых API

Короткий путь к Открытым финансам

1) Интеграция готового «коробочного» решения для подключения к Открытым API в процессинг банка-заказчика

2) Подать заявку оператору доверенной среды Открытых API (Ассоциация ФинТех)

3) Успешно отработать позитивные/негативные сценарии на сертификационном стенде Открытых API

Таблица 1. Два пути подключения к доверенной среде Открытых API

однако её итогом стала фактическая отмена «мобильного рабства», — и за десять лет более 24 млн пользователей воспользовались услугой МНР¹.

Рынок финансовых услуг столкнулся с подобным сценарием во время подключения банков к Системе быстрых платежей. Преимущества СБП на первых порах также были неочевидны — как для пользователей, так и для поставщиков платёжных услуг. И всё же по итогам 2023 года участниками системы являются более двухсот банков, а более 1 млн предприятий принимают оплату по СБП, которой за год хотя бы раз воспользовался каждый третий житель России².

Открытые API — общемировой тренд, развитие которого в нашей стране направляет финансовый регулятор (Банк России). Сейчас в России наступило время пилотных проектов с применением Открытых API — первые из них уже внедрены и монетизируются рядом банков и финтех-организаций, задающих вектор направления всей отрасли.

В ноябре 2023 года Ассоциация ФинТех опубликовала плейбук «Открытые

API» — практическое пособие, в котором рассказывается о пилотируемых в России бизнес-кейсах, где успешно используется технология открытых программных интерфейсов³.

ДВА ПУТИ К ОТКРЫТЫМ ФИНАНСАМ

Длительный процесс перехода банков и финансовых организаций к Open Finance начнётся с выполнения обязательств по подключению к доверенной среде Открытых API⁴. Существует два пути его реализации — долгий и короткий. Рассмотрим пошаговое движение по обоим (таб. 1).

Если банк или финансовая организация решили подключиться к среде регуляторных API по короткому пути, они могут обратиться к поставщику программного обеспечения с готовым «коробочным» решением. Такое ПО будет обладать рядом преимуществ перед внутренней разработкой:

³ В числе реализованных проектов рассмотрены сервис «Без бумаг», осуществляющий получение выписки для скоринга при онлайн-кредитовании юрлица (банки «Точка» и «Промсвязьбанк»), агрегатор информации по счетам и картам клиентов, платформа «Цифровая ипотека», проект интеграции микрофинансовых организаций с Финуслугами Московской биржи и проч.

⁴ <https://bosfera.ru/bo/vse-dumali-api-zima-eto-ottepel>

¹ <https://www.rbc.ru/newspaper/2022/12/28/63ab03e99a794751b4182367>

² https://www.cbr.ru/analytics/nps/sbp/3_2023/

♦ Банк сэкономит немало времени, не затрачивая его на изучение объёмной документации финансового регулятора;

♦ Не придётся отрывать собственных работников от решения бизнес-задач;

♦ Поставщик ПО возьмёт на себя все сложности по реализации обязательных стандартов безопасности и прикладных стандартов Открытых API;

♦ По завершении проекта поставщик ПО предоставит техническую поддержку и исчерпывающую документацию по интеграционному API.

Разработчик программного обеспечения, направленного на интеграцию инфраструктуры финансовой организации в среду Открытых API Банка России, должен учитывать два важных момента. ПО должно не только поддерживать существующие регуляторные стандарты, но и иметь возможность адаптироваться к будущим наборам требований. Если в наборе регуляторных Открытых API появляется новый программный интерфейс, разработчик может подключить его по прикладному протоколу.

Кроме того, в состав программного решения должен входить инструмент для создания и хранения ресурсов согласия пользователя. Это чрезвычайно важно: именно открытое согласие является краеугольным камнем Open Finance. Оно даёт пользователю право управлять своими бизнес-данными и предоставлять сторонним поставщикам финансовых услуг доступ к ним.

На праве пользователя предоставлять и отзывать явное согласие на доступ к своим ресурсам построено информационное сообщение «в духе» Открытых API.

Если банк хочет взаимодействовать с партнёрами посредством собственных API и при этом обеспечить эффективность и безопасность обмена информацией, он может использовать готовое ПО, используемое для подключения к регуляторной среде. Тем самым лучшие практики применения регуляторных стандартов Открытых API будут адаптированы финансовыми организациями для клиентского обслуживания в рамках обычного бизнес-взаимодействия.

«КОРОБОЧНОЕ» ПО В ПРОЕКТАХ С РЕГУЛЯТОРНЫМИ API

В 2022 году Московский кредитный банк стал полноценным участником среды Открытых программных интерфейсов Банка России в роли поставщика платёжных услуг для сценария «Получение информации о счёте клиента третьей стороной».

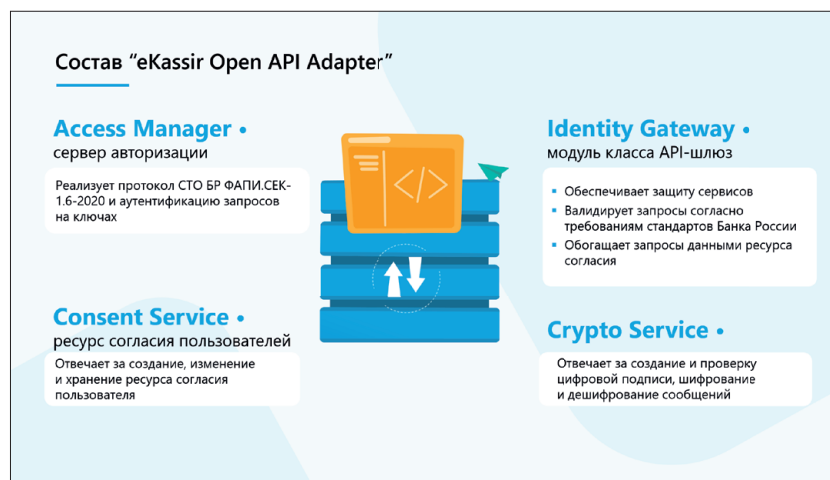


Рисунок 2. Состав решения eKassir Open API Adapter

МКБ получил опыт работы со стандартом безопасности СТО БР ФАПИ. СЕК-1.6-2020 и всего за несколько месяцев прошёл путь от внедрения eKassir Open API Adapter до успешного завершения сертификационных испытаний⁵.

Для успешного прохождения сертификационного тестирования и программное обеспечение, и бэкенд банка прошли отладку на стенде «Песочница»⁶, где проверяются конфигурации и настройки криптографии. Стандарт Банка России предполагает применение OIDC для аутентификации, формата передачи утверждений JSON Web Token и криптографического протокола mTLS, отвечающего за взаимную аутентификацию клиента и сервера на основе сертификатов (с использованием PKI).

Кейс Московского кредитного банка — пример проекта, реализованного в полном соответствии с регуляторными обязательствами, предваряющими развитие концепции Open Finance в России. Но как было сказано выше, практику использования готового ПО для интеграции со средой строго регламентированных Открытых API можно распространить и на частные задачи финансовых организаций, желающих расширить портфолио пользовательских услуг за счёт сервисов своих партнёров.

«КОРОБОЧНОЕ» ПО В ПРОЕКТАХ С НЕРЕГУЛЯТОРНЫМИ API

Если организация заинтересована в развитии собственных прикладных программных интерфейсов в соответствии с проверенными

⁵ <https://bosfera.ru/bo/kak-mkb-k-open-api-podklyuchalsya>.

⁶ Песочница — инструмент «Сертификационного стенда Открытых API», с помощью которого ПО проверяется на соответствие стандартам Банка России, включая криптографию.



Рисунок 3. Бизнес-кейс: применение технологии Открытых API для предоставления банковских услуг в мобильном приложении сотового оператора

стандартами регуляторных API, она может использовать «коробочное» программное обеспечение. Для интеграции с подобным ПО нет ограничений, однако необходимо учитывать функциональность модулей, входящих в его состав. Рассмотрим некоторые на примере решения eKassir Open API Adapter (рис. 2).

Важнейший из них — Consent Service — отвечает за создание, хранение и централизованное использование ресурсов согласия пользователя. Поскольку частные API подключаются через этот сервис, клиент финансовой организации может быть уверен, что доступ к его данным производится исключительно с явного и подтвержденного согласия.

Компоненты Identity Gateway и Access Manager отвечают за защиту информационного обмена между его участниками и сервисов, которыми они пользуются. Оба компонента входят в состав комплекса eKassir Identity Platform (внесен в Единый реестр российского программного обеспечения — запись № 13332 от 26.04.2022)⁷.

Identity Gateway выполняет функции шлюза, reverse-proxy, отделяющего внешнюю и локальную сеть, в которой происходит взаимодействие банка и стороннего поставщика. Identity Gateway обогащает API доступа к счёту пользователя информацией о ресурсе согласия, выполняет привязку транспортного сертификата к токenu доступа и проверяет цифровую подпись API-запроса.

Access Manager управляет централизованной многофакторной аутентификацией и реализует Стандарт СТО БР ФАПИ.СЕК-1.6–2020.

Описанные возможности заинтересовали один из банков СНГ, который захотел

использовать программное обеспечение eKassir Open API Adapter в частном проекте, поддерживающем развитие финансового обслуживания по модели Открытых API. Выбор нашего решения был обусловлен его применением на российском рынке, высокими темпами развития государственной стратегии внедрения открытого банкинга и общим уровнем цифровизации банковского сектора в России (в топ-10 по версии международного консалтингового агентства Deloitte)⁸.

Согласно дизайну проекта, проприетарный набор прикладных интерфейсов банка предоставляется одному из крупнейших местных операторов мобильной связи. Пользовательские данные передаются на основании явного согласия и предоставляют клиентам банка возможность открывать новые счета и управлять ими, заказывать изготовление платёжных карт и оформлять банковские продукты в мобильном приложении сотового оператора (рис. 3).

Обращение к бизнес-данным пользователей происходит с их явного согласия, а безопасность передачи сообщений осуществляется по тому же набору требований, что и в Стандарте СТО БР ФАПИ.СЕК-1.6–2020.

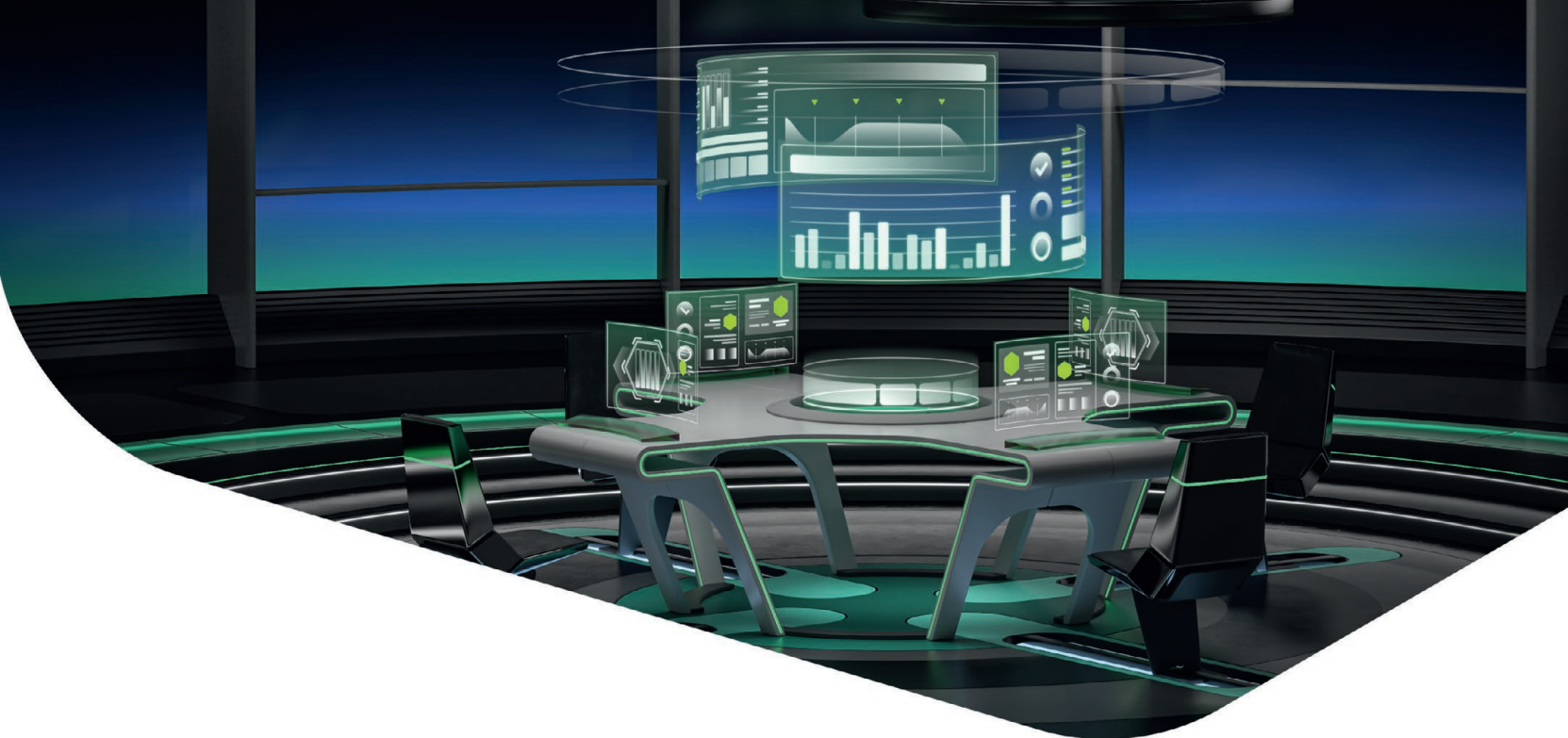
Таким образом, при помощи «коробочного» ПО создаётся частный контур взаимодействия, внутри которого участники обмениваются финансовой информацией по модели, реализуемой за счёт соблюдения требований к среде регуляторных API, но без внешнего контроля.

Пример подобного проекта характеризует зарождающийся у банков оптимизм в отношении Open Finance. Скоординированное вовлечение в развитие этой модели участников финансового рынка способно расширить их доступ к технологическим ресурсам и новым методам организации безопасного обмена данными.

Двустороннее движение к широкому применению Открытых API — то есть сочетание стимулирующих инициатив регулятора и самостоятельный практический опыт банков, финтехов и поставщиков услуг — способствует скорейшему повышению финансовой доступности и качества персонализации взаимодействия с клиентом.

⁷ <https://reestr.digital.gov.ru/reestr/696338/>

⁸ <https://frankmedia.ru/25912>



Kaspersky Anti Targeted Attack

Специализированная защита от целевых кибератак

- Защита основных точек входа потенциальной атаки
- Повышение эффективности процесса реагирования на инциденты
- Целостная картина происходящего в инфраструктуре
- Сбор, хранение и предоставление информации об инцидентах для соответствия требованиям законодательства
- Вместе с Kaspersky EDR составляет решение класса Extended Detection and Response (XDR)

kaspersky АКТИВИРУЙ
БУДУЩЕЕ

kaspersky.ru/enterprise

ДиалОгНаука

СИСТЕМНАЯ ИНТЕГРАЦИЯ В ОБЛАСТИ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

dialognauka.ru

ЗАПУСКАЕМ УМНУЮ АНТИФРОД-СИСТЕМУ

ОПЫТ АО «СВОЙ БАНК»



Ольга ГОРЮКОВА
директор департамента
управления рисками —
член правления,
АО «Свой Банк»

Вопрос настройки и запуска эффективной работы по антифрод-направлению является актуальным для большинства, если не всех действующих кредитных организаций. Банки, выстраивая ежедневное взаимодействие с клиентами через диджитал-каналы, должны уметь оперативно оценить и удостовериться по каждой транзакции (особенно в момент до её подтверждения и проведения), кто в действительности в этот момент находится на «той стороне» и отдаёт распоряжение банку в осуществлении операции по счёту — клиент или мошенник.

Если топ-менеджмент серьёзно задумывается о развитии банковского бизнеса в розничном сегменте, запуске в онлайн новых видов банковских продуктов и услуг для физических лиц, ему крайне важно заранее максимально обезопасить банк от фродовых кейсов и самостоятельно научиться управлять этим риском. Интуитивная настройка антифрода через «ручное» («полуручное») рассмотрение потенциально мошеннических операций без применения технологий и «умных» антифрод-систем — это трудоёмко, сложно и, как показывает практика, недостаточно эффективно. Очевидно, что при её реализации последствия могут быть катастрофическими как для самого банка, так и для его клиентов, учитывая открытую статистику рынка о ежегодном приросте объёмов списаний со счетов клиентов усилиями мошенников.

Сейчас к вопросам борьбы с мошенничеством активно подключается и регулятор. Банком России сформирована нормативно-правовая база и стандарты по ряду направлений в области противодействия мошенничеству. Создание Банком России

ФинЦЕРТа — системы информационного обмена между банками и другими участниками финансового рынка, правоохранительными органами, провайдерами и операторами связи, системными интеграторами, разработчиками антивирусного программного обеспечения и другими компаниями, работающими в сфере информационной безопасности, обеспечивает банки актуальной информацией о выявленных на рынке угрозах, в том числе о мошенничестве, и совершённых атаках. Поэтому банку как минимум нужно включиться в информационный обмен с ФинЦЕРТом. Однако использование только этого инструмента для мониторинга и борьбы с фродом недостаточно.

Почему же банку важно комплексно подходить к запуску процедур фрод-мониторинга и выстраивать умную систему транзакционного антифрода (УСТАФ), в основе которой лежат технологии:

- ♦ *гарантии надёжности для клиентов.*

Противодействуя мошенникам, банк может гарантировать своим действующим и новым клиентам качество проводимых расчётов, а именно их надёжность и безопасность;

- ♦ *минимизация фродовых потерь самого банка.*

Банк будет способен минимизировать потенциальные фродовые потери по проводимым транзакциям и тем самым достигать ключевых стратегических показателей деятельности и текущего бизнес-плана;

- ♦ *реагирование на фродовые «инновации и новые тренды».*

Методы, к которым прибегают мошенники, с каждым разом становятся всё изощреннее и сложнее. Систему транзакционного антифрода банку следует развивать, чтобы уметь противостоять любой фродовой логике, а также излюбленной ими методам социальной инженерии и др.;

- ♦ *возможность настройки собственных антифрод-правил и управление ими.*

В основе УСТАФ лежат риск-правила/триггеры, указывающие на признаки фрода по транзакции. При срабатывании преднастроенных антифрод-правил операции должны приостанавливаться, инциденты — разбираться до подтверждения отсутствия признаков мошенничества. Состав правил может быть общим,

а может калиброваться относительно различных клиентских профилей и участников расчётов, объёмов транзакций, геолокации и выbranного времени для перевода и т.д.

С ЧЕГО НАЧАЛИ МЫ

«Свой Банк» является молодым представителем известного и зарекомендовавшего себя на рынке финтех-холдинга IDF Eurasia. Сейчас банк переживает новую историческую веху своего развития и трансформации традиционной бизнес-модели в современный технологичный цифровой банк, обеспечивающий предоставление своим клиентам весь спектр банковских продуктов и услуг в диджитал-канале. В числе ключевых стратегических целей, стоящих перед командой топ-менеджмента, активное развитие розничного бизнеса. Поэтому задача по определению контуров УСТАФ и запуску антифрод-системы согласно задуманной дорожной карте является для банка жизненно важной.

Наша рабочая «дорожная» карта включает описание конкретных этапов построения УСТАФ и их временные границы с конкретными сроками реализации. Вместе с ней при построении антифрод-системы банку также важно было:

- ◆ определить ответственного топ-менеджера и/или внутреннее подразделение, в чьей зоне ответственности будут вопросы УСТАФ;
- ◆ силами собственной команды или привлечённых независимых экспертов провести ревью (обследование) действующей системы мониторинга противодействия мошенничеству, а также проанализировать лучшие практики рынка в отношении организации УСТАФ;
- ◆ подготовить подробные бизнес-требования по развитию антифрод-технологий, условия альтернативного выбора между тем, будет это собственное ИТ-решение или некий «коробочный» или кастомизированный продукт УСТАФ от стороннего вендора;
- ◆ оценить возможность использования внешних антифрод-правил, в том числе предлагаемых рынком, например внешним процессингом (при осуществлении расчётов с участием внешнего процессинга), преднастроенных правил в системах, предлагаемых поставщиками или независимыми консультантами;
- ◆ разработать собственные базовые антифрод-правила для различных типов клиентов и участников расчётов, а также понять все возможные варианты по действиям банка при их срабатывании;
- ◆ определить состав оценочных параметров (показателей) успешности в отношении УСТАФ и др.

По понятным причинам нам не пришлось долго объяснять руководству банка в отношении необходимости реализации дорожной карты и включении инвестиций в бизнес-план банка для развития действующей системы антифрода.

КТО НЕСЁТ ОТВЕТСТВЕННОСТЬ?

На начальном этапе необходимо определить внутреннее подразделение, в чьей зоне ответственности будет дальнейшее развитие УСТАФ. Если обобщить сложившуюся банковскую практику, то полномочия в направлении антифрода в структуре банков относятся к деятельности (ниже приводим альтернативные варианты, действующие на рынке) следующих структур.

◆ **Службы безопасности (СБ).** С одной стороны, это логично, ведь основной задачей подразделения как раз является выявление и работа с фродом. Сотрудники СБ глубоко знают, по каким признакам можно идентифицировать мошенников и какие источники данных для этого можно использовать. С другой стороны, не секрет, что СБ не всегда фокусируются (в силу специфики основной деятельности) на разработке риск-правил и аналитики транзакционной активности клиентов.

◆ **Подразделения по информационной безопасности.** Часто в банках антифродом занимается именно это подразделение, которое понимает «природу» фродовой транзакции и может компетентно среагировать на возникший инцидент.

◆ **Службы управления рисками (СУР),** которая может оперативно разработать основные риск-правила на базе лучших рыночных практик и требований законодательства, нормативно-правовых актов Банка России, рекомендаций платёжной системы и других участников платёжной системы. Антифрод может включаться в качестве одного из подвидов операционного риска, управление которым также, как правило, входит в функциональные обязанности СУР.

◆ **Подразделение розничного бизнеса,** что видится не самым удачным решением, так как здесь может возникать прямой конфликт интересов, учитывая, что основной целью бизнеса выступает привлечение клиентской базы и выполнение бизнес-показателей по наращиванию объёмов предоставленных клиентам продуктов и услуг.

◆ **Специально сформированного подразделения** в оргструктуре банка (антифрод-центра, подразделения по противодействию транзакционному мошенничеству и т.д.),

Вариант по внедрению технологии	Собственная разработка	Промышленное антифрод-решение (ПО/система) от внешнего поставщика	
		«Коробочная» система	Кастомизированная система
Общие параметры технологии			
Суть технологии	Разработка системы осуществляется «с нуля». Для этого выделяются ресурсы ИТ-подразделения банка (бизнес-аналитики, а также ИТ-специалисты, имеющие необходимые навыки в разработке)	Готовое решение от вендора – российского разработчика (ИТ-компании), которое предлагается к поставке участникам банковского рынка. Как правило, с ограниченной функциональностью и базовым набором преднастроенных антифрод-правил	В основе системы, как правило, лежит готовый «коробочный» продукт с базовыми настройками по функциональности и необходимым интеграциям. Для расширения её функциональности поставщик по заказу банка осуществляет значительную доработку / дополнительную разработку. В результате полученное решение максимально учитывает потребности заказчика (по функциональности, составу преднастроенных риск-правил, особенностям ИТ-инфраструктуры, источникам данных, требуемым интеграциям и проч.)
«Плюсы» технологии	Вся разработка ведётся силами специалистов банка, которые глубоко понимают механизмы функционирования и настройки системы Дальнейшее сопровождение и доработка системы также реализуются на стороне банка Обеспечивается высокое качество разработки и тестирования системы	Подтверждённая скорость внедрения Банк получает работающую антифрод-систему под ключ и обучающий курс по работе с системой Расходы по системе будут ниже, чем если бы это была собственная разработка или «кастомизированный» продукт	Банк получает работающую антифрод-систему под ключ и подробный обучающий курс по работе с системой и её доработкой У банка появляется возможность проводить самостоятельную доработку, в том числе риск-правил и рабочих интерфейсов без дальнейшего привлечения поставщика Все доработки системы сосредоточены в руках бизнес-аналитиков и риск-технологов с минимальным привлечением ИТ-специалистов банка, что позволяет обеспечивать высокую скорость изменений
«Минусы» технологии	Неподтверждённая скорость внедрения системы Потребуется значительные инвестиции во внутренние ресурсы (если потребуется наём дополнительных специалистов в ИТ-подразделение на разработку и сопровождение) Длительное ожидание выделения внутренних ресурсов разработки. У банка не всегда есть возможность выделить оперативно специалистов ИТ-подразделения на новые задачи длительного цикла Все доработки системы сосредоточены в руках ИТ-команды и не могут быть переданы, например, риск-технологам Любая собственная разработка несёт отложенные риски, так как в случае смены ИТ-команды (разработчиков) банк может остаться без дальнейшего сопровождения и развития данной системы (это может привести к тому, что в итоге банк будет вынужден искать замену данному решению)	Потребуется значительные инвестиции Поставщик, как правило, не поддерживает обновление и не предлагает услуги по доработке «коробки» под дополнительные задачи банка	Потребуется значительные инвестиции. Помимо расходов по внедрению, у банка могут возникать регулярные расходы по сопровождению системы, а также по использованию лицензии на полученное ПО Не всегда подтверждённая скорость внедрения системы Реальные сроки внедрения системы могут удлиняться и отличаться от сроков, определённых поставщиком до старта проекта (из-за дополнения скоупа проекта новыми неучтёнными доработками)

Вариант по внедрению технологии	Собственная разработка	Промышленное антифрод-решение (ПО/система) от внешнего поставщика	
		«Коробочная» система	Кастомизированная система
Оценочные параметры технологии			
Обеспечение полной функциональности системы	Да	Нет (только базовая функциональность)	Да
Возможность настройки в системе неограниченного количества риск-правил	Да	Нет (состав правил всегда ограничен возможностями ПО)	Да
Возможность развития аналитической работы с данными и разработки управленческой отчётности по данным антифрод-системы	Да	Да (минимальный состав данных, получаемый на основе настроек базовой функциональности)	Да
Наличие в системе рабочих интерфейсов для команды аналитиков антифрод-центра банка	Да (любой набор интерфейсов)	Да (базовый набор интерфейсов)	Да (любой набор интерфейсов)
Возможности по изменениям системы	Да	Нет	Да
Наличие участников рынка, успешно использующих технологию	Да, российские банки	Да, российские банки, в том числе обладающие ИТ-инфраструктурой, аналогичной банку	Да, российские банки, в том числе обладающие ИТ-инфраструктурой, аналогичной банку
Возможность получения банком референсов от участников рынка по применению технологии поставщика	***	Да, обязательное условие	Да, обязательное условие
Подтверждённая скорость внедрения технологии	Нет	Да	Нет
Фактические сроки внедрения технологии (учитывая опыт участников рынка)	от 6 месяцев и более	от 3 до 6 месяцев	от 6 месяцев и более (максимально — до 2 лет)
Статус разработчика технологии	ИТ-команда банка	компания, включённая в Реестр аккредитованных ИТ-компаний	компания, включённая в Реестр аккредитованных ИТ-компаний
Получение гарантии качества	Да	Да	Да

Таблица. Параметры, учитываемые при выборе варианта разработки ПО: собственными силами или от поставщиков

независимого в своей работе от других подразделений. Как правило, такой модели в оргструктуре придерживаются крупные банки и средние банки, входящие в банковские группы.

В «Своём Банке» после ряда внутренних обсуждений подразделением, отвечающим за развитие антифрод-системы, стал департамент управления рисками во главе с Chief Risk Officer (CRO). Была достигнута договорённость о создании в организационной структуре банка транзакционного антифрод-центра, обеспечивающего непрерывную аналитику и разбор транзакций в режиме 24/7.

НЕПРОСТОЙ ВЫБОР. ЧТО ЛУЧШЕ?

Концептуальный вопрос в отношении состава технологий, используемых в задачах транзакционного антифрода, на который банку крайне важно получить ответ, оценив все «за» и «против». Как правило, выбор сводится к двум альтернативным вариантам — вести

разработку ПО собственными силами или обратиться к поставщикам уже за готовым решением. Когда «Свой Банк» делал такой выбор, то учитывались параметры, которые мы свели в отдельную таблицу (см. Таблица).

Обобщая эти параметры, могу отметить, что при выборе антифрод-системы нами оценивались, прежде всего, следующие: функциональность, стоимость, конфигурация, возможность внесения изменений собственными силами.

Выстраивание системы фрод-мониторинга с нуля, несомненно, сложный многоэтапный процесс, в котором важна синергия усилий всех участников процесса для минимизации потерь банка по фродовым кейсам. И сегодня «Свой Банк» успешно справляется с этой задачей.

НОВАЯ ВЕРСИЯ ОС

USERGATE ПРЕДСТАВИЛ РЕЛИЗ-КАНДИДАТ ВЕРСИИ 7.1 СОБСТВЕННОЙ ОС UGOS И НОВЫЕ КОМПОНЕНТЫ ЭКОСИСТЕМЫ USERGATE SUMMA

Анна КАТАНКИНА
корреспондент BIS Journal

В середине ноября 2023 г. российский разработчик решений для информационной безопасности UserGate представил релиз-кандидат версии 7.1 собственной операционной системы UGOS. Она является основой для экосистемы UserGate SUMMA, которая включает в себя обновлённый межсетевой экран следующего поколения UserGate NGFW и новые решения UserGate Client и UserGate SIEM Light, доступные для тестирования.

ЧЕТЫРЕ ТРЕНДА

Открывая презентацию, менеджер по развитию компании Иван Чернов отметил четыре современных тренда в сфере ИБ:

- ♦ актуальные угрозы — вымогатели, которые теперь крадут данные и требуют выкуп за неразглашение утечки;
- ♦ долгое и скрытое нахождение злоумышленников в сети, наблюдение и продажа доступов на теневых площадках;
- ♦ рост сложности атак и, как следствие, увеличение периметра защиты, распространение контроля на всю инфраструктуру компании;
- ♦ реагирование и обмен опытом компаниями по ИБ на уровне орга-

низаций и государства, умение анализировать ситуацию во всей отрасли и на уровне страны.

Исходя из этих трендов, менеджмент компании понимает, что экосистема UserGate SUMMA движется по пути эволюции, развития концепции XDR — eXtended Detection and Response. Она покрывает всю инфраструктуру заказчика, предоставит инструменты для мониторинга и обнаружения угроз, реагирования на них, включая такие решения, как UserGate NGFW, WAF, UserGate Client и другие, в том числе разработки сторонних вендоров. Сегодня каждый компонент экосистемы UserGate SUMMA усиливает функциональные возможности других инструментов и обеспечивает синергетический эффект.

ЭКОСИСТЕМА

«Мы занимаемся разработкой комплексных решений для защиты цифровой инфраструктуры более 13 лет. Собственная научно-исследовательская и производственная база позволяла нам создавать независимые продукты и решения, которые среди корпоративных заказчиков пользовались стабильно высоким спросом. Мы реализовали более пяти тысяч проектов внедрения наших решений и накопили значительный экспертный опыт как в области противодействия киберугрозам любой сложности, так и с точки зрения понимания специфики наших заказчиков. В результате мы создали экосистему, состоящую

из продуктов, решений и услуг, которые обеспечивают главное условие защищённости — максимальную видимость событий безопасности. В рамках релиз-кандидата версии 7.1 мы представляем расширенный набор продуктов и решений, которые закрывают актуальные потребности рынка, в частности UserGate Client и UserGate SIEM Light», — отметил Иван Чернов.

Обновлённая версия UserGate NGFW включает технологию UserID, которая решает задачи идентификации пользователей в сети и точную информацию об их сетевой активности, применяет политики безопасности к работе приложений в сети, регламентируя доступ к ним в зависимости от привилегий пользователей. В релиз-кандидате ОС UGOS 7.1 предусмотрена возможность создания пользовательских сигнатур IDPS&L7. Таким образом, администраторы UserGate NGFW могут самостоятельно создавать набор правил и сигнатур для системы обнаружения вторжений и приложений, что особенно актуально для компаний финансового сектора и организаций, осуществляющих собственную разработку. Также версия 7.1 UGOS по многочисленным просьбам клиентов UserGate сможет поддерживать новый протокол VPN IKEv2, актуальный для современных версий ОС Android, и технологию UpStream Proху, которая позволяет осуществлять безопасный доступ в интернет в закрытых сегментах сети, например, для обновления ПО на объектах критической информационной инфраструктуры.

ТРИ ФУНКЦИИ

UserGate Client — это уникальное решение, предназначенное для управления безопасным доступом в сеть, объединившее в себе три функции для защиты удалённого доступа

Менеджмент компании понимает, что экосистема UserGate SUMMA движется по пути эволюции, развития концепции XDR

устройств: VPN, NAC и EDR, отметил Виталий Даровских, менеджер по развитию продукта. Оно обеспечивает контроль и расширенную защиту устройства, возможность его безопасного подключения к корпоративной сети посредством защищённого канала связи (VPN) и контроля безопасности подключаемого оборудования, ограничение доступа к приложениям в рамках единой стратегии ИБ, детектирования вредоносной активности и реагирования на угрозы, а также осуществляет фильтрацию вредоносных и запрещённых сайтов, защищает сетевые соединения.

Решение позволит осуществлять централизованное управление группами, политиками и событиями, а также мониторинг, аналитику и реагирование через единый UserGate Management Center. UserGate Client также является важным компонентом реализации концепции сетевого доступа с нулевым доверием (ZTNA) и осуществляет сбор логов, журналов и отчётов для SIEM-системы UserGate SIEM.

ЧТО НОВОГО?

Какие изменения произошли в UserGate SIEM? Появились UserGate LogAnalyzer — продукт с базовой лицензией, полноценная лицензируемая система UserGate SIEM light — система управления событиями информационной безопасности и UserGate SIEM Expert, включающая подписку на обновляемые правила аналитики от вендора.

UserGate SIEM Light (версия Release candidate) по состоянию на ноябрь 2023 г. отвечает за сбор информации из различных источников и приведение их к единому формату для удобства последующего разбора и анализа,

отмечает Дмитрий Чеботарев, менеджер по развитию продукта. Она включает в себя функциональность платформы реагирования на инциденты (IRP) и систему оркестрации, автоматизации и реагирования на инциденты (SOAR). Это позволяет анализировать поведение различных процессов, выявлять риски и на основе проведённого анализа обеспечивать автоматическую реакцию, осуществляя защиту от аномального поведения или реальных угроз на самой ранней стадии, а также управлять процессами реагирования на инциденты ИБ.

С помощью пакетов экспертизы от Центра мониторинга и реагирования (MRC) UserGate в решении появилась возможность обнаруживать следы компрометации (IoC) на конечных устройствах, а также блокировать вредоносную активность в случае обнаружения инцидента.

ПРО ДВИЖОК

Новая версия движка UserGate IPSv3, лежащего в основе системы обнаружения вторжений (IDS) и определения приложений на уровне L7 по модели OSI, может блокировать IP-адреса и порты, применять правила фильтрации трафика или автоматически отключать подозрительные соединения. IPSv3 также предоставляет информацию о попытках вторжения и сетевых угрозах, попытках эксплуатации уязвимостей и атаках, помогая специалистам принять своевременные меры.

Среди новых возможностей и преимуществ движка IPSv3 — проверка сетевого трафика после расшифровки SSL; возможность написания собственных сигнатур IDPS&L7 с помощью языка UserGate Application and

Security Language (UASL) и их добавление в правила межсетевого экрана UserGate NGFW, а также отдельная настройка действий для каждой сигнатуры; верификация и полноценное управление с помощью CLI (Command Line Interface).

Все продукты UserGate реализованы как в виде программно-аппаратных комплексов, так и в виртуальном исполнении, с возможностью развёртывания в облаке.

ПРО ПЕРСПЕКТИВЫ, КАДРЫ И САМОСТОЯТЕЛЬНОСТЬ

Оценивая перспективы развития, Дмитрий Курашев, директор и сооснователь UserGate, отметил, что UserGate — особенная компания, которая привыкла работать в долгую и развиваться за счёт собственных средств. Она сотрудничает с другими компаниями, рекомендуя применять их решения в экосистеме UserGate SUMMA, однако есть узкое место — люди, профессионалы. «Ни за какие деньги нельзя сразу сформировать сбалансированную команду, состоящую из талантливых профессиональных людей», — подчеркнул он. В этой связи UserGate открывает новые офисы: в Санкт-Петербурге (открыт в сентябре 2022 г.) и Минске, а также в Томске, где есть сильная учебная база.

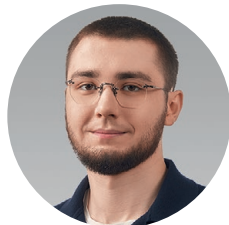
«Возможно, мы придём через несколько лет к тому, что на рынке будет 3–4 экосистемы, может, где-то будет пересечение и сотрудничество, как получится... Мы самостоятельный игрок, у которого есть все необходимые ресурсы для создания любых необходимых ИБ-решений всем категориям клиентов», — отметил Д. С. Курашев.



Компания UserGate — российский разработчик программного обеспечения и микроэлектроники, обеспечивает своими решениями информационную безопасность корпоративных сетей как предприятий малого и среднего бизнеса, так и крупных корпораций с распределённой инфраструктурой. В 2022 г. UserGate вошла в рейтинг TAdviser Security 100 крупнейших ИБ-компаний России, заняв в нём 14-е место. В рейтинге «CNewsFast: Самые быстрорастущие ИТ-компании 2022» компания занимает четвёртое место и лидирует среди разработчиков продуктов в сфере информационной безопасности.

«АТАКИ С ТЕХНОЛОГИЕЙ HTTP/2 RAPID RESET ПРОЩЕ ДЕТЕКТИРУЮТСЯ...»

О ПЛЮСАХ ГИБКОГО ПОДХОДА В ЗАЩИТЕ ОТ DDOS-АТАК



Даниил БОБРЫШЕВ
владелец
продукта
Servicepipe
DosGate

В середине октября практически все профильные СМИ написали о новой технологии DDoS-атак под названием HTTP/2 Rapid Reset, которая применяется с августа и благодаря которой бьются все рекорды DDoS. В то же время, по мнению владельца продукта Servicepipe DosGate Даниила Бобрышева, «не так страшен чёрт, как его малюют». И правильно выбранное решение по защите от DDoS-атак вполне способно справиться как с новой угрозой, так и с уже хорошо знакомыми.

— Начать наш разговор я бы хотела с нового типа DDoS-атак под названием HTTP/2 Rapid Reset, которая упоминается в последних отчётах мировых технологических лидеров AWS, Cloudflare и Google. Сообщают, что эти атаки бьют рекорды интенсивности. Если ваших клиентов вдруг атакуют с помощью HTTP/2 Rapid Reset, справитесь?

— Наши устройства фильтрации от DDoS-атак работают в первую очередь на сетевом уровне, а не внутри TCP-сессий, разбирая отдельно каждый HTTP-запрос. Для нас это выглядит как разновидность флуда внутри сформированного открытого

TCP-соединения, который мы блокируем точно так же успешно, как и любой другой. Атаки HTTP/2 Rapid Reset проще детектируются, так как очень большой объём сетевого трафика направляется в рамках одной TCP-сессии, а не распределяется на множество. Использование технологии нашей собственной разработки DosGate позволяет превентивно заблокировать более 99% сетевых атак на любые корпоративные сервисы. Бизнес-процессы не останавливаются, а сотрудники даже не замечают, что сервисы находятся под DDoS.

— На своём сайте вы называете DosGate гибкой системой контроля трафика для защиты от DDoS-атак. Это просто слоган из рекламных брошюр и буклетов или же есть принципиальное отличие от других решений на рынке?

— Это не слоган. Пример гибкости — заказчик может заказать у нас коробочное решение, не требующее дополнительных настроек. Есть экспертный и продвинутый режимы управления. В экспертном режиме администратор системы может самостоятельно реализовывать собственные контрмеры прямо из веб-интерфейса без написания программного кода. В продвинутом режиме для защиты сервисов и сетевых сегментов применяются пресеты. Это готовые к применению настроенные политики фильтрации для защиты сервисов или сетевых сегментов, в реальном времени синхронизирующиеся с нашей базой вредоносных сигнатур. Они доступны сразу после установки и защищают сотни разных сервисов и сетевых сегментов. Пресеты постоянно обновляются и эволюционируют.

— И что это даёт?

— Благодаря этой гибкости наши решения используют как крупнейшие заказчики (государственные и частные), так и небольшие игроки без ИБ и ИТ-специалистов в штате, которым хочется отдать управление системой, например, в свой сетевой департамент.

Ещё один пример гибкости — отличная интеграция с решениями заказчика. С теми же системами управления информационной безопасностью и событиями безопасности (SIEM), межсетевыми экранами для веб-приложений (WAF).

Например, почти любой ваш любимый WAF можно установить и запустить прямо рядом с нашим ПО. DosGate будет передавать выбранные пакеты и сессии на уровень WAF, например, определяя их по порту, IP-получателя и протоколу.

— Почему важна совместимость с теми же WAF, например? В чём плюс?

— Плюс в том, что удобно администрировать и поддерживать одну платформу вместо 10 разных. Удобнее для сетевых администраторов, инженеров ИБ. По сути, это комплексное решение: всё в одном месте и работает одинаково хорошо, не конфликтуя, а наоборот, интегрируясь друг в друга и страхуя.

— Одним из преимуществ DosGate вы называете качественную эшелонированную защиту. В то же время в рекламных материалах ваших конкурентов также есть эшелонированная защита как одно из преимуществ. В чём разница?

— В отличие от других игроков рынка мы сами владеем большой распределённой сетью, которую используем

наши заказчики при активации эшелонированной защиты. В дополнение к этому наша эшелонированная защита — это не просто «сигнал начать очистку», это также автоматизированный алгоритм передачи политик фильтрации с локального центра очистки клиента на наши облачные платформы. По сути, за счёт эшелонированной защиты мы позволяем клиенту расширить объём пропускной способности его локального центра очистки на наши ёмкости — больше 1200 Гбит/с по России и миру.

Наша эшелонированная защита также не всегда подразумевает ежемесячные платежи и активный канал связи. Заказчик может платить за количество часов, распределённое на год, в рамках которых он может включать наши каналы связи через BGP over GRE или физический стык, при этом делать это только во время больших атак, которые перегружают его локальный центр очистки (в автоматическом режиме). Таким образом, заказчик ещё и экономит бюджеты.

— **В качестве одного из преимуществ DosGate компания называет наличие системы компонентов для массового управления профилями защиты. Можете пояснить, в чём это преимущество заключается?**

— Представим себе крупную компанию, например системно значимый банк с множеством профилей защиты. И возникает необходимость внести изменения только в часть профилей (например, в 50 из 100). В большинстве решений изменения придётся либо вносить вручную, либо писать отдельный скрипт — моментально распространить изменения не получится. Система компонентов в DosGate позволяет строить профили защиты, отталкиваясь не от контрмер или правил, а от компонента, который можно создать и распространить сразу на ряд выбранных профилей. Таким образом, при обновлении системы всё происходиткратно быстрее. К примеру, в той же организации с 400 профилями защиты ранее обновление могло занимать несколько часов монотонной работы в стиле «вкладка открыть — вкладка

закрыть» или обновления применялись сразу на все 400 профилей защиты, а не на выбранные. В DosGate можно обновить конфигурацию, а затем опубликовать изменения в выбранные профили, например в 350 из 400. Ну то есть экономия времени от нескольких часов до буквально пары минут.

— **В DosGate сетевой фильтр работает одновременно с сетевыми пакетами и сессиями. Что это даёт?**

— Это позволяет эффективно защищать не только конечные устройства и сервисы, но и промежуточные узлы, уязвимые к сессионным атакам (например, те же межсетевые экраны или WAF). В конечном итоге это даёт более высокий уровень защиты. Сессионный фильтр DosGate не требует исходящего трафика, не терминирует на себе TCP-соединения, но при этом умеет разрывать эти соединения как с оборудованием, установленным после него, так и с изначальным установщиком этой сессии.

— **На рынке есть решения, в которых база вредоносных сигнатур формируется в автоматическом режиме. У вас тоже этот процесс автоматизирован?**

— Мы сознательно отказались от автоматизации при создании вредоносных сигнатур, поскольку излишняя автоматизация очень часто приводит к высокой частоте ложных срабатываний, а также низкой точности фильтрации при многовекторных атаках. Это в итоге приводит к тому, что инженер идёт и в любом случае модернизирует сформированные автоматически сигнатуры. В DosGate есть собственная база вредоносных сигнатур, когда вместе с IP и TLS-отпечатками распространяются пресеты для защиты сетей и сервисов без обучения, генерации сигнатур и др. Защита работает с первого часа после её установки. Пресеты поддерживаются нашей командой и обновляются каждый час, мы в том числе используем автоматизацию, но только как «помощник инженера», а не «его глаза и руки».

— **Есть какие-то новые продукты на основе DosGate, которые**

вы выпустили на рынок за последнее время?

— Если можно назвать продуктом возможность установки DosGate на конечные устройства, тогда да. В отличие от других решений, если у вас, например, большая облачная инфраструктура или вы просто не можете позволить себе установку чего-то на уровне периметра вашей сетевой инфраструктуры, теперь вы можете приобрести DosGate и установить его как ПО на уже существующий промежуточный или конечный узел.

Например, если у вас развёрнута виртуальная машина в облаке с WAF, то вы можете прямо на эту же виртуальную машину установить DosGate для защиты от L3–L7 DDoS-атак.

Или, например, у вас 50 разных виртуальных машин, где живут разные конечные сервисы: от VPN до RDP, вы можете на каждую из них установить DosGate и управлять всей этой системой из единого веб-интерфейса, таким образом организуя защиту не на уровне периметра, а непосредственно на конечных устройствах.

Это самый простой и бюджетный на рынке вариант on-prem-защиты от DDoS-атак на L3–L7. Легко устанавливается на веб-сервер или виртуальную машину перед WAF, NGFW или Load Balancer. Не является промежуточным узлом и не требует переключения текущей сетевой инфраструктуры.

— **Понимаю, что сложно прогнозировать действия хакеров, но если попытаться заглянуть в будущее — что нас ждёт? Стоит ли ожидать появления новых технологий, роста мощностей атак? Или, возможно, наоборот, ожидается спад?**

— Первая DDoS-атака была зафиксирована в 90-х годах, а первая DoS-атака — в 70-х. С тех пор объёмы атак и сложность их детектирования только росли. Такая тенденция будет сохраняться и в будущем, будут появляться новые многовекторные атаки уровня приложений, DoS-уязвимости в программно-аппаратных комплексах, новые амплификаторы и формироваться ещё более большие ботнеты. Неизбежно год за годом DDoS-атаки будут бить рекорды.

АВТОМАТИЗАЦИЯ ТЕСТОВ НА ПРОНИКНОВЕНИЕ

ВОЗМОЖНОСТИ И ПРЕИМУЩЕСТВА



Максим ПЯТАКОВ
заместитель генерального
директора, сооснователь CtrlHack



Виктор СЕРДЮК
генеральный директор
АО «ДиалогНаука»

ЧТО ЗАКАЗЧИК ХОЧЕТ ОТ ТЕСТА НА ПРОНИКНОВЕНИЕ?

За последние годы многие владельцы информационных систем поняли, что наиболее результативным методом оценки защищенности является проведение тестов на проникновение. Такие тесты позволяют посмотреть на свою сеть глазами хакера, выявить недостатки в системе защиты и подготовиться к возможным реальным кибератакам. Да и регуляторы все чаще выдвигают требования о необходимости проведения тестирований на проникновение на регулярной основе. Поэтому многие покупают услуги по проведению пентестов, а часть компаний создают свои внутренние команды по проведению тестов на проникновение или команды red team.

Основная цель, которая преследуется заказчиками при планировании таких работ — это имитация действий хакеров для оценки уровня реальной защищенности системы. При этом предполагается, что во время таких работ будет покрыта максимально возможная часть инфраструктуры. Хакеру же нельзя указать, в какой части инфраструктуры ему начинать и развивать атаку,

а в какой нет. В крупных инфраструктурах, особенно территориально-распределенных, настройки могут отличаться настолько, что в одном месте какие-то из хакерских действий невыполнимы, а в другой части инфраструктуры эти же действия вполне могут иметь успех.

Однако в рамках выделенного времени и стоимости работ ни одна команда не сможет охватить всю инфраструктуру и проверить возможность выполнения максимального количества хакерских техник. В результате команды вынужденно фокусируются на действиях, которые можно выполнить достаточно быстро и которые чаще всего дают необходимый результат (конечно, исходя из опыта работ каждой такой команды).

ПРОБЛЕМЫ «РУЧНЫХ» ТЕСТОВ НА ПРОНИКНОВЕНИЕ?

Рынок услуг по проведению тестов на проникновение хорошо развит. Есть большое количество компаний, готовых оказывать такие услуги. Однако у таких услуг есть свои минусы и ограничения. Если мы говорим о внешней команде, то каждый цикл работ это закупочные

процедуры, заключение договоров, согласование ТЗ, приемка работ. Т.е. долго, сложно. Поэтому такие работы обычно выполняются один или два раза в год.

При этом практически невозможно гарантировать высокую квалификацию команды во время выполнения ручного теста на проникновение. Кроме того, фактически внешние люди получают доступ к информации о возможных уязвимостях тестируемой инфраструктуры с соответствующими рисками утечки такой чувствительной информации.

Что же с технической стороны выполнения тестов на проникновение? В связи с ограниченным временем выполнения работ команда обычно успевает проверить ограниченный набор техник для получения результата. При этом хакер не имеет таких ограничений. Если посмотреть на общую картину, то на данный момент известно и описано несколько сотен реализаций различных техник на разных шагах выполнения кибератак. Понятно, что ни одна из команд физически не сможет проверить даже 10–15% таких техник. Да в большинстве случаев для достижения результата им это и не нужно. Если в ходе работ команда смогла найти один

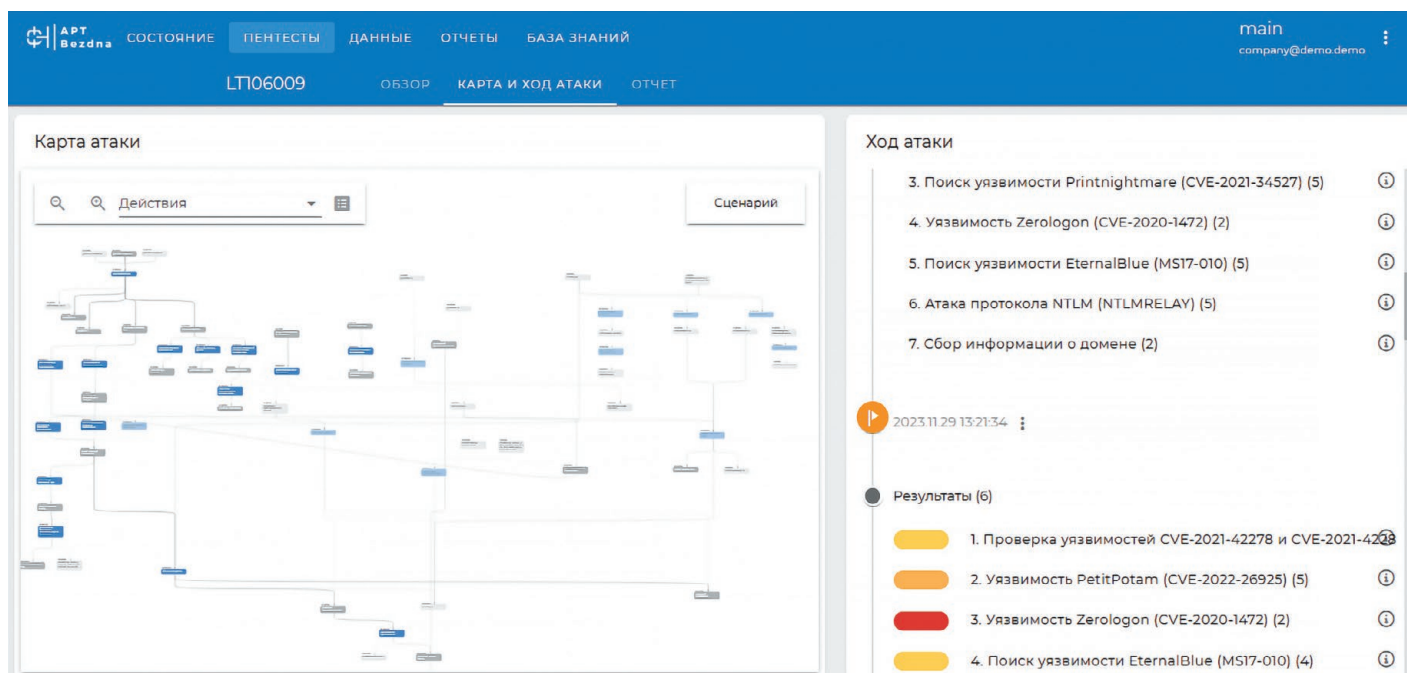


Рисунок 1. Сценарий атаки комплекса автоматического тестирования на проникновение CtrlHack APT Bezdna

вектор атаки, который успешно выполнен, то в большинстве случаев остальные возможные векторы не проверяются.

Сроки и ограничения по трудозатратам приводят также к тому, что проверками в рамках теста покрывается только часть инфраструктуры. Даже на первичном этапе внутреннего сканирования затрагивается обычно только небольшая часть машин и соответственно дальше атака в рамках теста распространяется также только по некоторому участку инфраструктуры. Также ни одна команда не сможет покрыть тестами большую часть машин в крупной сети (в которой может насчитываться несколько тысяч или даже десятков тысяч узлов). Как один из вариантов выхода из этой ситуации — заказывать работы, которые включают в себя выполнение тестов одновременно в разных сегментах сети. Но такие работы будут стоить значительно больших денег.

После окончания теста на проникновение исполнитель готовит отчет с описанием выявленных уязвимостей и несоответствий, и заказчик запускает процесс исправления выявленных недостатков. Но как проверить потом, что действительно ВСЕ недостатки исправлены? В большинстве случаев такие проверки

откладываются до следующего запланированного теста. И во многих случаях выясняется, что не все было корректно исправлено. К сожалению, оперативно проверить качество устранения недостатков практически невозможно.

Как результат — оценка защищенности только раз в полгода или год, по ограниченному набору векторов атак и только для части инфраструктуры.

ВНУТРЕННЯЯ КУХНЯ ТЕСТОВ НА ПРОНИКНОВЕНИЕ

Если мы говорим о «внутренних» тестах на проникновение, то такой тест (также как и реальная атака) состоит из набора шагов, которые позволяют выполнить закрепление, повышение привилегий, разведку, распространение в сети и т.д.

При этом большинство действий на этих шагах известны и описаны. А многие из этих действий не являются уникальными для каждого теста и могут использоваться без существенных изменений в разных сетях заказчиков. Некоторые операции могут быть уникальны, разрабатываться под конкретную сеть или требовать анализа человека. Но большинство операций рутинны и повторяются без существенных изменений из теста

в тест. Команды, которые выполняют большое количество тестов на проникновение, для сокращения трудозатрат используют специальные скрипты или разрабатывают свои скрипты для автоматизации таких действий. Более того, часть векторов атак, например, связанных с атаками на контроллер домена с целью его захвата, могут выполняться в автоматическом режиме практически без участия человека.

ПОМОЖЕТ ЛИ АВТОМАТИЗАЦИЯ?

Так как часть операций в рамках теста на проникновение можно автоматизировать, то возникает вопрос, а можно ли вообще выполнять такие тесты в автоматическом режиме и без привлечения специалистов из внешних команд? Ответ на него дали израильские разработчики, создавшие первую платформу автоматического тестирования на проникновение. Она позволила в автоматическом режиме выполнять ряд сценариев, выполняемых в рамках «внутреннего» теста на проникновение.

Такие системы позволяют устранить ряд недостатков «ручных» тестов:

- ♦ автоматизация поможет максимально покрыть инфраструктуру;

Обзор действий и их описание ×

☰ ДАННЫЕ

ATAKA NOPAC (CVE-2021-42278 и CVE-2021-42287)

Название:

Атака NoPac (CVE-2021-42278 и CVE-2021-42287)

Краткое описание:

NoPac это цепочка атак из состоящая из двух уязвимостей. CVE-2021-42278 и CVE-2021-42287

[CVE-2021-42278](#) позволяет обойти уязвимость системы безопасности, которая позволяет потенциальным злоумышленникам выдать себя за контроллер домена с помощью спуфинга учетной записи **sAMAccountName** учетной записи компьютера.

CVE-2021-42287

[CVE-2021-42287](#) уязвимость обхода безопасности, которая влияет на сертификат атрибута привилегий Kerberos (PAC) и позволяет потенциальным злоумышленникам олицетворять контроллеры домена.

Рекомендации по снижению выявленного риска:

- <https://support.microsoft.com/ru-ru/topic/kb5008380-обновления-проверки-подлинности-cve-2021-42287-9dafac11-e0d0-4cb8-959a-143bd0201041#:~:text=Сводка,потенциальным%20злоумышленникам%20олицетворять%20контроллеры%20дом ена.>
- <https://support.microsoft.com/ru-ru/topic/kb5008102-изменение-изменений-диспетчера-учетных-записей-безопасности-active-directory-cve-2021-42278-5975b463-4c95-45e1-831a-d120004e258e#:~:text=Сводка,записи%20sAMAccountName%20учетной%20записи%20компьютера.>

Рисунок 2. Описание найденных уязвимостей и рекомендации по устранению выявленных недостатков в платформе симуляции кибератак CtrlHack APT Bezdna

♦ автоматические сценарии могут использовать больше техник, чем человек в рамках своих работ;

♦ можно полностью повторить выполненный тест для проверки исправлений недостатков;

♦ можно делать тест на проникновение намного чаще и в то время, когда вам это нужно без привлечения внешних команд.

Как результат появляется возможность проводить постоянную оценку защищенности всей инфраструктуры компании (рис.1).

Безусловно, системы автоматического тестирования на проникновение не могут полностью заменить человека, и место для «ручного» теста на проникновение все равно остается, ведь нетривиальные действия автомат не сможет выполнить. Но при этом автоматизация основных и наиболее часто используемых

техник позволит существенно повысить защищенность инфраструктуры и на постоянной основе отслеживать возможные проблемы и недостатки с точки зрения безопасности сети. А для специалистов по тестам на проникновение остаются более сложные сценарии. В случае же наличия внутренней команды по тестам на проникновение автоматизация позволяет существенно повысить эффективность таких команд и избавить их от выполнения рутинных операций.

ПЕРВАЯ РОССИЙСКАЯ ПЛАТФОРМА АВТОМАТИЧЕСКОГО ТЕСТА НА ПРОНИКНОВЕНИЕ

Российский разработчик платформ симуляции кибератак компания CtrlHack представила свой новый продукт — CtrlHack APT Bezdna. APT

Bezdna — это комплекс автоматического тестирования на проникновение. Продукт предназначен для проведения тестов внутренней инфраструктуры. В разработке принимает участие команда «пен-тестеров» с большим опытом выполнения тестов у крупных корпоративных заказчиков. Свой опыт и глубокую экспертизу они переносят в сценарии, которые выполняются в рамках автоматических тестов. Комплекс позволяет одним кликом запустить тест с максимальным покрытием задач. По итогам выполнения теста предоставляется детальный отчет с рекомендациями по устранению выявленных недостатков (рис. 2). Результаты выполненного теста можно использовать для проведения последующих тестов и для приоритизации выявленных уязвимостей.

НОВАЯ ПАРАДИГМА ОТ INFOWATCH

ЗАЩИЩАТЬ ДАННЫЕ ПО КОНТЕКСТУ,
А НЕ ПО СОДЕРЖАНИЮ



Александр КЛЕВЦОВ
руководитель
по развитию
продукта
InfoWatch Traffic
Monitor

Кажется, накал страстей по поводу защиты персональных данных достиг апогея, но нет: общество, государство, бизнес и регуляторы продолжают активно обсуждать эту тему. Обеспечение безопасности данных остаётся сложной и до конца не решённой задачей. Но мы не сдаёмся и надеемся на успех в 2024 году благодаря уникальной разработке компании InfoWatch.

ВСЁ, ЧТО МОГЛО, УТЕКЛО?

На BIS Summit – 2023 внимание экспертов было сконцентрировано на проблеме утечки данных и их возможного обесценивания. Представители ФСТЭК РФ, депутаты Госдумы РФ, сотрудники Роскомнадзора и представители бизнеса единогласно выразили мнение, что утверждения об обесценивании утечки несостоятельны: утечка по-прежнему представляет опасность как для человека, так и для бизнеса.

Согласно данным аналитического центра InfoWatch, за первое полугодие 2023 года утекло около 18,3 миллиарда записей ПД, что сопоставимо с цифрами за весь 2022 год. То есть даже статистика подтверждает, что утечка — это по-прежнему серьёзная угроза.

В ЧЁМ СЛОЖНОСТЬ?

Эффективным инструментом в предотвращении утечек традицион-

но считаются DLP-системы. Но на практике не все они справляются с задачей. Письмо с подписью сотрудника и письмо со слитыми данными клиента — это два одинаковых письма для классических DLP-систем.

Стандартная технология — настройка политик защиты данных с применением регулярных выражений, специализированных словарей — не справляется с задачей полностью. Такой способ несоразмерно трудоёмкий, ведь когда база клиентов содержит миллионы записей, то нужно создать ровно столько же соответствующих правил. То есть с увеличением числа клиентов создание правил для защиты их данных превращается в нерешаемую проблему.

И второй сценарий, где традиционная DLP пасует, — это отправка персонализированных предложений. Выписка по счёту VIP-клиенту, коммерческое предложение новому партнёру, ошибочная отправка договора контрагенту, с которым не подписан NDA... Как определить, что письмо было отправлено именно адресату, а не по ошибке? Традиционные DLP-системы не способны дать ответ на этот вопрос.

НОВАЯ ПАРАДИГМА

InfoWatch предлагает новый подход, основанный на контекстном анализе данных, что позволяет точно идентифицировать конкретные ПД клиентов и проверять их принадлежность законным владельцам. Таким образом, у пользователя реализована автоматическая политика с миллионами правил, которые обновляются автоматически при обновлении данных в бизнес-системе.

Речь не только о защите данных, которые сложно описать формулой, но и об управлении качеством бизнес-процесса. Актуальные данные сотрудников синхронизированы с DLP-системой, при отправке определяются как легитимная отправка и не подсвечиваются как событие. Как пример из клиентской практики — легитимная отправка финансовых данных за периметр компании — зарплатные листки удалённым сотрудникам без шквала ложных срабатываний системы (см. рис.).

По результатам Национальной банковской премии в декабре 2023 г. компания InfoWatch была признана победителем в номинации «Лучшая система защиты персональных данных для банковской отрасли» за внедрение решения по защите данных в крупном российском банке.

ИС, где хранятся данные	Письмо с выгрузкой по счёту	DLP-система	
124. Иван Иванов, ivanov@mail.ru	Уважаемый Иван Иванов! Ваша выписка по счёту №...	ivanov@mail.ru ✓	Система проверила, что выгрузка о состоянии счёта принадлежит Ивану Иванову, его адрес электронной почты совпадает с тем, на который пытаются отправить данные. отправка легитимна и разрешена
3555. Пётр Сидоров, sidorov@yandex.ru	Уважаемый Сергей Собянин! Ваша выписка по счёту №...	sidorov@yandex.ru ✗	Система проверила, что выгрузка о состоянии счёта принадлежит Сергею Собянину, но его адрес электронной почты не совпадает с тем, на который пытаются отправить данные. отправка нелегитимна и заблокирована

КИБЕРБЕЗОПАСНОСТЬ-2024

ПРОГНОЗЫ РАЗВИТИЯ ОТРАСЛИ



Евгения КОЛОДИНА
первый
заместитель
генерального
директора
ЦИБИТ



Василий ОКУЛЕССКИЙ
эксперт ИБ,
преподаватель
учебного
центра ЦИБИТ,
к. т. н.



Илья ГЕЙМУР
заместитель
руководителя
кадрового
агентства
ЦИБИТ

ЦИБИТ (Центр исследования безопасности информационных технологий) – консалтинговая компания, работающая в области информационной безопасности в России с 2009 года. Занимая лидерские позиции в отрасли, ЦИБИТ постоянно исследует рынок и проводит аналитику. Сегодня эксперты компании делятся своими прогнозами для сферы информационной безопасности России на 2024 год.

Евгения Колодина, первый заместитель генерального директора ЦИБИТ:

«Чтобы делать экспертные прогнозы, необходимо сначала провести глубокую аналитику тенденций прошлого года, характерных для отрасли.

В 2023 году мы выделили несколько главных проблем, с которыми столкнулась сфера информационной безопасности России, – огромное количество утечек персональных данных, рост мошенничества с финансовой информацией и, конечно, нехватка квалифицированных специалистов».

Исходя из ключевых явлений прошлого года, эксперты ЦИБИТ видят несколько тенденций, переходящих в 2024 год:

- ♦ существенное ужесточение требований к защите персональных данных;
- ♦ ужесточение требований к защите критической информационной инфраструктуры;

♦ серьёзные изменения в области информационной безопасности финансовых организаций, в том числе в связи с законом о цифровом рубле;

♦ развитие форм социальной инженерии и методов борьбы с такими кибератаками;

♦ увеличение дефицита ИБ-кадров.

УЖЕСТОЧЕНИЕ ТРЕБОВАНИЙ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

В 2023 году значительно выросло количество крупных утечек персональных данных. По информации партнёра ЦИБИТ, компании InfoWatch, на конец осени 2023 года число утечек конфиденциальных данных в целом по миру возросло в 2,5 раза (по отношению к 2022 году), в России количество скомпрометированных записей ПДн составило 705 миллионов. Такие значительные цифры, конечно, требуют ответных мер в области регулирования.

Василий Окулесский,

эксперт ИБ, кандидат технических наук, преподаватель учебного центра ЦИБИТ:

«Мы знаем, что в конце прошлого года в Ростехнадзоре была зарегистрирована система сертификации систем менеджмента защиты персональных данных, и сейчас завершается процесс её согласования. И это не только в целом изменит регулирование в области персональных данных, но и приведёт к совершенно новому пониманию значимости

создания систем информационной безопасности».

УЖЕСТОЧЕНИЕ ТРЕБОВАНИЙ ПО ЗАЩИТЕ ЗНАЧИМЫХ ОБЪЕКТОВ КИИ

Весь прошлый год объекты КИИ находились под особенным ударом и под пристальным вниманием кибермошенников. Стоит отметить, что заметным стало изменение мотивации преступников. Всё чаще мотивация атак – не в получении прибыли, а в нанесении ущерба. Именно поэтому в 2024 году мы прогнозируем и усиленные ответные реакции, в том числе со стороны регуляторов.

Сегодня с уверенностью можно предположить, что в 2024 году нас ждут новые изменения в законодательстве, направленные на расширение действия закона в области защиты критической инфраструктуры. Это значит, что появятся новые субъекты КИИ, подпадающие под действие закона, и им необходимо будет проходить процедуру категорирования.

В состав ЦИБИТ входит отдельный департамент, специализирующийся на вопросах обеспечения защиты критической информационной инфраструктуры. Эксперты ЦИБИТ постоянно следят за актуальной ситуацией в законодательном регулировании и готовы помочь клиентам соответствовать всем заявленным требованиям.

ЗАЩИТА ФИНАНСОВОЙ ИНФОРМАЦИИ

Следующая тенденция 2024 года – серьёзные изменения в информационной безопасности в финансовой сфере.

24 июля 2023 года Президент Владимир Путин подписал федеральный закон № 339. Документ вступил в силу 1 августа 2023 года и ввёл в оборот дополнительную форму российской национальной валюты — цифровой рубль.

Во-первых, такое законодательное нововведение говорит о масштабной цифровизации банковской сферы. Во-вторых, появление новой цифровой валюты влечёт за собой и новые сложные задачи для кредитно-финансовых организаций. Здесь нужно упомянуть Положение Банка России от 17.08.2023 № 821-П, вступающее в силу с апреля этого года. Документ введёт дополнительные требования по контролю защиты платежей в рамках использования цифрового рубля.

Василий Окулесский,

эксперт ИБ, кандидат технических наук, преподаватель учебного центра ЦИБИТ:

«Перед банками встанут колоссальные задачи по созданию практически новых инфраструктур, обеспечивающих проведение операций с цифровым рублём параллельно с системой ДБО (дистанционного банковского обслуживания). Эти задачи лягут в первую очередь на плечи подразделений по информационной безопасности. Таким образом, мы говорим о сильном изменении ландшафта финансовых организаций».

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ И ДЕФИЦИТ ИБ-КАДРОВ

Эксперты ЦИБИТ отмечают ещё несколько ожидаемых тенденций в отрасли информационной безопасности в 2024 году.

♦ Социальная инженерия. В сфере информационной безопасности всегда остаётся сложно контролируемая «серая зона». Это атаки методами психологического манипулирования, и здесь постоянно появляются новые схемы и приёмы кибермошенников. В текущем году эта тенденция продолжится, но и ответные меры не заставят себя долго ждать — можно предположить, что будут вводиться новые способы повышения осведомлённости граждан в этой области.

В связи с расширением методов социальной инженерии всё более актуальным становится дополнительное профессиональное образование в сфере информационной безопасности. Учебный центр ЦИБИТ предлагает большое количество образовательных программ, помогающих сформировать нужные компетенции в области защиты информации, а также повысить общую осведомлённость в вопросах кибербезопасности.

♦ Дефицит кадров в области информационной безопасности. Эксперты кадрового агентства ЦИБИТ предполагают, что нехватка специали-

стов в отрасли в 2024 году будет только увеличиваться.

Илья Геймур,

заместитель руководителя кадрового агентства ЦИБИТ:

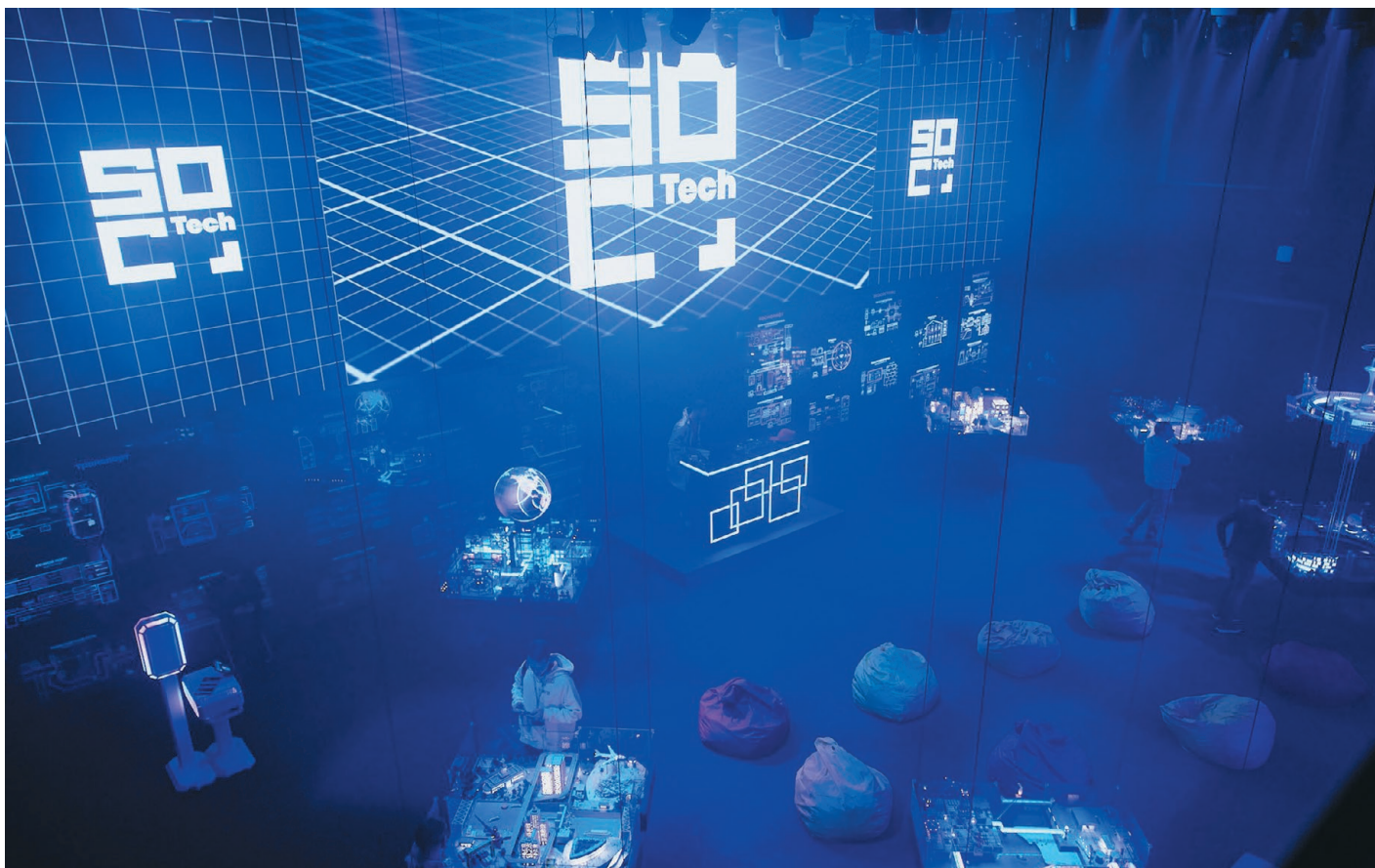
«Мы переживаем поистине исторический момент — рынок труда на глазах переформируется. И дело не только в том, что работодатели столкнулись с серьёзным дефицитом кадров. В нашем обществе кардинально меняется отношение к профессиям и должностям, многие из которых несколько последних десятилетий были менее популярны. Инженер, технолог, специалист по информационной безопасности, учитель, врач, рабочий на предприятии — эти и другие специальности становятся всё более престижными и высокооплачиваемыми. А интерес работодателей к офисным работникам, напротив, постепенно снижается».

Кадровое агентство ЦИБИТ специализируется на подборе и трудоустройстве квалифицированных сотрудников в области информационной безопасности, в том числе для соответствия лицензионным требованиям регулирующих органов. Эксперты ЦИБИТ уже более восьми лет решают самые сложные кадровые вопросы, помогая компаниям по всей России находить лучших специалистов.

ЦИБИТ имеет многолетний опыт экспертизы в области информационной безопасности. В рамках приведения организаций к соответствию требованиям к информационной безопасности ЦИБИТ предлагает комплекс услуг и продуктов:

- ♦ комплексная подготовка организаций к получению различных лицензий;
- ♦ аттестация объектов информатизации;
- ♦ поставка контрольно-измерительного оборудования, средств защиты информации и программного обеспечения;
- ♦ обучение в отраслевом учебном центре;
- ♦ кадровый подбор, тестирование, оценка и трудоустройство специалистов в области ИТ и информационной безопасности;
- ♦ аудит и приведение в соответствие требованиям Банка России;
- ♦ приведение организаций в соответствие ФЗ-152;
- ♦ приведение организаций в соответствие ФЗ-187;
- ♦ пентесты (тестирование на проникновение);
- ♦ поставка, внедрение и развёртывание различных средств, обеспечивающих информационную безопасность;
- ♦ комплекс услуг по обеспечению экономической безопасности предприятия;
- ♦ комплексные услуги по сопровождению клиентов в рамках долгосрочного сотрудничества.

ЦИБИТ: Мы помогаем соответствовать требованиям!



SOC TECH 2023

КИБЕРФОТОГРАФУ ОТДАЛИСЬ ВСЕ!

Марина ПЕРЕСИЛЬД
корреспондент BIS Journal

3 0 ноября прошлого года ведущие эксперты и представители бизнеса встретились на первой конференции SOC Tech 2023, чтобы по-новому обсудить технологии и сервисы для центров мониторинга и предотвращения кибератак. Почти 500 участников подтвердили, что тема развития технологий SOC в разных отраслях более чем актуальна. Конференция состоялась в мультифункциональном московском кибербез-хабе «Кибердом».

ОПЫТНЫЙ ТРЕНЕР

В деловую часть программы вошли более 30 докладов и мастер-классов,

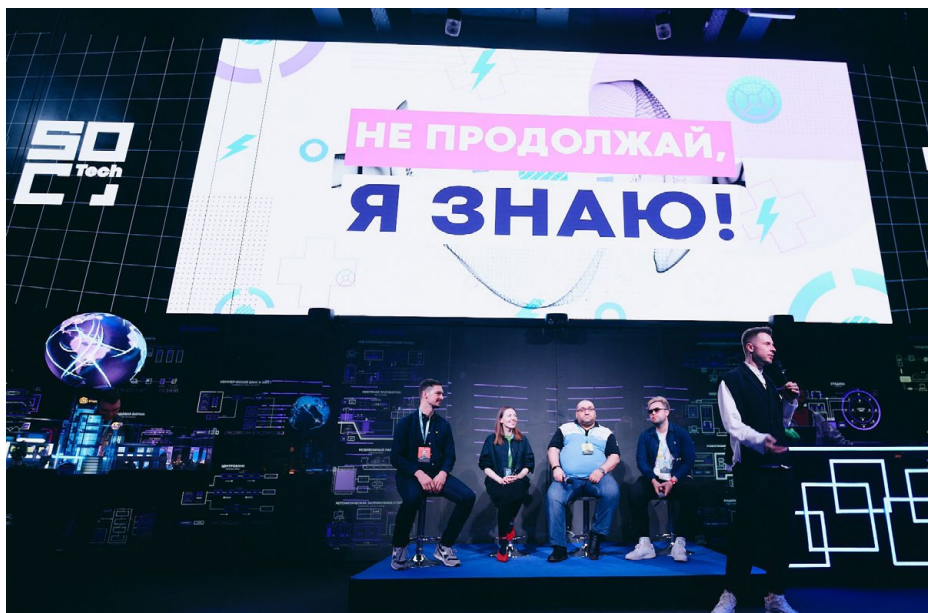
представленные 45-ю спикерами. На сцену поднимались известные в обществе ИБ и за его рамками эксперты: Алексей Лукацкий (Positive Technologies), Алексей Новиков (НКЦКИ), Павел Гусь (МТС RED), Максим Мельшиян (R-Vision), Артем Савчук («Перспективный мониторинг») и др.

Каждый из трёх параллельных треков был посвящён определённым аспектам ИБ. В первом потоке сосредоточили внимание на обнаружении, реагировании и расследовании инцидентов. Второй был посвящён технологиям и инструментам кибербеза. В третьем эксперты обменивались опытом построения SOC и рассказывали о передовых методах и практиках.

В целом участники обсудили практически весь актуальный спектр: от атак на цепочки поставок до

сложностей с переходом на отечественные средства защиты. В выступлениях предлагалось по-новому взглянуть на привычные аспекты ИБ, например, на многофакторную аутентификацию. Самыми актуальными темами уходящего года были признаны «слепые зоны» в мониторинге инцидентов и ключевые меры контроля при обнаружении атак на цепочки поставок.

На практических сессиях специалисты делились опытом и обсуждали проблемы, с которыми сталкиваются в повседневной работе. Участники сессий получили советы и рекомендации от лучших экспертов как повысить эффективность самих SOC и работающих в них специалистов. Компания «Перспективный мониторинг» организовала киберучения Amprige, на которых опытный тренер помог от-



работать новые навыки выявления компьютерных атак и расследования ИБ-инцидентов.

ИСТОРИЯ ОТ ЗАКАЗЧИКА

Одной из самых интересных стала сессия «Практика построения SOC». Сначала Никита Курмышкин, руководитель направления защиты ИТ-инфраструктуры Segezha Group, задался вопросом: «Зачем деревообрабатывающей отрасли нужен SOC?». Он рассказал, что представляет большую геораспределенную компанию, приобретающую филиалы по всей стране. Среди них и новые современные предприятия, и старые лесосеки, созданные в прошлом веке и не тронутые цифровизацией. В связи с этим при расширении сети возникают проблемы не только с защитой внешнего периметра компании, но и внутренней структуры. Изначально компания устанавливала межсетевые экраны для каждой подсети, однако не понимала, что происходит внутри предприятия, где в общей сложности работают более семи тысяч рабочих станций сотрудников и серверов. В компании имелась иностранная SIEM, развернутая, но не настроенная. Она собирала до 10 тысяч событий неструктурированных данных в сутки. Хорошего специалиста найти не удалось, таким образом хаос множился.

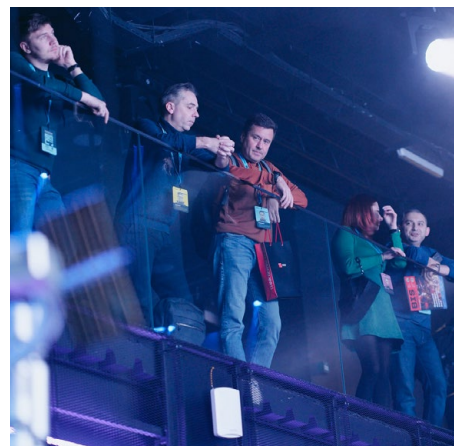
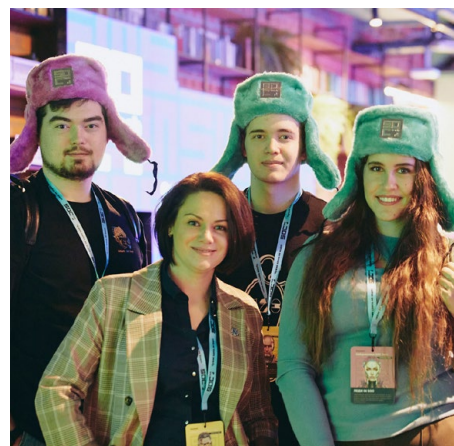
Выходом из ситуации стало обращение к внешнему провайдеру, который и обеспечил полную поддержку работы

SOC с учетом специфики работы компании. Как отметил докладчик, новая система была развернута за неделю. В результате заказчики получили информацию об инцидентах в структурированном виде с учетом приоритетов, налажился контроль процессов ИБ и выявление вредоносной активности. Закрываются критические уязвимости. Ведется мониторинг событий в режиме 24/7, что удобно с учетом работы в разных часовых поясах. Также компания подключилась к ГосСОПКА и передает туда информацию в соответствии с требованиями регулятора.

В планах компании — расширение систем мониторинга, интеграция с SOC систем обеспечения ИБ АСУ ТП, в первую очередь, КИИ... Компания расширяется, и такое решение позволяет быстро подключать филиалы к головной структуре.

АЛАВЕРДЫ ОТ ПОДРЯДЧИКА

Следующий докладчик Евгений Гуляев, R-Vision, рассмотрел другой опыт построения SOC — со стороны подрядчика. Согласно техническому заданию, организация со сложной структурой хотела в кратчайшие сроки обеспечить полноценный мониторинг и расследование инцидентов ИБ всей группы компаний, максимально вовлечь для этого ИТ-специалистов в филиалах и минимизировать трудозатраты в головной компании.





При первом запуске MSSP, аналитике и выдаче рекомендаций подрядчик столкнулся с тем, что 90 % времени было потрачено на определение зон ответственности в рамках разных структур заказчика. Поэтому были определены нюансы в работе дочерних компаний, механизмы взаимодействия, глубина детализации описания мероприятий по реагированию на инциденты и порядок внесения изменений в процесс реагирования.

Подрядчик использовал систему оркестрации, автоматизации и реагирования на инциденты безопасности (SOAR). По результатам работы был целиком автоматизирован наиболее трудоемкий участок с учетом зоны ответственности каждого филиала. Начались мониторинг и расследование инцидентов ИБ.

Механизм автоматизации удобен для масштабирования и расширяется на все структуры организации, включая многочисленные дочерние предприятия. Достигнута высокая скорость обработки инцидента с момента его выявления до момента начала реагирования. Сэкономлены немалые человеческие ресурсы,

снижены требования к компетенции сотрудников, эксплуатирующих систему. Всего два человека в головной организации обрабатывают более 120 инцидентов в день. Таким образом, все цели проекта достигнуты.

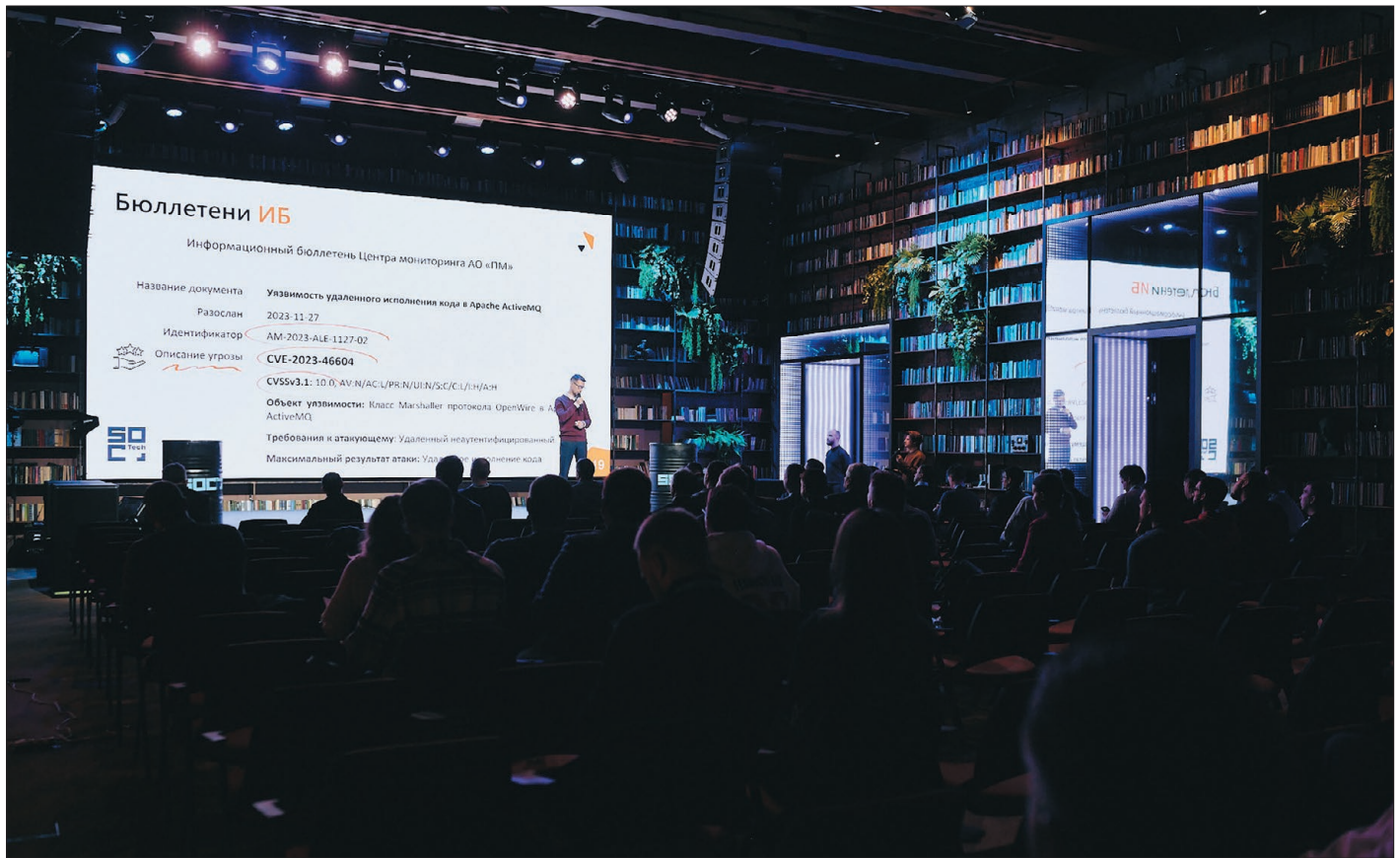
КОШКИ-МЫШКИ И ГЛОБАЛИЗАЦИЯ

О выстраивании процессов взаимодействия TI с EDR в объемах коммерческого SOC рассказал Константин Васильев, компания «РТ-Информационная безопасность», в докладе «Another brick in the SOC». Он представил принципиально новый подход и соответствующий ему продукт.

На определенной стадии SOC возникает вопрос: как интегрировать процессы мониторинга и реагирования с разведкой угроз! — начал докладчик. Он подчеркнул, что игра в «кошки-мышки» между атакующими и защитниками — бесконечный процесс, в ходе которого идет накопление знаний о действиях и тактиках атакующих. Чтобы эти знания работали, необходима единая точка экспертизы и пополнения базы данных актуальных угроз. Такой точкой К. Васильев видит TI-платформу,

которая представляет функционал по агрегации, корреляции и хранению данных о киберугрозах, а также обеспечению своевременности мер реагирования, плюс актуализации экспертизы. Основа реагирования — EDR, система обнаружения сложных угроз, обеспечивающая быстрое обнаружение вторжений, противодействие, сбор цифровых улик и тщательное расследование.

К. Васильев отметил, что решение предлагает пошаговое выстраивание процессов Threat Intelligence с опорой на EDR с возможностью интеграции с другими продуктами, журнализацией действий пользователей и пр. В результате SOC получает статистику обнаружений по организациям, возможность ретроспективного поиска по индикаторам компрометаций, а в итоге обнаружение множественных атак, пополнение аналитики и т.д. Такое решение позволяет построить зрелый SOC и обеспечить глобальную систему реагирования: обмен данными об угрозах в рамках отрасли, переход от реагирования в рамках ИБ-компаний к глобальному реагированию, в общем, Collective Defence Intelligence, включая прогнозирование.



ЗАЧЕМ ТЕБЕ ЭТО НАДО?

Завершил сессию Алексей Лукацкий, поведавший, от чего зависит выбор технологий для SOC. Он составил свой чек-лист на основе личного опыта участия в десятках проектов.

Спикер отметил, что сегодня при построении SOC классическая схема Gartner — связка EDR, SIEM, NDR/NTA — уже не актуальна. В некоторых сферах может потребоваться, например, UEBA/CASB или другие решения по хранению, обогащению данных, управлению знаниями, взаимодействию участников и т.д.

Эксперт подчеркнул: прежде чем выбирать технологии, надо сформулировать стратегию, определив, за-

чем строится SOC, какие сервисы и процессы нужны, есть ли для этого люди? И только после этого выбирать технологии, которые позволят решить поставленные задачи с учетом нюансов, касающихся импортозамещения, требований регуляторов, выбора между собственным SOC и аутсорсом. Только тщательный подход к мелочам позволит компании правильно построить центр мониторинга и не потратить деньги впустую, считает А. Лукацкий.

В КИБЕРУШАНКЕ НЕ ЗАМЕРЗНЕШЬ!

Между сессиями участники не только осмысливали доклады и налаживали

контакты, но и активно развлекались на киберполигоне, включавшем ИБ-стендап, подвижные квесты и интеллектуальные игры. В фотозоне ИИ без усталости создавал киберпортреты всех желающих. Перед таким соблазном не устоял практически никто.

Самые азартные киберзащитники, посетившие все стенды партнёров SOC Tech и верно ответившие на вопросы о представленных продуктах, получили фирменные призы организаторов. А по итогам дня спикеров, которых слушатели наградили наиболее громкими аплодисментами, наградили одним из символов конференции — яркой кибер-ушанкой с логотипом SOC Tech.

ЦИТАТА



Артем ЗУБКОВ
генеральный директор
Медиа Группы
«Авангард»,
организатор
SOC Tech 2023

«Команда «Авангарда» выражает искреннюю благодарность всем гостям и партнёрам за активное участие, «Кибердому» за содействие в проведении конференции, а спикерам и модераторам за невероятную энергию, пронизывающую каждое их выступление!

Ещё до завершения этого мероприятия мы поняли, что в 2024 году хотим порадовать отрасль ещё большими планами, ещё более захватывающими темами, новыми докладами и уникальными возможностями для общения и обмена опытом. До встречи на следующем SOC Tech!»

АНТИФРОД РОССИЯ 2023

ПРАВООХРАНИТЕЛЬНЫЕ ОРГАНЫ СТАНОВЯТСЯ АКТИВНЕЕ

Анна КАТАНКИНА
корреспондент BIS Journal

Важным событием в области борьбы с высокотехнологичным мошенничеством в прошлом году стал XIV Всероссийский форум «Антифрод Россия – 2023», собравший более 700 участников. Они подвели итоги 2023 года и обозначили планы на 2024-й.

ЗАКОНОДАТЕЛЬНЫЕ ИНИЦИАТИВЫ

Открывший пленарное заседание член Комитета Совета Федерации по конституционному законодательству и государственному строительству сенатор Артём Шейкин отметил, что осенью 2023 г. вступили в силу поправки к закону «О банках и банковской деятельности», а также ст. 27 Федерального закона «О национальной платёжной системе», которые направлены на совершенствование взаимодействия между Банком России и МВД РФ по вопросам возбуждения и расследования дел по фактам мошенничества при переводе средств получателям. Установлен новый порядок взаимодействия структур, существенно сокращены сроки ответов.

Генеральная прокуратура совместно с Роскомнадзором прорабатывает поправки в Закон «О связи». «Речь идёт об аннулировании лицензий операторов связи, это позволит решительно пресекать и привлекать к ответственности недобросовестных операторов, которые пропускают так называемые преступные звонки, понимая последствия этих звонков», — подчеркнул сенатор.

По новой схеме мошенничества злоумышленники вынуждают граждан оформлять кредиты и переводить средства на «безопасные счета». «Уверен, что при принятии соответствующих поправок количество мошеннических операций

с использованием телефона будет значительно ниже», — полагает А. Шейкин.

На рассмотрении в Госдуме находится законопроект, позволяющий гражданам устанавливать самозапрет на выдачу кредитов и займов. Он не распространится на ипотеку и автокредит, поскольку механизм оформления этих кредитов не предусматривает быстрого получения денег, подчеркнул председатель Комитета Госдумы по финансовому рынку Анатолий Аксаков. Предполагается, что закон заработает в 2024 г.

Готовятся изменения в закон о «Национальной платёжной системе», который обяжет кредитные организации сверять счета с базой данных Банка России о случаях и попытках осуществления переводов без согласия клиента — так называемой базой дропперов. В базе содержатся данные десятков тысяч сомнительных счетов, что позволит блокировать транзакции на счета мошенников, продолжил тему депутат А. Аксаков. Переводы будут «замораживать» на два дня с возможностью блокировать сомнительные транзакции. Также предусмотрены иные меры, которые помогут защитить граждан. Закон вступит в силу со второй половины 2024 г.

Несмотря на принимаемые меры, темпы роста преступлений в цифровой среде выросли более чем на 4 процента, отметил парламентарий. По данным Банка России, злоумышленниками было выведено со счетов больше 14 млрд рублей. «Граждане своими руками переводят деньги на счета злоумышленников», — подчеркнул депутат.

Ещё один законопроект введёт институт доверенных лиц для граждан пожилого возраста. Дети либо родственники должны будут подтвердить получение ими кредита или осуществление платежа в течение 12 часов. Если операция не подтверждена, она не должна быть совершена, подчеркнул А. Аксаков.

«У нас активно развивается крипто-рынок. Но, к сожалению, этот вопрос никак не удаётся отрегулировать, и эта сфера тоже становится сферой деятельности злоумышленников», — продолжил депутат. Хотя рынок криптовалют измеряется сотнями миллиардов рублей, многие вопросы не удаётся согласовать по причине противоречий между позициями Правительства РФ и Банка России. Для решения вопроса глава Комитета Госдумы готов создать рабочую группу для наведения порядка в сфере оборота и регулирования криптовалюты.

МИНЦИФРЫ

Повсеместное внедрение информационных технологий — неизбежная потребность, которая одновременно несёт риски мошенничества, отметил заместитель главы Минцифры Александр Шойтов. Комплексная борьба со злоумышленниками требует тесного взаимодействия уполномоченных федеральных органов исполнительной власти. Минцифры работает над тем, чтобы предупредить и сократить возможности мошенников по трём направлениям: борьба с подменой номеров и подменными сайтами, защита персональных данных.

Замглавы Минцифры заметил, что проблема защиты персональных данных — глобальная. Это сложная задача, и решается она всюду по-разному, но большие оборотные штрафы приняты во многих странах мира. При этом штрафы за утечки, действующие в России, не соответствуют масштабу утечек и потенциальному вреду, который они приносят.

А. Шойтов отметил, что ведомство поддерживает концепцию закона об оборотных штрафах, внесённого в Госдуму. Законопроект получил положительный отзыв Правительства РФ. Введение закона на фоне масштабных утечек, произошедших за последние два года, необходимо, полагает представитель регулятора.

Минцифры также противодействует распространению фрода и фишинга как на законодательном, так и на технологическом уровне. Для этого разработаны и функционируют платформы «Антифрод» и «Антифишинг». Развитие и поддержка этих платформ заложены в национальную программу «Цифровая экономика» и будут продолжены в новой программе «Экономика данных», рассчитанной на период 2025–2030 гг.

Оператором платформы «Антифишинг» является НИИ «Интеграл», подведомственный Минцифры. В 2022 г. система выявила 80 тыс. потенциальных фишинговых сайтов, 29 тысяч из них были направлены на блокировку в правоохранительные органы. За первое полугодие 2023 г. выявлено 144 тыс. потенциальных фишинговых сайтов.

О мошеннических звонках гражданам России могут сообщить на Госуслугах через форму обращения, отметил представитель Минцифры. Эти сообщения в ручном режиме обрабатываются совместно с операторами связи. Одновременно развивается платформа «Антифрод», запущенная Роскомнадзором и предназначенная для борьбы с телефонным мошенничеством. В 2022 г. платформа выявила 102 млн мошеннических звонков и 67 млн — за три квартала 2023 г. Операторы связи обязаны подключиться к ней до конца февраля 2024 года, что позволит автоматически блокировать номера в случае подмены.

БАНК РОССИИ

Вадим Уваров, директор Департамента информационной безопасности Банка России, как и сенатор Артём Шейкин, обратил внимание на вступление в силу 21 октября 2023 г. изменений в Федеральный закон «Об информации, информационных технологиях и защите информации», который регламентировал информационное взаимодействие с МВД РФ. «Это достаточно эффективный механизм с точки зрения получения информации по операциям без согласия», — считает В. Уваров. Поправки позволили представителям правоохранительных органов получать

информацию из базы данных Банка России по операциям без согласия клиентов. Представитель регулятора подчеркнул, что теперь в банковской сфере обсуждается инициатива, связанная с нюансами работы системы. Банки и МВД оттачивают механизм уведомления кредитной организации со стороны правоохранительных органов об операции без согласия, если такая есть, и взаимодействия банка с пострадавшим. По мнению В. Уварова, сходимость информации в базе и обращениями граждан со временем выровняется и представители Банка России и МВД будут работать в едином информационном пространстве.

За 9 месяцев 2023 г. согласно статистике Банка России об операциях без согласия клиентов были похищены порядка 11 млрд рублей. По сравнению с данными прошлого года объём хищений вырос на 16 %, число мошеннических операций увеличилось на 17 %, было совершено 820 тысяч операций без согласия клиентов. «Это большая цифра и по объёму денежных средств, и по количеству денег», — подчеркнул В. Уваров. Основной канал хищения денег — операции, совершаемые по счетам и картам граждан, это 80 % от всего объёма хищений. У юридических лиц в основном похищают денежные средства с использованием счетов, этот тренд имеет определённую тенденцию и отслеживается регулятором, отметил представитель Банка России.

В абсолютных цифрах за указанный период регулятор зафиксировал 20 млн попыток снятия средств без согласия клиентов, общая сумма предотвращённых хищений составила 3,3 трлн рублей. Это говорит об эффективности антифрод-процедур Банка России и финансовых организаций, отметил В. Уваров.

Банк России принял «Стратегию развития информационной безопасности на 2023–2025 гг.» Большое внимание уделено вопросам предупреждения мошеннических операций, разработке законодательных инициатив, направленных на защиту счетов граждан. По мнению регулятора, вступление в силу с 25 июля 2025 г. поправок в Федеральный закон

«О национальной платёжной системе», о которых говорили представители Федерального Собрания, должно кардинально изменить ситуацию в подходе банков к операциям без согласия клиентов и возмещению средств.

«Мы понимаем, что злоумышленники постоянно совершенствуют свои атаки. И поэтому постоянно находимся в диалоге с финансовыми организациями с точки зрения эффективности работы антифрод-систем», — завершил выступление представитель Банка России.

МВД РОССИИ

О начале работы Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России рассказал Максим Толкачёв, заместитель начальника Управления. Он отметил, что уже ведётся активная оперативно-разыскная работа в отношении владельцев так называемых Sim-боксов, которые позволяют проводить активацию карт и осуществлять обзвон со граждан с территории иностранных государств. При взаимодействии с Банком России и Минцифры проводятся мероприятия и готовятся, в частности, нормативно-правовые акты, которые позволят эффективно бороться с телефонными мошенниками. Отдельное внимание Управление уделяет профилактике преступлений с использованием социальной инженерии, поскольку граждане должны понимать, с кем они говорят, какие сведения готовы передать.

Представитель Следственного комитета РФ Михаил Муранов обратил внимание на необходимость повышения грамотности населения. Он углубился в историю развития информационных технологий. Технология Web 2.0 позволяет пользователям взаимодействовать, но при этом не даёт возможность контролировать свои данные, а компании и организации получают возможность использовать эти данные в своих целях, например, для таргетированной рекламы. Дальнейшее развитие — технология Web 3.0 — приводит к децентрализации ресурсов и данных, их хранению

на устройствах пользователей, развитию криптовалютных расчётов и технологий искусственного интеллекта. Анонимизирующие схемы становятся доступны широкому кругу лиц. Применение моделей генеративного и интерактивного ИИ приводит к созданию дипфейков и иного контента, который может быть использован в преступных целях. Интернет будет развиваться своим путём, противостоять этому невозможно, нужно прогнозировать витки развития этих технологий, считает представитель СК России.

ДИСКУССИЯ

В рамках дискуссии «Нормативно-правовое регулирование в сфере антифрода» Андрей Воробьёв, представитель АНО «Координационный центр доменов.RU/.RF», продолжил поднятую на пленарном заседании тему фишинга. Он отметил рост числа фишинговых атак в зонах.RU/.RF. За 10 месяцев прошлого года рост составил 173 % по сравнению с прошлым годом. Изменение их типа — это не только выуживание данных и денег, а подделка сайтов СМИ и госорганов для ведения контрпропаганды, госфишинг, скрытый фишинг... Для борьбы с фишинговыми сайтами активно используются инструменты и механизмы саморегулирования при блокировке таких ресурсов в национальных доменных зонах.RU/.RF. Время реакции на фишинговые ресурсы с использованием механизмов саморегулирования составляет от 1,5 до нескольких дней. При реагировании через уполномоченные организации время снизилось с 22,5 часа до нескольких часов, особенно активно работает взаимодействие с НКЦКИ. В международных зонах регистраторы и близко не подошли к такой скорости, отметил представитель координационного центра. Споры при снятии с регистрации — единичные на множество блокировок. При этом существует правовой пробел при саморегулировании, когда домен блокируется без извещения правоохранительных органов и злоумышленники остаются вне поля зрения компетентных органов.

Есть также проблема в терминологии, например, понятие «фишинг» не входит в состав УК РФ, правоохранительные органы квалифицируют его как «мошенничество» (ст. 159 УК РФ). Законопроект, ликвидирующий эти пробелы, находится в процессе согласования.

М. Муранов отметил активное вовлечение подростков в занятия преступной деятельностью в сфере информационно-коммуникационных технологий. Точка входа в создание фишинговых сетей — 15–16 лет. Однако в результате длительного межведомственного взаимодействия с органами прокуратуры в части определения подследственности дел с участием несовершеннолетних теряется время и оперативность отработки таких преступлений, отметил представитель СК.

Второй момент — высокая латентность преступлений. Многие пострадавшие не заявляют о преступлении. Влияет также слабое нормативно-правовое регулирование и трансграничность киберпреступлений. Структуры СК РФ ведут собственную базу следов и идентификаторов, так как многие рассматриваемые дела пересекаются, а злоумышленники находятся за границей. В этой части необходимо взаимодействие с компаниями и организациями, ведущими аналогичный сбор информации как в России, так и в дружественных странах.

ОПЫТ РЕСПУБЛИКИ БЕЛАРУСЬ

Опытом работы Главного управления цифрового развития СК Республики Беларусь поделился Сергей Гамко, возглавляющий подразделение, отвечающее за расследование преступлений в цифровой сфере. Он отметил, что в подразделении есть специалисты, которые отвечают за вопросы мониторинга фишинговых ресурсов, их выявление и направление информации для блокировки. Цепочка «генпрокуратура — регистратор — чёрный список операторов» отрабатывается в срок до 3 ч. На сайте МВД РБ ведётся перечень скомпрометированных ресурсов.

Отдельный вопрос — работа с дропами и их счетами. Совместными

усилиями правоохранительных органов и законодателей в Уголовный кодекс РБ введена уголовная ответственность за незаконный оборот средств платежа и инструментов. Наказание предусматривает крупный штраф или ограничение свободы на срок от 2 до 6 лет. За повторные нарушения, особо крупный размер хищений или участие в организованной преступной группировке предусмотрено наказание до 10 лет лишения свободы. Практика показала действенное противодействие дропам, отметил С. Гамко.

Он также поделился опытом работы с криптовалютами, легализация оборота которых введена Декретом № 8 Президента РБ в декабре 2017 г. Документ ввёл понятийный аппарат, который даёт правоохранителям возможность действий, документации и сохранения цифровых активов на холодных кошельках. Ведётся Единый реестр скомпрометированных криптокошельков.

Декрет позволяет гражданам открывать и вести криптосчета, проводить разовые сделки с криптовалютой. Если действия физических лиц носят системный характер, отмечено значительное число транзакций и привлечение третьих лиц, но при этом человек не регистрируется как оператор, он попадает в поле зрения правоохранительных органов.

* * *

Участники регуляторного трека отметили, что важным вопросом является не только противодействие, но и предупреждение преступных действий. И здесь возникают сложности и проблемы с регулированием. Есть технические и научные способы определения фишингового ресурса при нейминге. Однако уполномоченным организациям нужна единая база и активное взаимодействие участников рынка. Важны вопросы доверия, сотрудничество научно-технической сферы и готовность взаимодействия всех заинтересованных сторон, диалог правоохранителей и регуляторов, отметили участники дискуссии.

НАЦИОНАЛЬНЫЙ ПРОЕКТ «ЭКОНОМИКА ДАННЫХ»

ПРИДЁТ НА СМЕНУ НАЦИОНАЛЬНОМУ ПРОЕКТУ
«ЦИФРОВАЯ ЭКОНОМИКА» (2019–2024)



Марина
БРОДСКАЯ,
обозреватель
BIS Journal

Национальный проект «Экономика данных» придёт на смену национальной программе «Цифровая экономика РФ» и охватит различные области экономики и общественной жизни. Цель нацпроекта — перевести экономику страны, органы власти всех уровней и социальную сферу на новые принципы работы, внедрить управление на основе данных. Проект затронет такие сферы и отрасли, как образование, медицина, безопасность, промышленность, ЖКХ, развитие транспорта, связь, интернет и т.д.

ДОРОЖНАЯ КАРТА

Нацпроект возник по инициативе Президента РФ В. В. Путина. Летом прошлого года глава государства посетил Форум будущих технологий. По его итогам президент поручил Правительству РФ обеспечить утверждение национального проекта по формированию экономики данных на период до 2030 г. Он должен предусматривать создание инфраструктуры вычисления и хранения данных с использованием отечественного оборудования, технологий и программного обеспечения, в том числе облачных платформ, центров обработки данных и вычислительных мощностей. В проект должны быть также заложены:

- ♦ сбор данных, в том числе с использованием высокочувствительных датчиков на основе квантовых сенсоров;

- ♦ передача данных и развитие систем связи нового поколения;

- ♦ обеспечение безопасности данных, в том числе с использованием технологий квантового шифрования;

- ♦ совершенствование отечественных стандартов и протоколов работы с данными;

- ♦ разработка алгоритмов обработки и анализа данных, в том числе основанных на использовании искусственного интеллекта (ИИ);

- ♦ создание отечественных хранилищ кода (платформ и сервисов), необходимых для совместной работы российских и иностранных программистов.

В рамках формирования нацпроекта необходимо предусмотреть инструменты комплексной поддержки развития цифровой экономики, ИИ, квантовых вычислений и коммуникаций, а также фундаментальных исследований в сфере вычислительных технологий, говорится в поручении президента России. Необходимо также обеспечить преемственность ранее действовавших программ, в том числе в рамках национальной программы «Цифровая экономика», научно-технологических заделов и предусмотреть необходимое финансирование этих направлений в целях бесперебойной деятельности научных коллективов и лабораторий. Также правительству поручено определить источники и ежегодный объём финансирования нацпроекта, в том числе за счёт средств федерального бюджета.

Плановые параметры нацпроекта «Экономика данных», рассчитанного на 2025–2030 гг., планируется

утвердить до 1 июня 2024 г., сообщил позднее министр цифрового развития РФ М. Шадаев. Финансирование проекта будет осуществляться как за счёт бюджетных средств, в том числе путём перераспределения расходов на другие госпрограммы и иных доходов, полученных за счёт роста тарифов и штрафов, акцизных сборов и налогов, так и за счёт коммерциализации систем «Электронного правительства». Дополнительные источники финансирования позволят инвестировать в реализацию нацпроекта более 80 млрд руб. ежегодно. Эти данные глава Минцифры привёл в рамках презентации на стратегической сессии Правительства России, посвящённой формированию нового нацпроекта. Всего на реализацию «Экономики данных» потребуется более 1,5 трлн руб., писали «Ведомости».

В нацпроект «Экономика данных» войдут 10 федеральных проектов: «Цифровая инфраструктура», «Искусственный интеллект», «Цифровые платформы в госуправлении», «Системы и сети передачи данных», «Кадры», «Инфраструктура вычислений и облачных сервисов», «Отечественные решения в сфере ИТ», «Развитие квантовых технологий», «Кибербезопасность» и «Наука». На первые три направления, согласно презентации, планируется суммарно потратить более 1 трлн руб., при этом на первые два проекта придётся почти половина бюджета нацпроекта.

По данным «Ведомостей», самыми дорогими мероприятиями нового нацпроекта станут внедрение облачной платформы «ГосТех» (142 млрд руб.), создание цифровой инфраструктуры образовательных учреждений (129 млрд руб.), развитие группировки спутниковой

связи ГПКС (80 млрд руб.) и платформы «Госуслуги» (78 млрд руб.). Распределять финансирование планируется путём выделения субсидий, заключения контрактов, межбюджетных трансфертов, предоставления грантов и льготных кредитов.

Согласно дорожной карте подготовки проекта, до 15 марта должны быть подготовлены финансово-экономические обоснования реализации программ.

В рамках подготовки проекта предстоит проработать многочисленные вопросы.

- ◆ К 16 февраля Росстату, Минцифры и Минэкономразвития (МЭР) необходимо разработать стандарты качества данных. В числе задач — подготовка классификатора для обеспечения унификации данных для различных отраслей экономики.

- ◆ К 20 февраля Минцифры поручено сформировать и представить Правительству РФ отраслевую карту существующих и планируемых к созданию государственных и коммерческих цифровых платформ.

- ◆ До 19 марта Минцифры должен обеспечить проработку мероприятий по выявлению недостоверных данных, в том числе генерируемых с использованием ИИ.

- ◆ В эти же сроки Минцифры вместе с межведомственными рабочими группами необходимо предусмотреть мероприятия по разработке и производству отечественного оборудования для сетей передачи данных, оценке необходимых и достаточных параметров вычислительных мощностей, формированию рынка данных, правил доступа к ним и обмена данными.

- ◆ К 28 марта должны быть разработаны и внесены в правительство паспорта федеральных проектов, которые войдут в нацпроект. Эта работа поручена Минцифры, МЭР и Минфину при участии АНО «Цифровая экономика», экспертного сообщества и представителей отраслевых предприятий, профильных министерств и ведомств.

- ◆ К этой же дате Минцифры должны подготовить план нормативного правового обеспечения реализации

нового нацпроекта на 2024–2026 гг. В работе над планом примут участие МЭР и АНО «Цифровая экономика».

- ◆ До 17 апреля Минцифры и Минэкономразвития должны разработать стимулирующие меры поддержки участников рынка, направленные на повышение качества данных и их востребованности. Эти меры войдут в Цифровой кодекс РФ, который создаётся для обеспечения комплексного регулирования развития и использования ИТ- и инфраструктуры связи в РФ.

- ◆ До 30 апреля нацпроект должен быть внесён на рассмотрение в правительство.

- ◆ До 1 июля, согласно поручению президента России, финальный вариант нацпроекта должен быть уже готов.

- ◆ До 1 сентября заинтересованными ведомствами должен быть подготовлен план законодательного регулирования, необходимого для реализации нацпроекта.

ИИ: ОПЕРЕЖАЮЩЕЕ РАЗВИТИЕ

Федеральный проект по развитию искусственного интеллекта станет частью нового нацпроекта «Экономика данных». Отвечать за него будет Минэкономразвития. По итогам стратегической сессии, посвящённой развитию ИИ, глава Правительства РФ М. Мишустин поручил МЭР, Минцифры и Минфину определить перечень показателей нацпроекта в части развития ИИ с расчётом их плановых значений по годам и необходимое финансирование, включая средства федерального бюджета и внебюджетных источников. Эта работа должна быть завершена к 15 апреля.

Проект по развитию ИИ будет сформирован на базе и с учётом обновлённой «Национальной стратегии развития искусственного интеллекта на период до 2030 года», которая была утверждена Указом Президента РФ в 2019 г. и является основным документом, направленным на развитие и внедрение отечественных решений ИИ, формирующих внедрение инноваций во все сферы экономики и жизни граждан.

Выступая на стратегической сессии, посвящённой ИИ, М. Мишустин отметил возросшую роль продуктов на основе ИИ в экономике страны и необходимость вывода их на качественно новый уровень. Он подчеркнул важность создания отечественных моделей ИИ и обеспечение независимости от иностранных поставщиков, укрепления безопасности России.

В целях повышения уровня внедрения ИИ в отраслях экономики Минцифры предстоит:

- ◆ до 1 апреля обеспечить создание доступной для органов власти платформы по искусственному интеллекту на базе единой цифровой платформы «ГосТех»;

- ◆ до 20 декабря проработать создание отечественных инструментов (сервисов) обработки данных, использующих технологии ИИ для обогащения и разметки набора данных;

- ◆ до 15 февраля в рамках национального проекта «Здравоохранение» Минздраву, Минфину и МЭР требуется обеспечить формирование необходимой системы управления реализацией мероприятий по внедрению ИИ в сфере здравоохранения; с 2025 г. Минздраву и Минфину поручено предусмотреть финансирование внедрения решений с ИИ при формировании нового федерального проекта «Цифровые сервисы здравоохранения»;

- ◆ к 15 февраля Минэнерго, МЭР, Минцифры и Минфин должны представить в Правительство РФ предложения и проработать вопросы льготного технического присоединения к электрическим сетям новых специализированных центров обработки данных и предоставления льготных тарифов на электроэнергию для таких ЦОД;

- ◆ до 1 марта Минобрнауки, МЭР, Минцифры и РАН совместно с профильными исследовательскими центрами поручено сформировать подходы по определению приоритетных направлений научных исследований и механизмов поддержки проведения прорывных фундаментальных и прикладных научных исследований и их включению в действующие инструменты господдержки научной

деятельности; эти меры будут направлены на обеспечение опережающего развития ИИ;

- ♦ до 30 марта Минобрнауки и МЭР предстоит обеспечить разработку учебных программ для вузов по подготовке высококвалифицированных специалистов в сфере ИИ; обеспечить реализацию этих программ и привлечь в учебные заведения в качестве научно-педагогических кадров специалистов из организаций в сфере ИИ поручено Минобрнауки;

- ♦ также до 30 марта Минпромторгу и МЭР поручено обеспечить деятельность Федерального центра прикладного развития искусственного интеллекта для повышения доступности инфраструктуры, необходимой для решения задач в области ИИ; работа будет идти в рамках госпрограммы «Развитие промышленности и повышение её конкурентоспособности»; ожидается, что эти меры будут способствовать повышению уровня внедрения ИИ в отраслях промышленности;

- ♦ до 15 апреля в целях стимулирования развития научной деятельности Минобрнауки, Минэкономразвития и Минфин должны представить в правительство предложения по учреждению в России единовременной премии за решение математических «задач тысячелетия»;

- ♦ до 1 июня в целях развития кадрового потенциала для массового внедрения технологий ИИ Минобрнауки, Минпросвещения, Минэкономразвития должны представить в правительство предложения о запуске национальной инициативы подготовки кадров на всех уровнях образования, а также переподготовке исследователей с целью их обучения методам применения технологий ИИ в научной деятельности;

- ♦ в рамках проведения мониторинга рисков социально-экономического развития России Минэкономразвития и Минтруд поручено обеспечить ежегодный анализ и оценку рисков, связанных с внедрением технологий ИИ в отраслях экономики и социальной сферы, в том числе его влияния на состояние рынка труда.

О БЕЗОПАСНОСТИ

В рамках федерального проекта «Кибербезопасность» до 2030 г. Минцифры намерено инвестировать около 25,2 млрд руб. (данные по состоянию на ноябрь 2023 г.). 7,1 млрд руб. планируется направить на развитие новой системы противодействия компьютерным атакам «Мультисканер» на базе ГосСОПКА. На развитие госсистем «Антифрод» и «Антифишинг» пойдёт 3,7 млрд руб., а на внешнюю оценку защищённости ключевых ГИС — 2,4 млрд руб. Ещё 12 млрд руб. направят на системы обеспечения кибербезопасности (криптография, средства защиты и пр.), писал «Коммерсант» по итогам ноябрьской стратегической сессии.

По оценке Минцифры, в результате реализации проекта «Кибербезопасность», к 2030 г. пройдёт импортозамещение иностранных средств защиты российскими аналогами. Система «Мультисканер» (аналог американского сервиса VirusTotal) сможет обрабатывать более 90 млн файлов в год, а число инцидентов, связанных с нарушениями безопасности ключевых ГИС, снизится до нуля. Разработкой системы «Мультисканер» занимается Национальный технологический центр цифровой криптографии (НТЦ ЦК). Прототип системы должны были запустить до конца прошлого года. В 2024 г. планируется дополнить систему новыми функциями, а после 2025 г. она заработает в полную силу, сообщал ранее замглавы Минцифры А. Шойтов.

ПРОСТЫМИ СЛОВАМИ

В ноябре 2023 г. в Санкт-Петербурге прошёл III Международный форум кибербезопасности государства «ЦИФРОТЕХ». В рамках пленарной дискуссии А. Шойтов подробно рассказал о концепции нового национального проекта «Экономика данных».

Цель проекта — «новый уклад экономики, основанный на обработке данных», включающий весь жизненный цикл работы с данными: сбор (IoT) и передача данных (сети), числители и работа с данными, хранение данных (центры обработки

данных), платформы обработки данных, методы обработки данных, в первую очередь ИИ. Это основные отраслевые направления, отметил спикер. Также в проекте закладываются сквозные направления — наука, кадры, нормативное регулирование и непосредственно вопросы ИБ всех элементов этого проекта. Проект формируется и обсуждается на уровне правительства и всех заинтересованных ведомств.

В стране в целом система ИБ построена, что не раз отмечалось и продемонстрировано в последние два года, подчеркнул замглавы Минцифры. Кибербезопасность будет заложена в основу новых перспективных технологий и максимально быстро внедрена. В текущей версии нацпроекта на 2025–2030 гг. закладываются меры ИБ (подход *secure-by-design*) на каждом этапе жизненного цикла данных. Так, для IoT планируется внедрение криптозащиты и принципа *secure-by-design* при разработке ПО, а также внедрение механизмов ИБ на уровне датчиков.

А. Шойтов отметил, что ИБ — комплексное мероприятие, его ключевые направления будут наследованы из старой программы «Цифровая экономика», также добавятся новые методы — информационная безопасность самих технологий на ранней стадии. Отвечая на вопросы о мерах по защите информационных систем органов власти различного уровня, А. Шойтов подчеркнул, что кардинально решить вопрос кибербезопасности может перевод систем на платформу «ГосТех». Государство в лице регуляторов и не только подключилось к обеспечению ИБ системы, и реализованы три линии защиты:

- ♦ комплексная система защиты информации;

- ♦ безопасная разработка защиты ПО;

- ♦ многоуровневая система мониторинга и реагирования на кибератаки.

Представитель Минцифры призвал все региональные органы власти переходить на «ГосТех», поскольку, кроме экономической эффективности, платформа надёжно защищена от компьютерных атак.



НОВАЯ ТЕХНОЛОГИЯ УДАЛЕННОЙ РАБОТЫ

ЧТО ТАКОЕ ZTNA И КАК С НИМ СВЯЗАНЫ VPN, ZERO TRUST, NAC, NGFW, SASE И SDP



Денис
БАТРАНКОВ
эксперт
BIS Journal

Хочу рассказать о самом современном способе удалённого подключения ваших сотрудников — о Zero Trust Network Access, сокращённо ZTNA. Если разделить это словосочетание на две части — Zero Trust и Network Access, станет понятно, что это одна из разновидностей удалённого доступа к вашей сети, такая же, как и VPN. У технологии

ZTNA такие грандиозные функции, что я рекомендую руководителям компаний направить своих сотрудников на её изучение или сразу нанять тех, кто в ней разбирается.

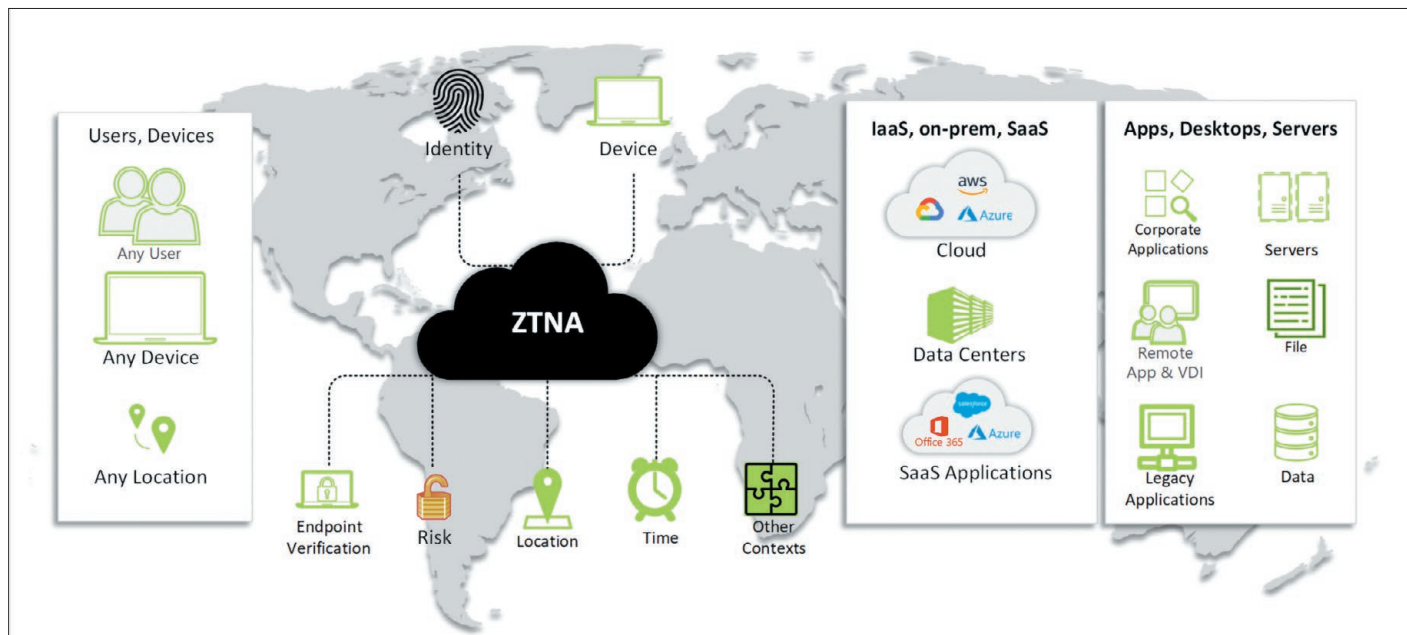
Чтобы дать полную картину, нужно рассказать про VPN, Zero Trust, NAC, NGFW, SASE и Software — Defined Perimeter (SDP). В конце этой статьи вы уже будете понимать, какой общей нитью связаны все эти термины. Хотя, собственно, зачем тянуть: эта нить — снижение рисков взлома вашей компании.

НАЧНЁМ С VPN...

VPN — это сокращение от Virtual Private Networks. Если перевести на русский — виртуальные частные сети. Уже из названия понятно, что основная идея заключается

в создании собственной приватной сети поверх публичной сети Интернет. Цель — предоставить защищённый доступ к информации только доверенным лицам и устройствам через сеть Интернет. При этом мы хотим гарантировать конфиденциальность обрабатываемой, передаваемой и хранимой информации. Изначально VPN предназначался для объединения сетей вашей компании в различных точках страны или мира. Основывается VPN на работе семейства протоколов IPSEC между специальными шлюзами, установленными в каждом офисе компании. И такие подключения называются site-to-site VPN.

Есть вторая разновидность — удалённое подключение отдельных сотрудников к сети вашей компании. Этот тип подключения по-английски



так и называется — Remote Access VPN. Он нужен в том случае, если вашим сотрудникам приходится (или хочется) работать из дома, аэропорта, кафе или отеля. Чтобы организовать удалённое подключение, нужны два компонента: клиент и сервер VPN. Таким образом, удалённый доступ сотрудников к сети компании предоставляет специальный клиент VPN, который устанавливается непосредственно на вашу операционную систему: Windows, MacOS, Linux или Android.

Ещё можно использовать встроенный в операционную систему VPN-клиент. В частности, такой клиент есть у Open VPN, у Cisco он называется AnyConnect, у Palo Alto Networks — GlobalProtect.

Работает это следующим образом: клиент VPN подключается к шлюзу VPN вашей компании, и все данные передаются в обе стороны в зашифрованном виде, чтобы гарантировать защиту от их прослушивания и подмены. Замечу, сегодня работа с включённым VPN-клиентом — это рекомендованный режим работы для работы с конфиденциальной информацией в публичных сетях, например, если вы подключились к публичному Wi-Fi в кафе или к гостевому Wi-Fi вашего офиса. Везде ваш трафик хотят прослушать хакеры, поэтому пользуйтесь VPN, чтобы не оставлять им ни одного шанса.

Сейчас для подключения к шлюзу VPN-сети стали использовать

протокол TLS. Он позволяет избежать установки отдельного клиента, потому что клиентом является установленный у вас браузер. Вы заходите с помощью браузера в сеть своей компании через специальный шлюз TLS VPN.

Для аутентификации сотрудников и устройств в сетях VPN чаще всего используются пароли и сертификаты. В компаниях с высоким уровнем зрелости применяется двухфакторная аутентификация, например на основе одноразовых паролей и даже аппаратных токенов.

Подведём итог: Remote Access VPN предполагает наличие программных клиентов VPN, установленных на операционной системе ноутбука или смартфона и заранее подготовленных центральных шлюзов VPN, установленных на серверах компании, к которым эти клиенты VPN подключаются. Поверх созданного виртуального зашифрованного соединения между вашим компьютером или смартфоном передаются данные. Чаще всего основным алгоритмом шифрования является алгоритм AES с 256-битным ключом, в России — алгоритм ГОСТ.

ПЕРЕХОДИМ К ZERO TRUST

Разберемся как Zero Trust связан с NGFW, и заодно вспомним NAC.

В последние годы новой концепцией стал принцип нулевого доверия, по-английски Zero Trust. Здесь прослеживается аналогия с принципом

минимальных привилегий, когда мы даём доступ ровно к той информации, которая сотруднику положена по работе, — и ничего лишнего. Этой концепции оказалось недостаточно — сейчас появилась новая угроза: от имени аккаунта сотрудника на его же компьютере спокойно может работать злоумышленник, причём уже внутри вашей сети. Поэтому, по мнению Джона Киндервага, изобретателя концепции Zero Trust, сегодня к действиям любого пользователя нужно относиться с подозрением и вводить дополнительные проверки. Для удалённых подключений чаще всего проверяется информация о местоположении сотрудника и о настройках его рабочего места. Для внутренних подключений сотрудников ещё и рекомендуются средства контроля их поведения и выявления аномалий, часто это класс продуктов NTA или UEBA.

Сегодня также проверяется, верно ли работает приложение, к которому человек получил доступ.

Именно в этом разница Zero Trust и принципа минимальных привилегий: мы непрерывно контролируем, что доступ до сих пор находится у того самого человека и к тому самому приложению.

Опишу всё на примерах. Допустим, ваша сеть сегментирована. Обычно в любой компании администраторы и их компьютеры находятся в одном

сегменте, а прикладные сервисы — в другом. И вашим администраторам требуется подключаться к сети управления вашей компании, чтобы настраивать в ней различные сервисы. Политику доступа на эти сервера можно прописать тремя вариантами.

1-й вариант: политика доступа на самих серверах. Обычно это проверка логина и пароля на SSH- или RDP-сервисах и последующая выдача нужных прав доступа. Так вы обычно проходите в самолёт: стюардессы проверяют ваш посадочный талон и отправляют вас либо в эконом-, либо в бизнес-класс. Этот процесс называется авторизация.

2-й вариант: политика на сетевом оборудовании вашей компании. Обычно здесь архитекторы по безопасности применяют решения класса Network Access Control, или NAC. Устройства NAC дают вам доступ к какому-то конкретному сегменту сети, который выделяется при помощи технологии VLAN или обычной маски подсети. Само сетевое оборудование даёт доступ к нужному сегменту. Похожим образом в аэропортах вы проходите все контроли и получаете доступ в терминал. Заметьте, там у вас есть доступ ко всем выходам на посадку. Билет у вас, допустим, в Хабаровск, а вы можете пройти на рейс в Сочи. К счастью, здесь на вырубку поспевает контроль доступа согласно первому варианту.

3-й вариант: политика доступа на межсетевом экране, разделяющем сеть администраторов и сеть управления. И тут появляется термин Zero Trust. Межсетевые экраны бывают нескольких типов и даже поколений. Если у вас межсетевой экран нового поколения, по-английски Next Generation Firewall (NGFW), то в нём одновременно работает множество интеллектуальных модулей, которые получают дополнительную информацию по каждому подключению в сеть. И поэтому Zero Trust обогащает новыми проверками наши старые политики доступа, реализованные на старых межсетевых экранах, как и было со времён царя Гороха. **Самое важное, что в правилах доступа стало**

больше критериев. И называем мы этот новый вид контроля доступа Zero Trust, чтобы как-то отличать обычные старые правила по IP-адресам и портам от новых видов правил.

Какие же это новые критерии? Например, страна. Вы можете разрешить подключение только из России. Иными словами, если ваш админ будет подключаться к вашему VPN-шлюзу из Америки, к нему возникнут вопросы: «А чей-то он там делает?»

Второй пример: новым критерием правил NGFW стало конкретное приложение, к которому вы даёте доступ. Чуть-чуть расшифрую: вы даёте доступ не к порту tcp 3306, а к приложению MySQL, которое там работает. Если вдруг NGFW увидит, что там ходит другой трафик, опять появляются вопросы к админу: «Почему ты другой сервис повесил на этот порт?» Вот тут-то и проявляется отличие от принципа минимальных привилегий: мы не просто даём админу минимально точные доступы, мы проверяем, что тот сервис, к которому мы дали этот доступ, является тем самым сервисом, т.е. проверяем и админа, и сам сервис. Именно это считается высшим пилотажем в сегодняшнем мире информационной безопасности. Пользуйтесь Zero Trust!

Дополню третьим примером. Ещё одним критерием Zero Trust в современных NGFW будет проверка файлов. Если ваш сотрудник имеет доступ к файловому серверу компании и пытается выложить туда вредоносный код, хорошо бы проверять, какие файлы передаются туда и обратно, а идеально — не просто проверять их антивирусными сигнатурами, а помещать файлы в «песочницу», которая сможет выявить неизвестные ранее вредоносные файлы.

Здесь есть ещё одна важная вещь: для получения дополнительной информации о состоянии хоста на нём лучше иметь специальную программу-агент, которая бы собирала нужную информацию, перед тем как выдать доступ. Часть поставщиков использует сбор информации без

агентов. Но, как правило, они не могут собрать столько же дополнительного контекста о подключении, как это может сделать агент на самом хосте. Такие агенты используются для реализации и NAC, и для Zero-Trust-доступа. Просматривается устойчивый тренд, что такие агенты сбора информации совмещают с клиентами VPN.

Часто спрашивают о разнице между Zero Trust на NGFW и NAC. Ключевое отличие: NGFW представляет доступ на уровне приложений, а NAC — на сетевом уровне. Иначе говоря, если NAC даст доступ в сегмент заражённому устройству, все устройства в том сегменте будут под угрозой. Использование NGFW устраняет этот риск.

Если продолжить аналогию с аэропортом, NAC даёт доступ ко всему терминалу и ко всем выходам, а NGFW — к конкретному выходу на самолёт.

ОБЪЕДИНЯЕМ VPN И ZERO TRUST, ПОЛУЧАЕМ ZTNA

Если раньше по VPN в сеть компании подключалось пять ответственных за информационную безопасность сотрудников, то сегодня — вся компания, а в ней может работать 10 000 сотрудников. И уровень ответственности большинства из них, простите, я оцениваю как нулевой.

Если безответственный человек подключается по VPN, может проიзойти всё что угодно: с его компьютера могут быть организованы атаки на компанию, на его компьютер может быть скачано что угодно и т.д. Поэтому следующим этапом развития информационной безопасности в организации стала проверка, а что же сейчас установлено и как оно настроено на компьютере или смартфоне сотрудника, который подключается к нам по VPN.

Должны быть требования необходимого минимума средств защиты и настроек для каждой операционной системы. Например, во многих организациях удалённый доступ разрешается только с устройств, где как минимум стоит антивирус с последними базами и загружены все обновления операционной системы,

некоторым нужна системы защиты от утечек информации (DLP).

А что делать, если всего этого у человека нет? Ответ простой: не пускать, пока все требования политики не будут выполнены. Да, ещё нужно этому человеку рассказать, как эти требования выполнить: откуда скачать антивирус или EDR, как установить все обновления и т.д.

Если вам требуется управлять установкой софта и его настройками удалённо, применяйте решение класса Mobile Device Management (MDM).

Итак, система, которая даёт доступ вашим сотрудникам к сети удалённо, одновременно проверяя состояние этого устройства и постоянно контролируя его работу, называется Zero Trust Network Access. По сути, это набор вышеописанных технологий.

У компании Cisco данная функциональность встроена в клиент VPN под названием AnyConnect, она собирает информацию о хосте, которая у них называется posture.

У компании Palo Alto Networks данную функцию сбора информации о хосте тоже выполняет VPN-клиент — GlobalProtect; он собирает всё в файл в формате XML и отправляет на проверку на NGFW. Эта функция называется Host Information Profile.

У компании Fortinet данную функцию выполняет их хостовая защита EDR. Она собирает информацию о хосте и отправляет её на шлюз безопасности для проверки.

У компании Positive Technologies данную функцию проверки состояния хоста выполняет MaxPatrol EDR, он не даёт подключиться по VPN к сети, пока не будут выполнены все требования политики безопасности компании.

После того как вы подключились данными клиентами в сеть, вы уже можете работать с необходимым вам приложением, например RDP или SSH.

Часть поставщиков реализует доступ к внутренним приложениям через обратный HTTPS-прокси. Вы заходите на портал с помощью браузера и после аутентификации получаете доступ к заранее опубликованным приложениям, которые видны прямо из браузера. В этом случае клиент

VPN не нужен. Получается, что и клиент RDP или SSH не нужен — вы работаете непосредственно из своего браузера. Такая реализация раньше часто использовалась в Microsoft TMG для публикации доступа к Outlook Web Access (OWA). А сегодня обратный прокси либо встраивают в NGFW, либо продают отдельно.

Прошу заметить, что вышеперечисленным технологиям ещё требуется внешний сервис, который хранит списки пользователей и проверяет их пароли или второй фактор. Часто для этого используются сервисы Microsoft Active Directory, OpenLDAP, RADIUS и TACACS+.

Для многофакторной аутентификации нужен ещё один внешний сервис. Это может быть облачный сервис, такой как OKTA или Multifactor.

ПОЧЕМУ ПОЯВИЛОСЬ SASE?

Мы разобрались в том, что ZTNA работает на основе технологий, встроенных в NGFW: VPN, Zero Trust и другие движки. Однако во время пандемии COVID выяснилось, что покупка аппаратного устройства имеет определённые недостатки:

1. *Долгая поставка.* Если нужно реализовать удалённый доступ всем сотрудникам, быстро закупить оборудование очень сложно. Спасибо тем производителям, которые бесплатно выдавали виртуальные NGFW на 3 месяца во время пандемии.

2. *Ограничена по производительности.* Если вы отправляете на удалённую работу ещё одно подразделение из 5000 человек, то текущий NGFW уже не справляется со всеми одновременными подключениями.

3. *Неоптимально расходуются каналы интернета.* Если вашим сотрудникам из Владивостока нужно подключиться к Москве, а оттуда снова трафик идёт к серверам во Владивостоке. Это выглядит странно, поэтому приходится покупать ещё один NGFW ближе к сотрудникам, а это расходы на CAPEX и OPEX.

Что можно сделать, чтобы от этого избавиться?

Производители клонировали свои виртуальные NGFW и поместили их

у облачных провайдеров по всему миру. Получилось, что нам сегодня предоставляются сотни доступных шлюзов VPN по всему миру, вы подключаетесь к ближайшему территориально и снижаете задержки. И это VPN, совмещённый с NGFW, т.е. вы получаете набор дополнительных проверок ваших сотрудников в любой точке мира. Сам облачный провайдер уже оптимально перенаправляет ваших сотрудников к ресурсам вашей компании по каналам, защищённым IPSEC. Вы можете узнать у поставщиков, как они минимизируют время подключения, задержки и потери к вашим сервисам. Часто подключения к разным шлюзам ещё и балансируются на основе технологии SD-WAN.

Эту технологию подключения ваших сотрудников через облачные сервисы в Gartner назвали Secure Access Service Edge, сокращённо SASE.

Уверен, вам нужно время, чтобы переосмыслить это описание современных технологий. Возможно, вы слышали и другие названия от различных производителей, однако идеологически и функционально все они будут подобны тем, что описаны выше. Например, термин Software — Defined Perimeter (SDP) — это то же самое, что и ZTNA. Причина в том, что коллеги в своём маркетинге фокусируются на том преимуществе технологии, что внутренние сервисы доступны только через VPN или через обратный HTTPS-прокси и не выставлены наружу. Действительно, именно для этого и были созданы VPN и ZTNA. Пользуйтесь ими, пожалуйста! И используйте двухфакторную аутентификацию!

Смотрите
видео-версию
статьи на канале
Дениса
Батранкова



КОНТЕЙНЕРЫ — НАИМЕНЕЕ БЕЗОПАСНОЕ ОКРУЖЕНИЕ

ЕСЛИ НЕ СЧИТАТЬ ВСЕ ОСТАЛЬНЫЕ



**Никита
ЛАДОШКИН**
руководитель
разработки
PT Container
Security
в Positive
Technologies

Большинство статей про контейнерную безопасность начинается с постулатов о повсеместном применении контейнеров для построения инфраструктуры компаний (по моей оценке, их распространённость в России в среднем достигает около 70 %); в них описываются основные методики оценки векторов атак (по матрице MITRE ATT&CK или стандарту NIST 800-190) и минимально необходимый набор технологий защиты. Я как человек, который уже шесть лет работает с контейнерами, уверен, что всё это вы уже знаете, а вот каких ошибок можно избежать в работе с контейнерами разработчикам, blue team, вендорам — об этом расскажем с точки зрения разных ролей.

КОНТЕЙНЕРЫ И ЗЛОУМЫШЛЕННИКИ

По данным исследования Red Hat, 94 % ИТ-специалистов сталкивались хотя бы с одним инцидентом безопасности, связанным с контейнерами. Половина DevOps-инженеров и специалистов по ИБ даже откладывали развёртывание приложений из-за проблем с безопасностью.

При этом сам по себе факт наличия контейнеризации не является для атакующих триггером для воздействия на инфраструктуру, а недостаточный уровень безопасности таких систем диктуется, как правило, скоростью

апробации проектов и технологий и барьером между контейнеризацией и классическими инструментами ИБ.

Представим типичную схему действий хакера над инфраструктурой контейнеризации с точки зрения классического cyber kill chain:

«Наиболее передовая часть инфраструктуры компании, скорее всего, уже переведена или изначально тестировалась для имплементации на контейнерах → специалисты по ИБ вряд ли успели позаботиться об их защите → изначально целиться буду в них» (рис. 1).

РАЗВЕДКА И ВООРУЖЕНИЕ

Атакующий всегда ищет способы проникнуть в организацию, чтобы перейти к следующим шагам. Разведку, первоначальный этап доступа к контейнерам, можно выполнить путём

сканирования любого общедоступного приложения, созданного разработчиками компании и запущенного на её мощностях. В качестве демонстрационного примера можно выбрать типичное веб-приложение с формами, комментариями, слабой защитой от внедрения SQL-кода или реализации XSS — межсайтового выполнения сценариев. Если же мы хотим получить пример, специфичный для контейнерной среды, то включённый SSH в одном контейнере кластера вполне подойдёт. Злоумышленнику совсем не обязательно иметь прямой доступ к управляющим элементам среды контейнеризации, чтобы проникнуть в инфраструктуру: многие атаки начинаются именно с классических сценариев эксплуатации уязвимостей в ПО.

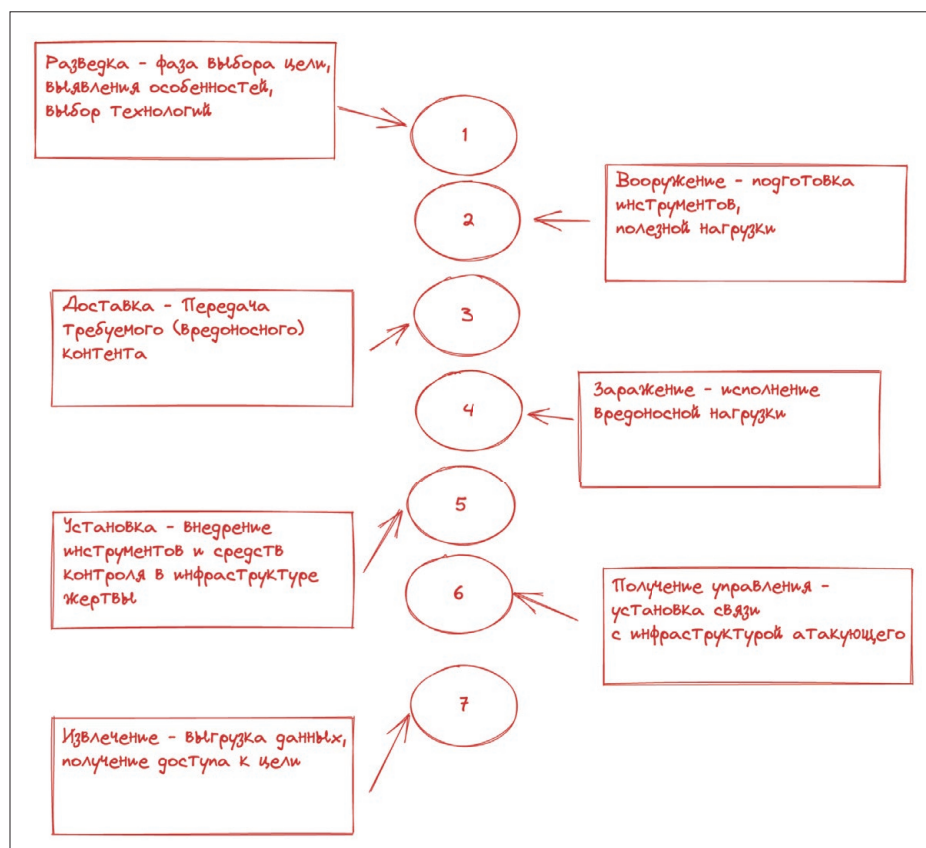


Рисунок 1. Этапы cyber kill chain

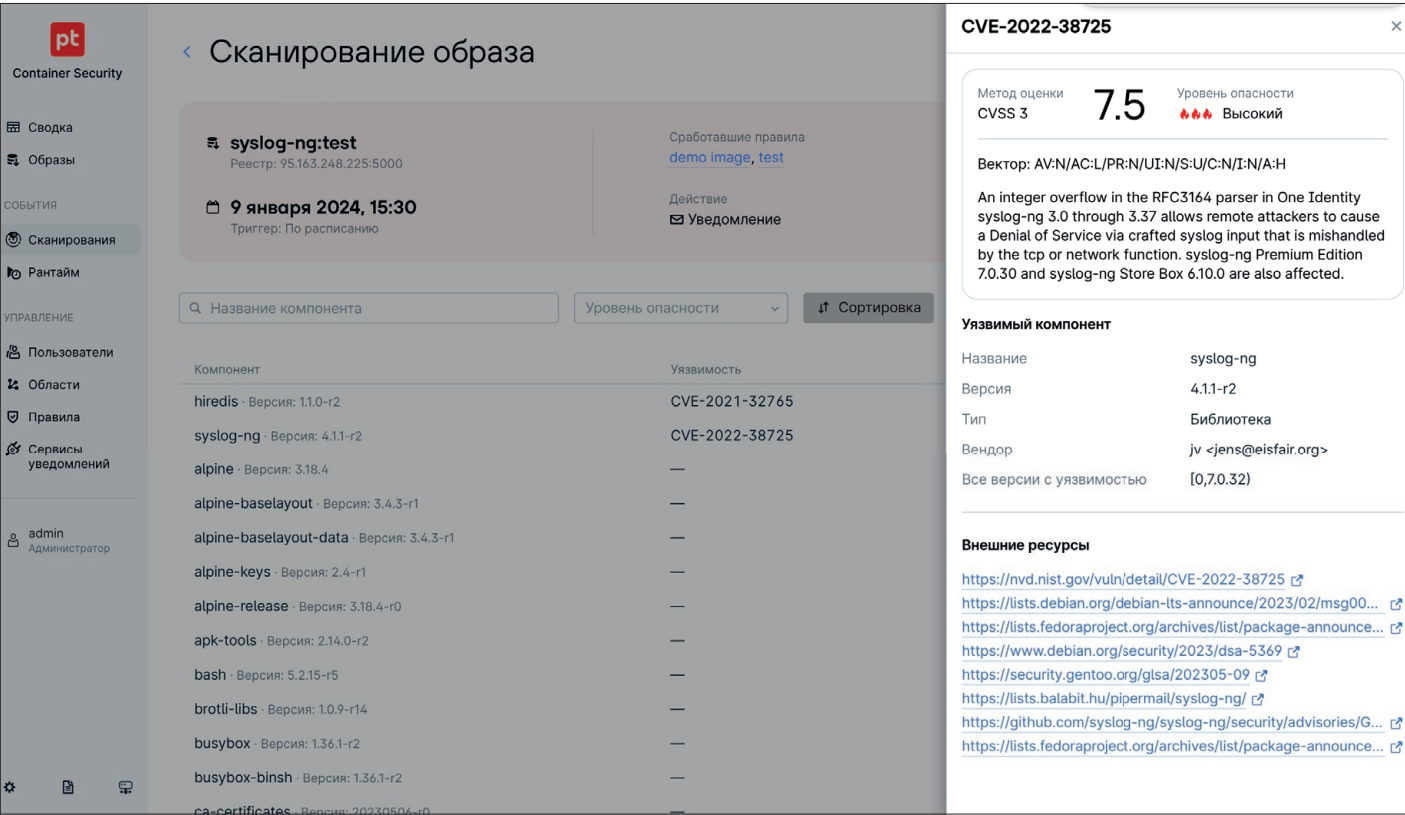


Рисунок 2. Интерфейс PT Container Security при работе с уязвимостями образов

ДОСТАВКА НАГРУЗКИ

Доставка инструментов и вредоносного кода в контексте использования контейнеров ещё острее поднимает вопрос безопасности цепочек поставок. Помимо классических способов с использованием туннелей, активно развиваются атаки с компрометацией публичных репозиториев (например, вредоносных образов docker hub, пакетов PyPi). Отсутствие поддержки таких подходов, как принцип zero trust, на деле может привести к тому, что отделы эксплуатации (DevOps) компании будут использовать непроверенный образ из публичных репозиториев, который изначально был подготовлен злоумышленником для будущей разведки, что может привести к рискам утечки конфиденциальной информации и доступу к инфраструктуре по сторонним каналам (рис. 2).

ЭКСПЛУАТАЦИЯ И ИСПОЛНЕНИЕ КОДА

После анализа инфраструктуры и подготовки инструментария следует попытка выполнения вредоносного кода. Контейнеры добавляют

дополнительные слои абстракции над инфраструктурой, такие как рантайм (среда исполнения) контейнеров и инструменты оркестрации, которые при неправильной настройке могут значительно повысить вероятность запуска вредоносного кода. В первую очередь атакующий может попытаться эксплуатировать дефекты конфигурации доступа самой среды контейнеризации. Сделать это можно через стандартную утилиту для управления кластером kubectl, которая позволяет получить доступы к терминалам контейнеров, стандартному выводу, а также строить сетевые тоннели для взаимодействия с узлами атакующего. Такие действия становятся возможными в случаях, если в организации не озаботились тем, чтобы ограничить ролевую модель, — это встречается в Kubernetes несколько чаще, чем хотелось бы, особенно у инсталляций на собственной инфраструктуре. В такой ситуации атакующий может выполнить абсолютно любой код в любом контейнере, что приведёт к компрометации приложений и данных компании, использующей контейнеризацию.

Однако усложняется не только инфраструктура. Контейнеризация позволяет делать приложения модульными и выносить часть функций в отдельные сервисы (контейнеры). Как правило, такие сервисы служат для повышения доступности и конфиденциальности данных (например, реализация подхода сервисных сетей — Service Mesh). Но ошибки конфигураций могут привести как к повышению рисков компрометации инфраструктуры внешним атакующим, так и к рискам непреднамеренного раскрытия конфиденциальной информации (некорректные правила маршрутизации трафика между сервисами). Что же касается атак через сторонние сервисы, атакующий может проникнуть через вспомогательный контейнер (который находится рядом с основным и использует ресурсы хранилища и сети совместно с другими контейнерами в кластере), внедрив дополнительный контейнер, чтобы запустить вредоносный код и скрыть свою активность, или запустив код в уже существующем сервисном контейнере.

ЗАКРЕПЛЕНИЕ В ИНФРАСТРУКТУРЕ И ИЗВЛЕЧЕНИЕ ДАННЫХ

Основная цель атакующего — получить выгоду от атаки (репутационную, финансовую, политическую). Для этого ему необходимо украсть критически важные данные, нарушить работу систем или внедрить некорректную логику в сервисы (нарушить целостность инфраструктуры). Чтобы это сделать, злоумышленники могут использовать бреши в конфигурации уровня управления контейнеризацией и недостатки процессов сборки и доставки контейнеров: запускать свои вредоносные нагрузки, инъектировать код в образы контейнеров компании, менять конфигурации сервисных сетей для выгрузки данных и прочее. Методы, используемые для этого, включают в себя любые изменения доступа или конфигурации, которые позволяют сохранять своё влияние в системах, например замену или перехват легитимного кода.

Наиболее актуальным примером таких действий для контейнерной среды является, например, использование контроллеров Kubernetes, таких как DaemonSets или Deployments, — так постоянное количество контейнеров атакующего всегда гарантированно работает в одном или всех узлах кластера. Злоумышленники также часто используют возможности нарушения изоляции контейнеров для сохранения данных на узлах (возможность hostPath-монтирования, которая позволит связать файл или директорию узла с контейнером), для обхода сетевой изоляции в контейнерах (hostNetwork), для доступа к управляющим процессам на узле (hostPID). Такие действия позволяют атакующему закрепиться на базовом узле контейнеризации, оставаясь невидимым для классических средств защиты.

К отдельному классу атак на контейнеры стоит отнести атаки на API Kubernetes для доступа к учётным данным. Одним из примеров таких атак является использование вредоносных контроллеров ValidatingAdmissionWebhook (отвечает за перехват и проверку

API-запросов) — оно может быть использовано для перехвата конфиденциальной информации, такой как запросы к kube-API, а также для записи секретов.

Это только некоторые примеры атак на контейнеры и рисков, которые они несут для компаний. Если подробно упоминать остальные тактики, можно написать целый учебник, даже не затрагивая классические методы атак. Важный вывод этой части: необходимо учитывать увеличенную поверхность атаки и повышенную сложность управления инфраструктурой при использовании контейнеров.

КАК РАЗРАБОТЧИКАМ ПОЛЮБИТЬ КОНТЕЙНЕРЫ?

Так, может, проще отказаться от контейнеров совсем? Зачем разработчику технология, для нормальной работоспособности которой необходимо иметь огромное количество компетенций, внедрять отдельные, специфичные только для данного домена инструменты защиты, даже платные (об этом поговорим позже), добавляя в вакансии новый пункт на и без того дефицитном рынке? Даже один из создателей Kubernetes заявил, что контейнерная среда настолько сложная, что просто необходимо что-то с этим делать. Но ведь можно и не внедрять. Можно подождать 10 лет — не исключено, что появится замена контейнерам, ещё более изолированная среда, более легковесная и безопасная.

Однако есть уверенность, что смена парадигмы и новая разновидность инфраструктуры появятся ещё нескоро, а значит, жить придётся с уже морально устаревшими для определённых сценариев подходами. Например, на базе контейнеров построены такие сервисные модели, как SaaS и PaaS, а также инструменты доставки ПО, такие как бессерверные вычисления (serverless).

Если говорить о недостатках и преимуществах при создании современных микросервисов, то у контейнеризации значительно больше плюсов:

- ♦ возможность внедрять декларативный формат для описания процесса установки и настройки, что

сводит к минимуму затраты времени и ресурсов для новых разработчиков, подключённых к проекту;

- ♦ подготовка сервисов для развёртывания на современных облачных платформах устраняет необходимость в серверах и системном администрировании;

- ♦ минимизация расхождения между средой разработки и средой выполнения позволяет использовать непрерывное развёртывание (continuous deployment) для максимальной гибкости;

- ♦ масштабирование без существенных изменений в инструментах, архитектуре и практике разработки;

- ♦ внедрение подхода к безопасности как к коду (security as a code), что позволяет декларативно указывать настройки безопасности для конкретного микросервиса;

- ♦ возможности реализации механизмов микросегментации и нулевого доверия на уровне отдельных компонентов внутри системы, что сильно повышает уровень безопасности систем.

Помимо сложности в использовании и настройке, контейнеризация несёт в себе большие возможности как по разработке и мониторингу вашего сервиса, так и по обеспечению его безопасности из коробки.

И даже новые технологические тренды опираются на классические концепции работы с контейнерами. Например, distroless-контейнеры, содержащие только нужные для работы приложения файлы. Из контейнера убираются неиспользуемые файлы дистрибутива с целью уменьшить его размер. Вместо сотен или тысяч ненужных файлов дистрибутива остаются только файлы, требуемые для работы. То есть гибкость, заложенная в контейнерах «из коробки», позволяет уменьшить площадь атаки без внедрения спецсредств.

Или, например, WebAssembly — открытый стандарт, который определяет формат двоичных инструкций. Он позволяет создавать портируемые исполняемые файлы из исходников, написанных на различных языках программирования. Изначально созданный под безопасный запуск legacy-приложений в браузере, он

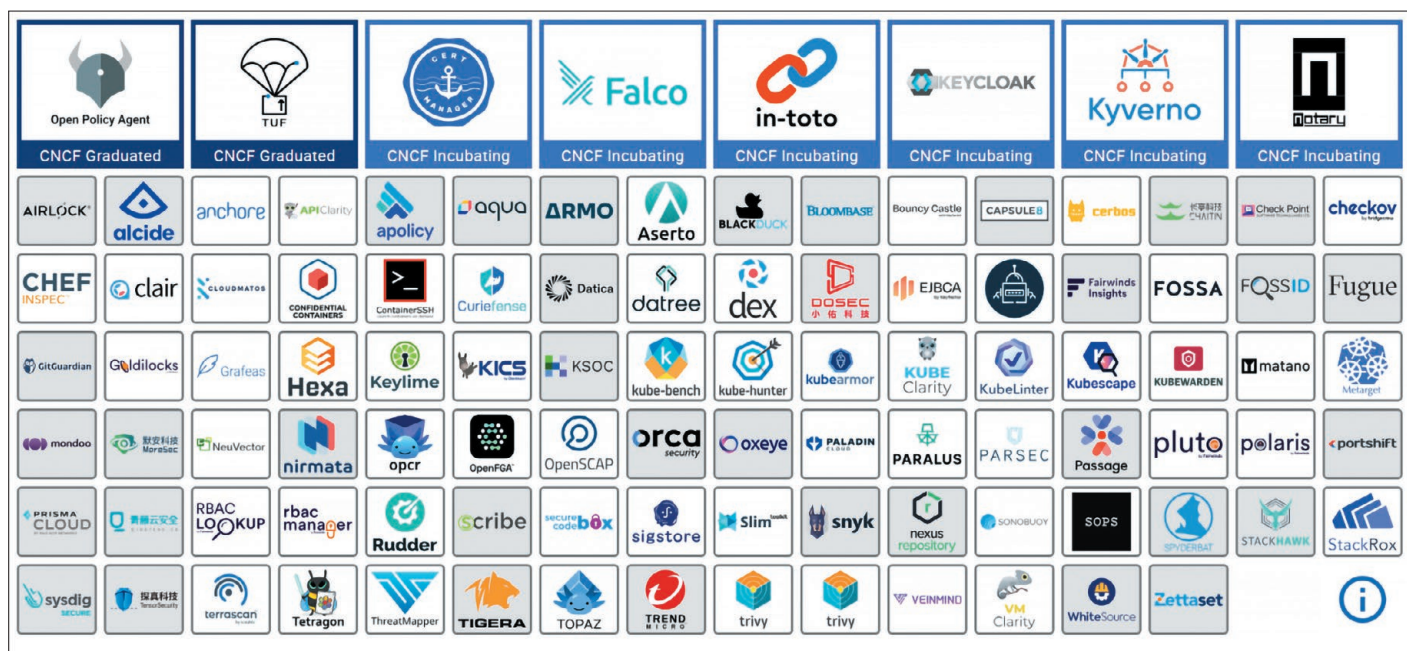


Рисунок 3. CNCF Security & Compliance

развился настолько, что в этом году Docker объявил о поддержке WebAssembly; сейчас он рассматривается как «преемник» контейнеров и следующий логический шаг в развёртывании инфраструктуры. Учитывая, что рантайм Wasm по умолчанию работает в режиме песочницы и следит за безопасным доступом к памяти, а его capabilities-based-модель гарантирует, что Wasm-приложение имеет доступ только к тому, к чему ему явно разрешено иметь доступ, переход на WebAssembly-контейнеры выглядит для меня неизбежным. Даже Соломон Хайкс (один из соучредителей корпорации Docker) писал: «Если бы Wasm+WASI существовали в 2008 году, нам бы не пришлось создавать Docker. Вот насколько они важны. WebAssembly на сервере – будущее компьютерных технологий».

Однако пока такие технологии только развиваются, в контейнерах нужные инструменты уже доступны разработчикам «из коробки» – остаётся их настроить. Например, использование компонентов Linux Security Module (AppArmor, SELinux, Seccomp) для повышения изоляции процессов, управление привилегиями процессов в контейнерах через Linux Kernel Capabilities, управление лимитами на вычислительные ресурсы, использование трассировки и телеметрии для мониторинга контейнеров.

КАК К НИМ ОТНОСИТЬСЯ ЗАЩИТНИКАМ?

А что делать тем, кто встал на стражу контейнерной безопасности, если контейнеры – это инструмент для разработчика и эксплуатации? В первую очередь опираться на системный подход и максимальное покрытие всех возможных стадий разработки программного обеспечения, выстраивая грамотную эшелонированную защиту – от написанного разработчиком кода в репозитории до запущенного итогового микросервиса.

Есть распространённое мнение, что порог входа в безопасность контейнеров весьма высок. Оно имеет место, однако большинство функций безопасности контейнеров имеют под собой основание технологии защиты ядра Linux, и сообщество уже разработало стандарты и практики построения безопасности контейнеров и их инфраструктуры. К таким стандартам можно отнести бенчмарки (NIST 800–190, CIS Kubernetes Benchmark и др.), описывающие рекомендации по харденингу (сокрытию) инфраструктуры. Как правило, это открытые стандарты, и есть открытые имплементации, позволяющие их частично автоматизировать.

Помимо непосредственных рекомендаций, разрабатываются и специализированные фреймворки для защиты цепочек поставки, такие как

Sigstore, Google SLISA, а также процессы контроля целостности ПО (например, The Upgrade Framework).

Разработка таких стандартов и решений по защите объединена в рамках сообщества Cloud Native Compute Foundation (CNCF – часть Linux Foundation) и призвана покрыть все аспекты работы с контейнерами от разработки и безопасности до размещения в облаке. От себя рекомендую ознакомиться с проектом сообщества CNCF Cloud Native Interactive Landscape – собранная в рамках этого проекта информация ориентирована на компании, которые только начинают свой путь в мир инфраструктуры для cloud-native-приложений, и призвана знакомить их с множеством имеющихся решений с открытым исходным кодом и не только. В нашем случае наибольший интерес представляет блок Security&Compliance, демонстрирующий многообразие аспектов и различных инструментов для защиты облаков и контейнеров, что доказывает актуальность проблемы (рис. 3).

Почему я вообще об этом упоминаю? Positive Technologies верит в open source и считает его помощником, а не препятствием. Мы приняли для себя стратегию активного участия в open source, создали группу, которая занимается вопросами участия разработчиков в открытых проектах и создания наших собственных проектов.

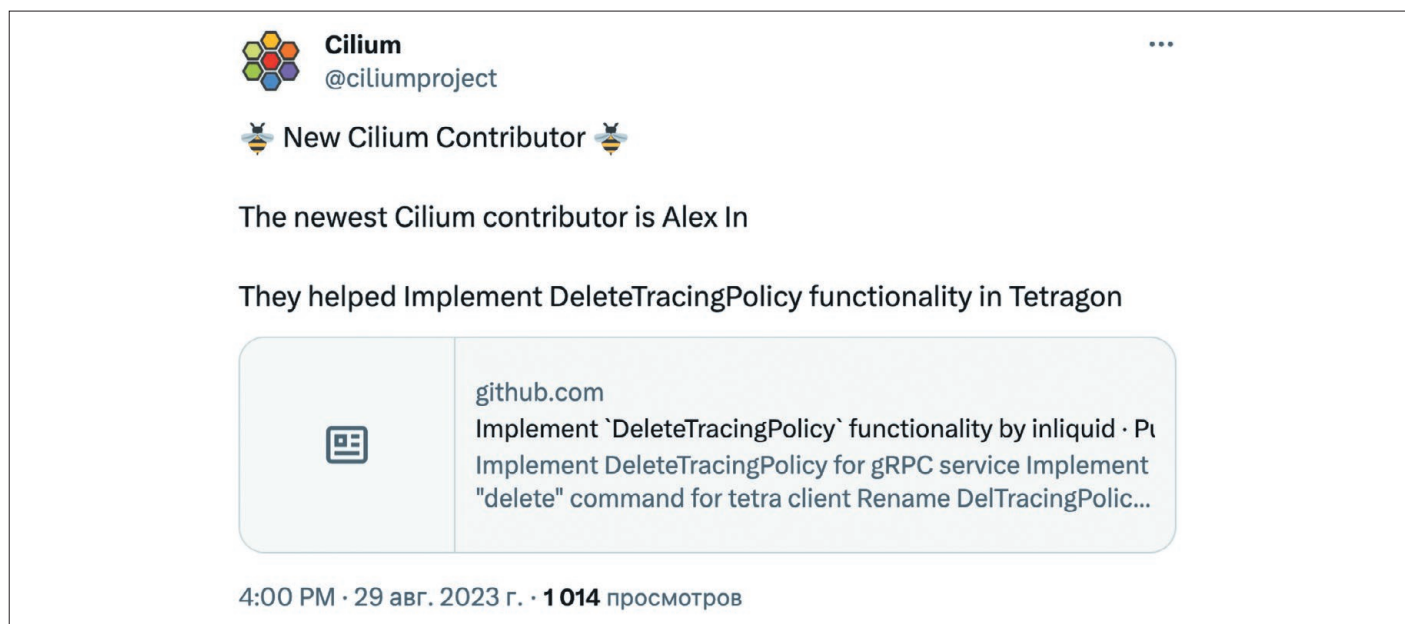


Рисунок 4. Вклад команды PT Container Security в развитие OpenSource

Мы в команде продукта по защите контейнерных сред — PT Container Security — активно поддерживаем эту инициативу. Мы никогда не скрывали, что используем проекты с открытым кодом для реализации функций продукта (например, что мы используем библиотеку syft для сбора software bill of material (SBOM) в образах контейнеров, но оперируем своими БДУ). В рамках сервиса для защиты среды исполнения контейнеров основным сенсором событий рантайма контейнеров для нас является проект Cilium Tetragon, который поставляет события безопасности в нашу подсистему детектирования угроз; в ней в виде детекторов описаны наиболее актуальные атаки на среды контейнеризации.

Важно отметить нашу политику в отношении этих проектов: мы не

просто бесплатно используем данные технологии, а активно участвуем в их развитии. В послужном списке команды PT Container Security уже есть принятые Pull Request, так что мы можем в том числе считать себя причастными к релизу 1.0 данного проекта (рис. 4).

ПОЗИЦИЯ ВЕНДОРОВ

Тут могу рассказать на примере Positive Technologies. Продукт для защиты контейнерных сред от Positive Technologies, PT Container Security, — это результат стратегии развития сервисов компании и экспертизы по части Kubernetes и Docker. Я лично в рамках другого продукта компании — PT Sandbox — переводил вместе с командой наши микросервисы в контейнеры. Страшно вспомнить,

но у Kubernetes актуальной версией тогда была 1.8, то есть 6 лет назад, — тогда не было и половины текущих средств для управления и защиты контейнеров! А вот атаки уже были.

В 2023 году мы представили рынку коммерческую версию продукта PT Container Security.

И защита контейнеров является для нас частью большого направления безопасной разработки (AppSec), в рамках которого мы развиваем свою экспертизу и подходы к повышению безопасности на всех этапах жизненного цикла ПО, а контейнеры являются неотъемлемой частью этого процесса и будут развиваться, как и наш продукт (рис. 5).

Что будет дальше, увидим, но прогнозирую, что контейнеры ещё долго с нами!

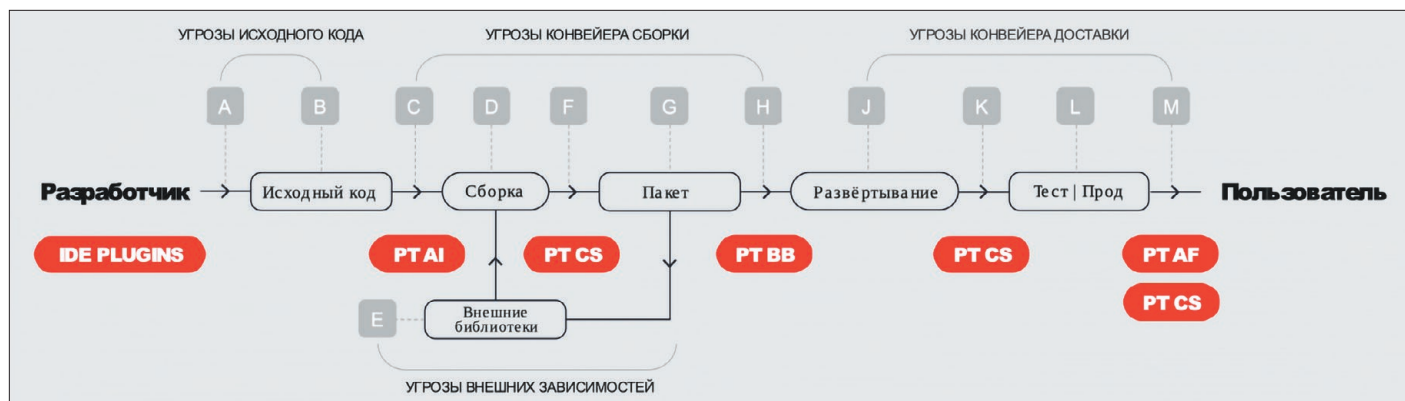


Рисунок 5. Видение процесса безопасной разработки. Версия Positive Technologies

БЕЗОПАСНОСТЬ ИЗОЛИРОВАННОЙ СРЕДЫ

ЗАЩИТА СРЕД КОНТЕЙНЕРИЗАЦИИ ОТ А ДО Я



Тимофей ТИТКОВ

руководитель направления развития
продуктов облачной и сетевой безопасности
«Лаборатории Касперского»

Современные крупные ИТ-системы практически всегда используют ту или иную форму виртуализации или контейнеризации. Это позволяет ускорить процесс разработки, сэкономить деньги и другие ресурсы. Но к контейнерам неприменимы напрямую подходы, работающие при защите виртуальных серверов. Какие риски нужно учесть при внедрении контейнеризации и какие меры защиты применять?

ВЫГОДЫ КОНТЕЙНЕРИЗАЦИИ

Контейнер — это изолированная среда для запуска одного приложения, создаваемая средствами на уровне ядра ОС. В контейнер входит как приложение, так и необходимые настройки и вспомогательные компоненты, поэтому разработчикам крайне удобно запаковать в контейнер всё необходимое, а пользователям — эксплуатировать его. Изоляция значительно снижает влияние контейнеризированных приложений друг на друга, поэтому в контейнерной инфраструктуре меньше причин для сбоев и администраторам легче контролировать её.

Контейнеризация — более лёгкая технология по сравнению с виртуализацией: в контейнерах не эмулируется оборудование и не нужно поставлять полное содержимое виртуальной машины, в частности гостевую ОС. Во многих случаях контейнеризированные нагрузки проще масштабировать.

Контейнеризация — важная составная часть в современной ИТ-разработке. Также она прекрасно вписалась в методологию непрерывной интеграции и развёртывания (CI/CD, continuous integration, continuous delivery), помогающую выпускать обновления приложений быстрее и с меньшим числом ошибок. Этот подход предусматривает короткий цикл разработки, параллельную работу команд над одним кодом, автоматизацию рутинных действий. Применение контейнеризации в конвейере CI/CD повышает его эффективность, так как каждый отдельный контейнер — это один микросервис, отдельный сегмент большого приложения, создавать, обновлять и отлаживать который гораздо быстрее и безопаснее, чем при традиционном подходе монолитного кода. Принципиальный момент — обновление поставляется в виде нового образа, а не разворачивается внутри существующего контейнера. В результате быстрее готовится и отлаживается релиз, снижаются требования к инфраструктуре разработчика и заказчика, повышается стабильность работы и облегчается масштабирование приложения.

УГРОЗЫ В КОНТЕЙНЕРНОЙ ИНФРАСТРУКТУРЕ

Хост-система, среды контейнеризации и приложения в контейнерах подвержены большинству типичных рисков ИБ, таких как уязвимости в компонентах и небезопасные настройки.

Всем перечисленным уже активно пользуются злоумышленники. Например, в публичном репозитории Docker Hub были обнаружены 1650 образов контейнеров, содержащих вредоносное ПО. Известны вредоносные кампании, использующие Docker API, чтобы создавать зловредные контейнеры на атакованных системах, отключать системы мониторинга и заниматься майнингом. Также в репозиториях могут подолгу сохраняться не обновлённые образы контейнеров, содержащие известные уязвимости наподобие Log4shell. Кроме того, разработчики регулярно забывают в контейнерах API-ключи и другие секреты.

Систематизируем возможные угрозы в единую таблицу 1.

ЗАЩИТА ТРАДИЦИОННЫМИ СРЕДСТВАМИ

Многие подходы, хорошо зарекомендовавшие себя при защите виртуальных машин, не могут быть применены в контейнерной безопасности. Внутри контейнера невозможно запустить VM, поэтому трудно обнаруживать, например, уязвимое и вредоносное ПО, применять к контейнеризированным приложениям такие инструменты защиты, как WAF. Трафик между контейнерами зачастую передаётся при помощи виртуальной сети на уровне оркестратора, и он может быть недоступен инструментам сетевой безопасности.

Более того, даже на ОС хоста неадаптированный агент защиты может приводить к деградации производительности или стабильности развёрнутых контейнерных приложений. Безопасность кластера должна быть обеспечена на хосте с учётом конкретной применённой среды оркестрации и характера контейнерных нагрузок.

Ряд проблем, таких как предотвращение запуска недоверенных контейнеров, поиск секретов в контей-

Образы	Реестр образов	Оркестратор	Контейнеры	ОС хоста
Использование недоверенных образов	Незащищённое подключение	Не ограничен административный доступ	Уязвимости среды выполнения	Общее ядро ОС для всех контейнеров
Уязвимости ПО	Устаревшие образы с уязвимостями	Доступ без авторизации	Неограниченный доступ к сети	Уязвимости компонентов ОС
Ошибки в конфигурации	Недостаточные аутентификация и авторизация	Отсутствие изоляции и инспекции трафика между контейнерами	Небезопасная конфигурация среды выполнения	Некорректные права доступа пользователей
Вредоносное ПО		Не разнесены по хостам контейнеры с разным уровнем важности данных	Уязвимости приложений в контейнерах	Файловая система доступна из контейнеров
Секреты в открытом виде		Ошибки конфигурации оркестратора	Незапланированные контейнеры в среде выполнения	

Таблица 1. Схема угроз элементам системы контейнеризации

нерах, ограничение сетевого трафика для каждого конкретного контейнера с учётом его функций, решать могут лишь специализированные решения.

ЗАЩИТА ШТАТНЫМИ СРЕДСТВАМИ

Поставщики сред контейнеризации активно повышают уровень безопасности своих продуктов. С помощью штатных средств Kubernetes, например, можно настраивать квоты ресурсов, политику логирования, внедрять RBAC (role based access control), реализуя принцип наименьших привилегий. Но целые классы задач ИБ, такие как контроль процессов внутри запущенного контейнера, анализ на уязвимости, контроль соответствия ИБ-политикам, не могут решаться штатными инструментами.

Зрелая система контейнерной безопасности должна обеспечивать защиту на ранних стадиях работы с контейнерами: разработки, поставки, хранения. Для этого безопасность контейнеризации должна быть буквально встроена в процесс разработки и интегрирована с инструментами разработчиков.

ЗАЩИТА КОНТЕЙНЕРОВ СТАНОВИТСЯ ЧАСТЬЮ DEVSECOPS

Подход DevOps эволюционировал в DevSecOps из-за постоянно повышающихся требований к надёжности и безопасности приложений. Чтобы сделать безопасность органичной

частью разработки, основные требования ИБ автоматически проверяются на всех фазах подготовки и доставки приложения, где это возможно, и контейнерные среды создают для этого благоприятные условия.

Фаза исследования — защита операций с VCS и реестром. На ранних этапах цикла разработки создатели ПО выбирают компоненты, в том числе контейнеризированные, которые будут применяться в приложении. Система безопасности должна проверять образы из реестра на актуальность, анализировать конфигурационные файлы на наличие ошибок, небезопасных настроек. Базовые образы должны быть проверены на уязвимости, ВПО, наличие секретов. Благодаря этому значительно снижаются риски компрометации цепочки поставок.

Фаза создания и тестирования — защита операций Continuous Integration. Здесь необходимо убедиться, что в образ не попали секреты, уязвимые версии библиотек, ВПО, что все подпадающие анализу ИБ-аспекты соответствуют уровню требований регуляторов и самой организации. Сборка приложения не может успешно завершиться, если часть политик нарушена. Это делается при помощи интеграции системы контейнерной безопасности с платформой CI/CD. Наряду со статическим и динамическим тестированием приложения на безопасность эта мера отличается DevSecOps от других подходов к разработке.

Фаза доставки и развёртывания — защита на уровне Continuous Delivery. Образы, передаваемые в эксплуатацию, должны быть проверены на целостность, а также полностью соответствовать принятым политикам. Если ситуация требует сделать исключение (например, опубликована уязвимость, но ещё нет патча), то оно всегда должно документироваться и быть ограниченным во времени.

Фаза выполнения — защита оркестратора и запущенных контейнеров. На этом этапе минимизируются риски, связанные с уязвимостями среды выполнения или её неверной настройкой. Только здесь можно выявить различные аномалии в работе приложения, такие как избыточно большая вычислительная нагрузка или неожиданные коммуникации с другими контейнерами и сетью в целом. На этом этапе также отслеживаются безопасные настройки самого оркестратора и доступа к нему. Для системы контейнерной безопасности тут критичны нативная работа с оркестратором Kubernetes или OpenShift. При этом нельзя оставлять без защиты и саму ОС на хосте. Чтобы работать на этих этапах, система контейнерной безопасности должна быть многокомпонентной.

ЗАЩИТА ДЛЯ КАЖДОГО КОМПОНЕНТА

Детальный список мер защиты выглядит так (таблица 2).

Образы	Реестр образов	Оркестратор	Контейнеры	ОС хоста
Проверка на уязвимости	Интеграция с реестром и проверка образов	Обнаружение ошибок конфигурации и рекомендации по устранению	Контроль запуска и работы только доверенных контейнеров	Обнаружение ошибок конфигурации и рекомендации по устранению
Проверка на ошибки в конфигурации образов	«Закрытый список» — использование только одобренных и актуальных образов	Визуализация ресурсов в кластере	Контроль целостности контейнеров	Уменьшение рисков безопасности за счёт контроля запуска контейнеров
Проверка на вредоносное ПО	Поиск неверных конфигураций и настроек доступа	Обнаружение и сканирование образов в кластере (поиск неучтённых контейнеров)	Контроль запуска приложений и сервисов внутри контейнеров	Адаптированная версия ОС для минимизации поверхности атаки
Поиск секретов			Контроль трафика контейнеров	
Оценка рисков и выявление потенциально опасных образов			Минимизация привилегий контейнеров	
			Группировка контейнеров на нодах по уровню риска / важности	

Таблица 2. Список мер защиты

Центральный элемент системы защиты — детальная проверка образов. Система безопасности должна интегрироваться с ключевыми реестрами, как публичными, так и корпоративными, и регулярно сканировать используемые образы в соответствии с политиками организации. Каждая проверка из списка сама по себе важна, но профиль риска и специфика приложений в каждой организации свои, поэтому можно, например, допустить эксплуатацию образов с уязвимостями низкой критичности. Образы контейнеров, не прошедшие проверку, либо просто помечаются для администраторов, либо блокируются для использования на следующих этапах.

Вторая группа инструментов защиты отрабатывает на этапе развёртывания и запуска контейнеров. Прежде всего предотвращается запуск контейнеров, не соответствующих политикам и не входящих в списки доверенных.

Также необходимо проверять сам оркестратор, чтобы выявить ошибки в настройках, несоответствие политикам безопасности и неправомерные попытки изменения конфигурации. После запуска контейнеров

мониторинг активности оркестратора позволяет обнаруживать и пресекать подозрительные операции как внутри кластеров, так и между ними.

Некоторые задачи невозможно переложить на защитное решение. Это изначальный выбор защищённой и минималистичной сборки ОС, специально приспособленной для запуска контейнерных нагрузок, а также задача по группировке контейнеров. Для организации правильной эшелонированной защиты и удобного управления нужно сгруппировать запущенные контейнеры на нодах так, чтобы информация с высоким уровнем требований к защите обрабатывалась отдельно от информации с более низкими требованиями.

Решать каждую задачу по защите контейнеров изолированно чересчур трудозатратно, поэтому для средних и крупных контейнерных сред нужны цельные решения, глубоко интегрированные с платформой контейнеризации, конвейером CI/CD и используемыми в компании инструментами ИБ.

Работу ИБ-специалистов упростят интеграция с SIEM-системой и уже используемыми каналами

оповещений о найденных проблемах, возможность регулярно автоматически сканировать все образы по обновляемой базе уязвимостей (NVD или БДУ), функциональность для временного принятия ИБ-рисков, а также детальное логирование административных событий в системе защиты сред контейнеризации.

ОСОБЫЕ ТРЕБОВАНИЯ РОССИЙСКИХ ЗАКАЗЧИКОВ

Российские регуляторы накладывают жёсткие требования к информационной безопасности, в том числе по оперативному устранению известных уязвимостей. В связи с этим решение для защиты контейнеров должно отслеживать уязвимости не только по западным источникам, как NVD, но и в БДУ, поддерживаемой ФСТЭК. Растёт интерес к разработкам из Реестра отечественного ПО, поэтому система контейнерной безопасности должна поддерживать базовые образы, основанные на отечественных ОС. Так, Kaspersky Container Security удовлетворяет этим требованиям, уже сегодня поддерживая образы на базе Astra Linux и РЕД ОС.

БЕЗОПАСНАЯ РАЗРАБОТКА: ВИТОК РАЗВИТИЯ

ИНТЕГРАЦИЯ НА КАЖДОМ ЭТАПЕ



**Юрий
ШАБАЛИН**
ведущий
архитектор
Swordfish
Security

Финансовые организации сегодня в большинстве своём уже пришли к осознанию необходимости выстраивания процессов безопасной разработки. Этому способствует, в частности, ЦБ. После недавнего появления методического документа «Профиль защиты прикладного программного обеспечения и автоматизированных систем и приложений...» стало понятно, что для соответствия политикам регулятора качественный процесс безопасной разработки иметь просто необходимо. Поговорим о том, какие возможности существуют сегодня для повышения эффективности уже функционирующего процесса безопасной разработки.

БЕЗОПАСНОСТЬ «ПО КЛАССИКЕ»

Подход, при котором проверки на безопасность были периодическими и проводились ближе к концу выпуска релиза продукта, а специалисты по ИБ были изолированы от процесса, уже остался в прошлом. Тогда считалось вполне нормальным в качестве заключительного штриха провести для продукта тестирование на проникновение. Причём обнаруженные по итогу проблемы безопасности не всегда устранялись из-за угрозы срыва поставок.

Но довольно быстро разработчики и отдел сопровождения начали работать совместно, руководствуясь

принципами Agile, постепенно автоматизируя свои процессы и переходя к непрерывной разработке (DevOps). Безопасность поначалу сильно отставала, но постепенно пришло понимание, появились средства анализа защищённости, предназначенные для контроля различных аспектов ПО, включая SAST (статический анализ кода), SCA (анализ используемых библиотек с открытым исходным кодом), DAST (динамический анализ приложений). Эти практики начали не только применять вручную, но и включать их в процесс разработки для автоматизации.

ПАРАДИГМА «ДВИЖЕНИЯ ВЛЕВО»

На следующем этапе произошёл «сдвиг влево» практик безопасной разработки, то есть максимально близко к началу создания продукта. Так, статический анализ приложения стал проводиться сразу при сборке новой тестовой версии, после внесения изменений разработчиком. За счёт этого дефекты безопасности начали выявляться и устраняться на раннем этапе, без необходимости проверять стабильность работы системы после исправления.

Аналогично стали проверяться библиотеки с открытым исходным кодом — сразу при попадании в код, благодаря чему отпала необходимость впоследствии переделывать ощутимую часть продукта в попытках найти замену уязвимой библиотеке.

Все практики стали ориентироваться на максимальное смещение в сторону начала процесса разработки и на уменьшение показателя «стоимость исправления дефекта». И уже когда компании начали выходить на определённый уровень зрелости, они начали задумываться о том, что всё это можно использовать на более поздних этапах, тем самым обеспечивая контроль не только при разработке, но и при эксплуатации. А так же обратить внимание и на более

ранние этапы, ещё до попадания кода или библиотеки в репозиторий.

НОВЫЕ ВЫЗОВЫ — «ИНТЕГРАЦИЯ НА КАЖДОМ ЭТАПЕ»

Сегодня всё большую популярность набирает новый подход — «интеграция на каждом этапе жизненного цикла», с которым проверки могут дать наибольшую пользу.

SAST

Статический анализ кода, как правило, применяется после попадания кода разработчика в основную ветку. Но эффективность данной практики можно повысить.

♦ Проверка на этапе написания кода

Так, можно анализировать код из среды разработки, в которой он пишется. Это делается при помощи плагина от инструмента безопасности, который подсвечивает опасные места или небезопасные конструкции сразу после создания строки кода или, в других случаях, после нажатия на специальную кнопку. Такой подход позволяет не просто обнаруживать уязвимости, а не допускать их появления в системе контроля версий (VCS). При этом он очень удобен в работе.

♦ Сканирование перед загрузкой в систему контроля версий

Ещё один пример реализации: при отправке разработчиком кода в систему контроля версий происходит блокировка в случае нарушения одного из требований. Его часто применяют для поддержания качества кода. Но также можно использовать его для статического анализа — чтобы обновлённая версия кода автоматически проверялась, после чего принималось бы решение о возможности её загрузки. Оптимально проводить быстрый поверхностный анализ для выявления наиболее простых или критических вещей (исключив их попадание



в репозиторий), так как последующие этапы покроют всё остальное.

♦ Интеграция с системой проведения код-ревью

При отправке кода на процесс ревью другими разработчиками он также может уходить в систему SAST. И тогда после анализа выявленные уязвимости будут добавляться в комментарии, которые видят все участники процесса ревью. Это исключит «умалчивание» уязвимостей и их попадание в стабильную ветку.

SCA/OSA

Как правило, анализ библиотек с открытым исходным кодом проводят на уже собранном артефакте, который содержит в себе все зависимости, или для исходного кода, в котором есть файлы сборки.

Есть решения, которые позволяют упростить внедрение этой практики и получать эффект на многих этапах, включая и выпуск в промышленную эксплуатацию:

♦ Анализ компонент, которые попадают во внутренний репозиторий

Некоторые компании разрабатывают свои системы в закрытом контуре, и их системы сборки, а иногда и рабочие места не имеют доступа в интернет. В таком случае загрузка всех библиотек, необходимых для сборки приложения, проходит через единую систему хранения библиотек. И можно применить подход с файнволом

для компонент с открытым исходным кодом, которые не удовлетворяют требованиям безопасности. Допустим, при создании новой функциональности разработчик хочет подключить внешнюю библиотеку, которой ещё нет во внутреннем контуре. Он обращается к репозиторию с соответствующей просьбой. Если процесс выстроен грамотно, библиотека проходит анализ на безопасность внутри и принимается решение о возможности её использования. Это позволит свести риски попадания уязвимого компонента из неё к минимуму.

♦ Мониторинг компонент в промышленной эксплуатации

Также возможно мониторить то, что уже находится в периметре компании. В частности, библиотеки и их версии, которые на данный момент используются в развёрнутом приложении. Ведь может случиться, что библиотека считалась безопасной, когда компания выпускала продукт, а через неделю в ней обнаружили критическую уязвимость. Как можно быстро узнать об этом? Как понять, какие продукты используют именно эту уязвимую версию? Ответы на эти вопросы поможет дать механизм мониторинга. Непосредственно перед разворачиванием продукта происходит составление SBOM-файла с перечнем используемых библиотек и их версий. И к нему проводится периодическая проверка на наличие новых, неизвестных ранее проблем с безопасностью.

При их появлении ответственные лица сразу же получают уведомление и смогут принимать решения и реагировать.

Выводы

Примеров того, как разные практики эволюционируют, предоставляя новые возможности для интеграции их в самые разные этапы жизненного цикла, великое множество. К сожалению, охватить их все в рамках одной статьи и показать, как различные активности могут применяться ближе к «правой» части разработки, как контролировать целостность артефактов, как обрабатывать срабатывания с инструментов защиты приложений, как использовать информацию из сообщений технической поддержки, как развиваются программы BugBounty, физически невозможно, хоть и очень хочется.

Отрадно наблюдать за развитием процессов безопасной разработки, за тем, как они предоставляют компаниям всё больше возможностей для повышения эффективности и качества работы.

Важно то, что каждая компания, с которой мы работаем, успешно развивается от «классической безопасности» в сторону «интеграции на каждом этапе». Очень надеюсь, что в ближайшем будущем мы увидим новый виток развития процессов безопасной разработки и сможем выйти на новый уровень защищённости наших сервисов.

СПАСИТЕЛЬНЫЙ SLSA

ОЦЕНКА ЭФФЕКТИВНОСТИ ЗАЩИТЫ ЦЕПОЧЕК ПОСТАВОК



Мария
ЗУБЧЕНКО
Yandex Cloud

БЕЗОПАСНАЯ РАЗРАБОТКА И ЗАЩИТА ЦЕПОЧКИ ПОСТАВОК

Безопасная разработка, очевидно, помогает предотвращать риски, связанные с уязвимостями приложений, ещё на этапе разработки, минимизирует риски и повышает надёжность системы. Для этого применяются специализированные методы, инструменты и анализ безопасности. Обнаружение и устранение уязвимостей являются важными этапами процесса безопасной разработки, требующими постоянного мониторинга, анализа и корректирующих мер, о которых уже рассказывали на страницах этого журнала.

При этом особо остро сейчас стоит задача защиты цепочки поставок при использовании сторонних библиотек и модулей в разработке приложений. В связи со сложностью и зависимостью процессов разработки от сторонних инструментов атаки на разработку стали более возможными. Теперь целью атак могут быть не уязвимости в конечном продукте, а сам процесс разработки. Атаки supply chain обычно нацелены на внедрение вредоносных изменений во время написания кода, замену распространяемых компонентов или зависимостей. Основная цель такой атаки — получить несанкционированный доступ к данным, интеллектуальной собственности или нанести ущерб компании.

Все помнят масштабы атаки на финансовую отрасль с помощью вредоноса NotPetya, который эксплуатировал уязвимости в одном из поставщиков ПО, или известную

атаку на Solarwinds. По данным Positive Technologies, в III квартале 2023-го количество атак на финансовые организации и их клиентов удвоилось по сравнению с таким же периодом прошлого года. При этом в 22 % инцидентов было зафиксировано эксплуатация уязвимостей в цепочках поставок ПО. То есть обороты не сбавляются.

ЗНАЧЕНИЕ SLSA ДЛЯ DEVSECOPS

Как удостовериться, что выстроенный вами SSDL обеспечивает нужный уровень безопасности цепочки поставок ПО? Есть ли у сообщества DevSecOps эталон или чек-лист, по которому можно удостовериться, что контролей безопасности достаточно для снижения этих рисков? Тут на помощь и приходит такой стандарт, как SLSA (Supply-chain Levels for Software Artifacts).

SLSA (уровни цепочки поставок) — это фреймворк, предложенный компанией Google и поддерживаемый ассоциацией Open Source Security Foundation, которая обеспечивает процессы контроля целостности и

безопасности программных компонентов на всех этапах их поставки.

SLSA представляет собой набор руководящих принципов для описания необходимых мер безопасности в процессе создания и развёртывания ПО. Цель SLSA — снизить риск атак на ПО путём установления передовых практик и стандартов для разработчиков и команд DevOps. SLSA включает набор требований и рекомендаций по безопасности, которые охватывают такие задачи, как подписание программного обеспечения, проверка происхождений артефактов, контроль процессов сборки и выпуска приложений, сканирование уязвимостей и аттестация (рис. 1).

СТАНДАРТЫ БЕЗОПАСНОЙ РАЗРАБОТКИ

Давайте посмотрим, как удостовериться, что ваши коллеги, которые предпочитают разрабатывать в облаке, будут разрабатывать с учётом рекомендаций и требований безопасности. Возьмём в качестве примера стандарт SLSA. Облачные приложения создаются с использованием сложных экосистем контейнерных приложений и микросер-

Уровень	Что значит на практике
1	Процесс сборки должен быть полностью написан по сценарию/автоматизирован и генерировать происхождение. Происхождение — это метаданные о том, как был создан артефакт, включая процесс сборки, исходный код верхнего уровня и зависимости.
2	Требует использования системы контроля версий и размещённой службы сборки, которая генерирует аутентифицированный источник. И плюс подпись происхождения, сгенерированного на первом уровне.
3	Платформы хранения кода и его сборки соответствуют определённым стандартам безопасности, гарантирующим возможность проверки источника и целостность происхождения соответственно. На хостах должны быть определённые проверки для исключения фальсификации происхождения.
4	Ревью кода двумя лицами и герметичный, воспроизводимый процесс сборки. Соответствие стандартам безопасности и сканирование на уязвимости.

Рисунок 1. SLSA включает набор требований и рекомендаций по безопасности

висов. Защита их цепочки поставок необходима для обеспечения целостности всего приложения. SLSA как раз и предлагает рекомендации по защите цепочек поставок образов контейнеров, микросервисов и компонентов, используемых для облачных приложений.

Соответствие SLSA в облаке показано на рис. 2.

◆ **Уровень 1 и 2** покрывается за счёт встроенных возможностей Managed Service for GitLab, одна из которых – генерации provenance attestation.

Attestation (аттестация программного обеспечения) – это аутентифицированное заявление (метаданные) о программном артефакте или коллекции программных артефактов. Основным предполагаемым вариантом применения является использование в автоматизированных механизмах разработки политик, таких как in-toto и Binary Authorization. Сообщество Open Source Software Security (OpenSSF) в целом и проект SLSA в частности проделали большую работу по определению структуры и эталонной реализации. Суть её в том, что основной частью метаданных является заявление, заворачивающееся в конверт, который затем подписывается, формируя окончательную аттестацию.

◆ **Уровень 3** достигается с использованием решения Cosign, интегрированного с сервисом Yandex Key Management, для подписи образов и локальных артефактов.

Cosign – это инструмент, разработанный командой Google, который предоставляет возможность подписывать и проверять подписи контейнерных образов. Он разработан с целью обеспечения безопасности и доверия при работе с контейнерами, особенно в контексте поставки и развёртывания контейнерных образов.

Yandex Key Management Service – сервис для управления криптографическими ключами. Эти ключи используются, чтобы защитить секреты, личные данные и другую конфиденциальную информацию, которую вы храните в облаке.

В сервисе Key Management Service можно использовать ключевые пары

1-й и 2-й уровни	Процесс сборки задокументирован, и сервис сборки устойчив к взломам	 Managed Service for GitLab Генерация Provenance attestation
3-й уровень	Дополнительная устойчивость к конкретным угрозам	Подпись артефактов:  Key Management Service +  cosign  Yandex Container Registry
4-й уровень	Высочайший уровень доверия	 Managed Service for GitLab  Стандарт по защите облачной инфраструктуры Yandex Cloud  Сканер уязвимостей в Container Registry

Рисунок 2. Соответствие SLSA в облаке

электронной подписи, созданные с помощью утилиты Cosign. Вот QR-код с инструкцией, как с помощью Cosign сохранять созданную ключевую пару в сервисе Yandex Key Management Service, подписывать файлы и артефакты закрытым ключом этой пары и проверять электронную подпись с помощью её открытого ключа:



◆ **Уровень 4:** система должна соответствовать стандартам безопасности и обладать свойствами герметичности и изолированности. Помимо того, что само облако соответствует стандартам безопасности, как отечественным, так и международным, и отдельным рекомендациям о безопасности CI/CD-системы на базе управляемого GitLab. У пользователей есть возможность проводить сканирование на уязвимости своих образов, хранящихся в Yandex Container Registry, с помощью Сканера уязвимостей. Проверка образов на уязвимости важна для защиты цепочки поставок от атак и обеспечения безопасности облачных приложений.

Если говорить про отечественные стандарты, стоит упомянуть недавно обновлённый стандарт ГОСТ Р 56939–202X «Защита информации. Разработка безопасного программного обеспечения» который мы сейчас активно изучаем. ГОСТ Р 56939 направлен на

достижение целей, связанных с предотвращением появления или устранением уязвимостей программ, и содержит перечень мер, которые рекомендуется реализовать на соответствующих этапах жизненного цикла программного обеспечения.

Кроме того, рекомендуем обратить внимание на то, что у Yandex Cloud есть собственный Стандарт по защите облачной инфраструктуры. Этот документ включает рекомендации по техническим мерам защиты и помогает выбрать меры обеспечения информационной безопасности при развёртывании информационных систем на облачной платформе Yandex Cloud.

Рекомендации и меры обеспечения безопасности в стандарте сопровождаются ссылками на инструкции и решения по настройке безопасных конфигураций ресурсов с помощью штатных средств защиты информации и дополнительных средств защиты, доступных пользователям Yandex Cloud. На основе SLSA был написан 9-й раздел, посвящённый защите приложений, который устанавливает дополнительные требования к безопасности в цепочке поставок программных продуктов. Этот раздел учитывает рекомендации и лучшие практики, представленные в SLSA, и расширяет их для обеспечения максимальной защиты.

ИНСТРУМЕНТЫ КОНТРОЛЯ ЦЕПОЧЕК ПОСТАВОК

Давайте рассмотрим некоторые ключевые этапы в построении надёжного пайплайна для безопасной разработки с инструментами контроля

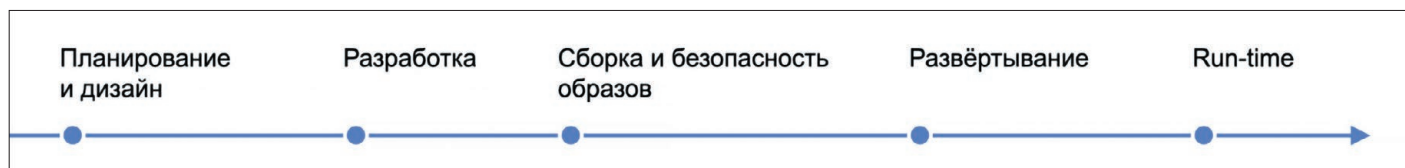


Рисунок 3. Этапы построения Pipeline

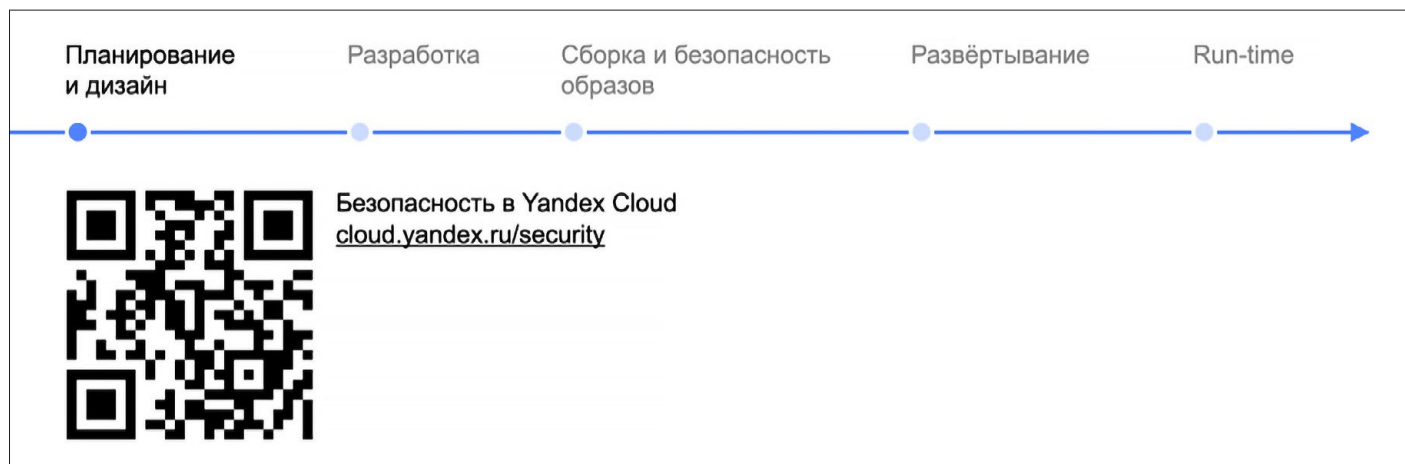


Рисунок 4. Планирование и дизайн

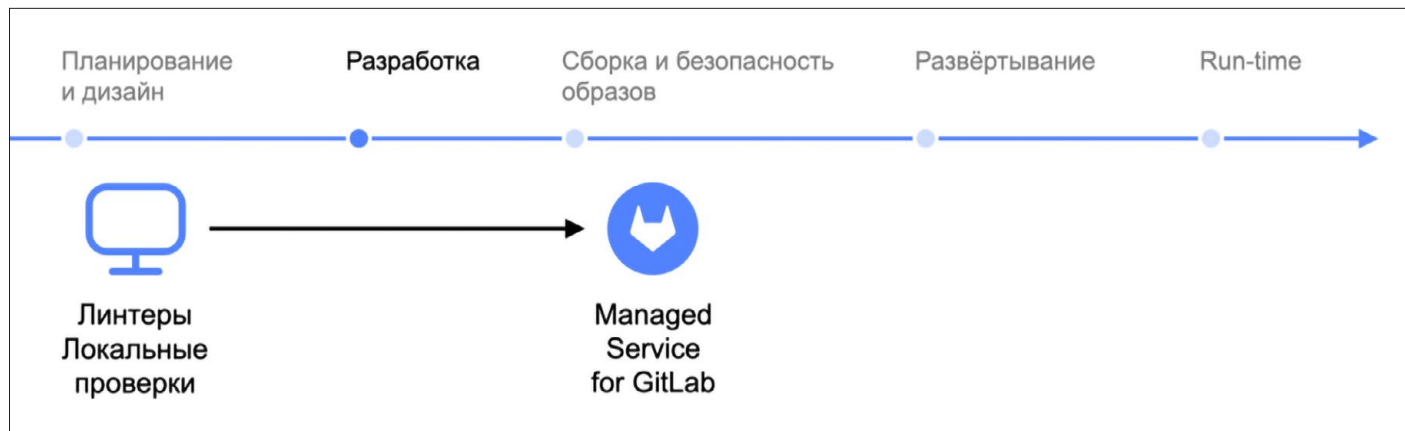


Рисунок 5. Разработка



Рисунок 6. Сборка и безопасность образов

цепочки поставок, чтобы соответствовать SLSA.

Этапы построения Pipeline

По результатам опроса наших клиентов четверть пользователей Yandex Cloud используют облачную платформу для разработки. Так выглядит DevSecOps-пайплайн (рис. 3). Погрузимся в каждый этап подробнее.

Планирование и дизайн

Перед тем как написать первые строчки кода, необходимо верхнеуровнево понять, как вы будете выстраивать безопасную инфраструктуру. В контексте Yandex Cloud можно посетить портал безопасности, где собраны материалы по тому, как само облако соответствует требованиям регуляторов, как вы можете соответствовать этим требованиям, и много ещё интересного (рис. 4).

Разработка

Этап безопасной разработки нужно начинать с обучения разработчиков: подготовить гайды и рекомендации по безопасному программированию с примерами на ваших языках. Это поможет не допускать типовых и простых ошибок в начале пути. Так как разработка начинается с компьютера разработчика, необходимо выставить политики на уровень организации о том, каким должно быть рабочее место разработчика и какие локальные проверки должен проходить код, прежде чем он попадет в удалённый репозиторий (рис. 5).

Сборка и безопасность образов

Этап сборки и обеспечения безопасности образа состоит из следующих процессов.

- ◆ Проверка в CI-пайплайне.
 - Проверка безопасности исходного кода после того, как он попал в систему контроля версий. Инструменты SAST выполняют статический анализ исходного кода и его зависимостей, чтобы обнаружить распространённые уязвимости, например из списка OWASP Top Ten.
 - Проверка на наличие утёкших секретов с помощью Secret Detection, встроенного в Gitlab.
 - Сканирование на уязвимости Docker-образа. Сканер уязвимостей интегрирован в сервис Yandex Container Registry и настраивается с помощью веб-интерфейса. Это позволяет освободить время специалистов ИБ и DevOps.
 - SBOM содержит полный список всех компонентов и зависимостей, используемых в проекте ПО. SBOM помогает определить все составные части программного обеспечения, что позволяет контролировать безопасность и управлять рисками, связанными с использованием сторонних компонентов. На этом этапе генерируем его с помощью syft и подписываем с помощью Cosign как локальный файл, далее отправляем его в Object Storage.
 - Подпись образа и SBOM с помощью Cosign, интегрированного в Yandex KMS для обеспечения подлинности, целостности, доверия и соответствия требованиям в вашем программном обеспечении.
- ◆ Далее сканер уязвимостей можно настроить на сканирование Docker-образов в реестрах автоматически при загрузке или по расписанию либо встроить в пайплайн, как мы сделали выше.

◆ Audit Trails – это сервис для сбора и загрузки аудитных логов ресурсов Yandex Cloud (рис. 6).

Развёртывание и RUN-TIME

Ну, и наконец, этап развёртывания. Но и тут проверки не заканчиваются, мы проводим проверку безопасности приложения, которое запущено из собранного артефакта. Инструменты DAST (динамический анализ кода, метод «чёрного ящика») в этой фазе пытаются «сломать» приложение, имитируя действия злоумышленников (рис. 7).

В Run-time-этапе происходят непрерывные проверки безопасности приложения после развёртывания в production-среде. Инструменты в режиме реального времени мониторят открытые реестры известных уязвимостей и отправляют уведомление, обнаружив угрозу для приложения.

ЗАКЛЮЧЕНИЕ

SLSA призван защитить от атак на целостность цепочки поставок, число которых увеличилось за последние годы. После атак на SolarWinds и Codecov мы рекомендуем обратить внимание на необходимость создания инфраструктуры для защиты сложной цепочки поставок.

Как производители программного обеспечения, так и потребители могут извлечь выгоду из спецификаций SLSA. Производители могут придерживаться этих рекомендаций, чтобы повысить стандарты безопасности своих цепочек поставок программного обеспечения, а потребители могут использовать SLSA для принятия обоснованных решений о доверии пакету программного обеспечения.



Рисунок 7. Развёртывание

SECURITY CHAMPIONS

ГДЕ НАЙТИ ЧЕМПИОНОВ?



Андрей ЖАРКЕВИЧ
ведущий
рубрики, эксперт
«Антифишинг»

Разработка ПО всё больше напоминает бег в темноте по ледяным торосам. Маршрут вроде бы известен, но постоянно обнаруживаются новые препятствия. Менеджер проекта торопит разработчиков, потому что конкуренты уже анонсировали релиз. Разработчики никак не могут перейти на новую версию фреймворка, без которой проект не собирается. И тут неожиданно появляется безопасник, который заявляет, что не согласует выпуск новой версии, пока не устроят уязвимости.

В ходе разбирательств выясняется, что источник проблем в том, что безопасность и разработка существуют изолированно. Тем и другим хватает своих задач, но не находится ни времени, ни желания общаться.

Чтобы подружить разработчиков с безопасниками и сместить безопасность влево в жизненном цикле разработки ПО, придумали программу «чемпионов безопасности» (Security Champions).

В ЧЁМ ПРОБЛЕМА?

Массовая цифровизация вынудила многие компании к самостоятельному созданию программных продуктов. Взаимодействие со сторонними разработчиками занимает больше времени, чем внутренние процессы, в результате новые версии и новые продукты выпускаются позже. Конкуренты обгоняют и забирают себе клиентов, а это неприемлемо.

Результат мы наблюдаем уже сейчас. СберТех с полным правом называет себя одним из крупнейших разработчиков ПО в России. Приложения для банка Тинькофф, ВТБ и QIWI пишут тысячи собственных программистов. Миллионы строк кода превращаются в продукты, воплощающие бизнес-идеи. И всё было бы прекрасно, если не вспоминать про безопасность этих продуктов.

Все понимают, что безопасность софта важна, но руководство требует ускорения циклов выпуска программ, чтобы удовлетворить запросы пользователей. Сокращение сроков и повышение безопасности конфликтуют, превращаясь в противостояние разработчиков и специалистов по ИБ. Разработчикам некогда обучаться вопросам безопасности, да и обучать их некому: команды безопасности сами испытывают кадровый голод и вынуждены буквально сражаться за таланты.

Массовая потребность в безопасности в условиях ограниченности

ресурсов приводит к появлению «островов безопасности». ИБ-подразделение может разрабатывать политики и стандарты кодирования, но из-за нехватки ресурсов они так и останутся никому не нужными файлами где-то на внутреннем портале. Разработчики когда-нибудь узнают, что в компании есть руководство по безопасной разработке, а если в компании внедрён документооборот, даже поставят галочку «Ознакомлен». Но применять этот документ они вряд ли начнут. В результате забота о безопасности продуктов перемещается на более поздние этапы жизненного цикла разработки ПО. О Shift-Left Security и речи не идёт. Каждая обнаруженная проблема безопасности становится «золотой».

КАК ДОБАВИТЬ ИБ?

Приставить к каждому разработчику по безопаснику нереально. Внедрить принципы безопасной разработки в головы программистов силами ИБ-подразделения — сложная в реализации задача, потому что люди, занимающиеся информационной безопасностью, не могут масштабироваться на команды разработчиков.

Но если невозможно отправить безопасников «в программисты», значит, нужно отыскать среди разработчиков приверженцев идеи безопасности ПО, тех, кто готов делиться знаниями и вести за собой остальных, чемпионов.

ОТКУДА ВЗЯЛИСЬ ЧЕМПИОНЫ

Одно из первых упоминаний о чемпионах безопасности как о сотрудниках, распространяющих среди коллег принципы безопасного поведения, встречается в статье Selecting security champions Тренора Габриэль и Стивена Фернелла из Центра безопасности, коммуникаций и сетевых исследований университета Плимута, Великобритании, опубликованной в журнале Computer Fraud & Security в августе 2011 года.

Габриэль и Фернелл изучали, какими качествами должны обладать приверженцы идей безопасности, чтобы преодолеть сложившуюся в коллективе традицию пренебрегать требованиями ИБ и изменить поведение коллег. Таких людей они назвали чемпионами безопасности.

T. Gabriel and S. Furnell, «Selecting security champions», Computer Fraud & Security, vol. 2011, no. 8, pp. 8–12, 2011.

https://www.academia.edu/5444900/Selecting_security_champions



«ПОЯСА БЕЗОПАСНОСТИ» — УРОВНИ СЕРТИФИКАЦИИ ЧЕМПИОНОВ В ADOBE

В Adobe чемпионы безопасности заметно отличаются от «коллег по цеху» из других компаний. Это уже не просто люди, которые интересуются вопросами безопасности, посещают тренинги и другие мероприятия по ИБ. У Adobe более 200 продуктовых команд, и компания не в состоянии выделить персонального безопасника для каждой. Именно поэтому чемпионы по безопасности стали критически важным элементом разработки.

Одна из самых интересных сторон программы чемпионов по безопасности Adobe — требования к набору навыков сотрудника, который берёт на себя эту роль:

- ◆ обширные и глубокие знания о продукте своей команды;
- ◆ способность предвидеть потенциальные проблемы безопасности и риски в ходе разработки продукта;
- ◆ готовность влиять на изменения.

КТО СТАНЕТ ЧЕМПИОНОМ?

Выявленные чемпионы помогают улучшить коммуникацию между разработчиками и ИБ. Они знают «болевые точки» кодовых баз и культуры своих коллег, говорят с ними на одном языке и поэтому могут представить безопасность таким образом, чтобы она была принята как элемент рабочих задач, а не блажь ИБ-руководителя. В идеале чемпионы безопасности становятся ключевым элементом повышения зрелости процессов разработки безопасных приложений.

Стать чемпионом безопасности может любой член продуктовой команды, который готов стать её «со-вестью» в области безопасности и следить за проблемами, требующими экспертизы службы безопасности. Должность не имеет значения. «Агент влияния» ИБ не обязательно должен быть руководителем разработки или скрам-мастером. Главные требования к нему — систематическое участие в процессе разработки и понимание целей, процессов и культуры команды. Чемпионом может стать программист, тестировщик, архитектор и даже менеджер продукта.

Наличие «своих людей» в продуктовых командах помогает развивать ИБ-культуру и внедрять знания и опыт в области безопасности на более ранних этапах жизненного цикла разработки ПО. Чемпионы являются частью технической команды, поэтому они более естественно увязывают необходимые для безопасности моменты с требованиями бизнеса и инженеров. Они понимают требования, предъявляемые к быстрым циклам выпуска релизов, и могут сформулировать, что работает и что не работает в существующем процессе. Чемпионы по безопасности работают над решениями, которые удовлетворяют как критериям безопасности, так и инженерным требованиям, тем самым снижая трение и способствуя развитию культуры безопасности в организации.

ПЛАН ДЕЙСТВИЙ

Чемпионы безопасности не появляются сами по себе. Здесь не обойтись без административного ресурса. Программу должны поддерживать на самом высоком уровне. Без этого инициатива станет просто бесполезным набором лозунгов.

Представим ситуацию, когда чемпион предлагает всем разработчикам

пройти обучение по защите от SQL-инъекций или указывает, что поступившие от ИБ требования реализованы лишь частично. Но вместо поддержки коллеги стали упрекать его в саботаже и принижать значимость проблемы, пугая возможным срывом сроков сдачи проекта. Важно, чтобы в таких обстоятельствах он мог обратиться к руководству для урегулирования вопроса.

Кроме поддержки, план запуска программы чемпионов должен содержать следующие пункты:

1. Цели — зачем компании эта программа.
2. Ожидания — какие результаты она должна принести.
3. Способы выявления чемпионов.
4. Мотивация.
5. Обучение.

Остановимся на этих пунктах подробнее.

Цели программы чемпионов

Безопасность программного обеспечения не повышается автоматически, как только в команде появляется чемпион по безопасности. Прежде всего, необходимо понять текущую ситуацию с безопасностью и определить области, в которых

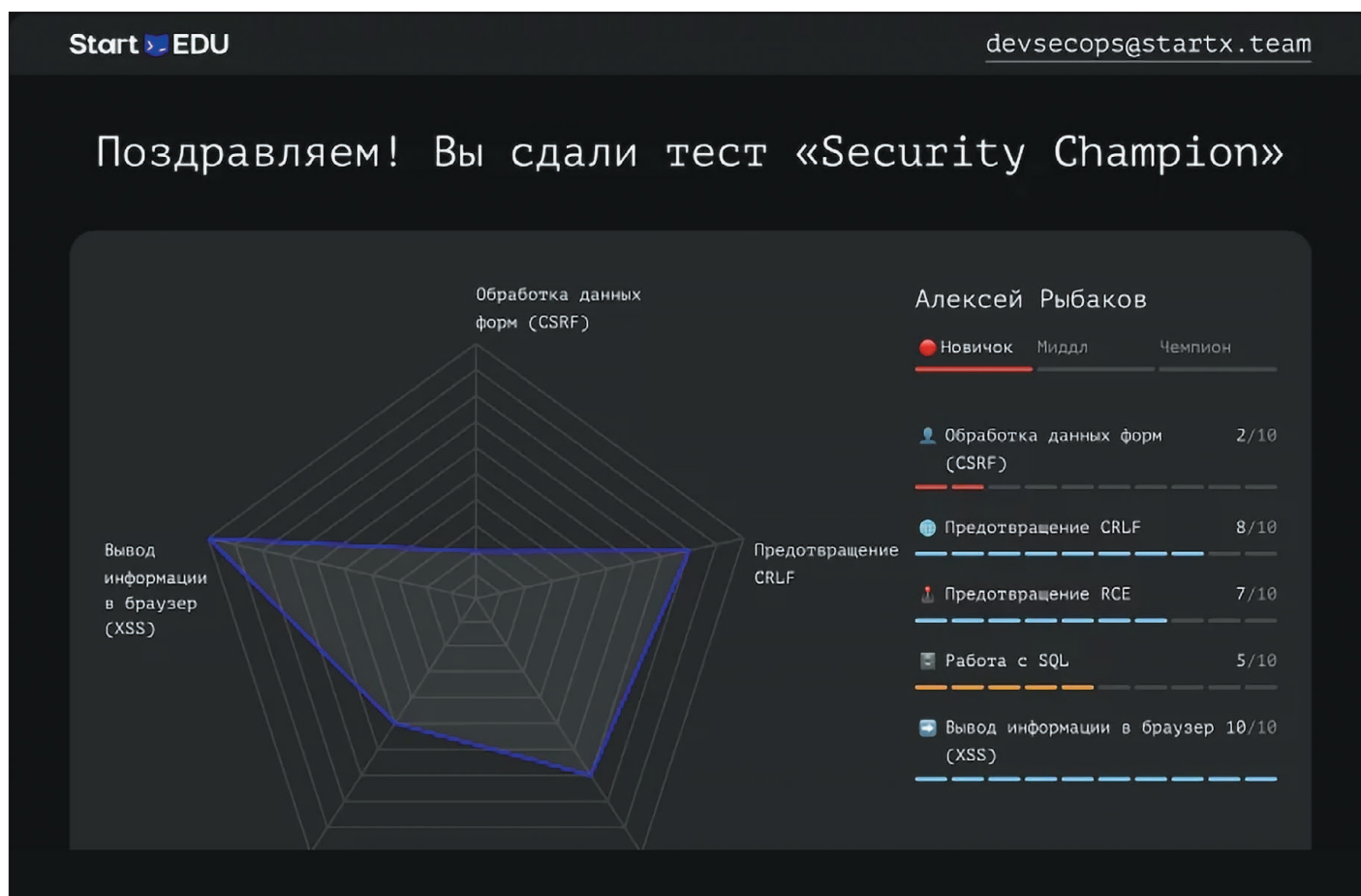


Рисунок 1. Тест Security Champions. Составлен на базе 20 реальных взломов известных приложений. Задания отличаются по сложности и проверяют пять важных навыков безопасной разработки

чемпион может помочь. Это могут быть, например, внедрение стандартов безопасного кодирования, помощь в согласовании требований безопасности или просто привлечение внимания разработчиков к устранению уязвимостей.

Ожидания

В задачи чемпионов не входит выявление ошибок вместо тестировщиков или выполнение других задач ИБ-подразделения. Их основная ценность заключается в обмене знаниями, распространении передового опыта и помощи в принятии решений. По мере развития навыков они могут помогать определять лучшие практики, писать тестовые примеры и следить за состоянием открытых проблем.

Как выявить чемпионов

Никто не любит, когда ему поручают дополнительную работу, поэтому большой ошибкой будет назначать

чемпионов приказом по компании. Это противоречит самой идее программы внедрения культуры безопасности в продуктовые команды.

Необходимые для чемпиона качества — инициативность, интерес к вопросам безопасности и профессионализм. Иногда чемпионы заметны сразу, но бывает, что они оказываются слишком скромными, чтобы предложить свою помощь команде.

В этом случае выявить их поможет специализированное тестирование, подобное тесту Security Champions, разработанному командой Start EDU (рис. 1).

Тест составлен на базе 20 реальных взломов известных приложений. Задания отличаются по сложности и проверяют пять важных навыков безопасной разработки.

Результаты тестирования могут использоваться не только для выявления настоящих чемпионов, но и для создания духа конкуренции,

мотивации разработчиков к повышению своих ИБ-навыков.

Мотивация

Роль чемпиона безопасности означает, что человек берёт на себя дополнительные обязанности и ответственность. Поэтому нужно крайне серьёзно подойти к способам мотивации сотрудников, готовых помочь ИБ-службе.

В качестве мотивации может выступать не только прибавка к зарплате, но и нематериальные методы, например.

- ♦ Участие в мероприятиях. Чемпионы по безопасности могут за счёт компании посещать конференции по безопасности, участвовать в CTF и хакатонах.

- ♦ Признание и поощрение. Важно признавать достижения чемпионов по безопасности, например регулярно сообщать о достигнутых результатах в информационных бюллетенях. Для обозначения прогресса чемпиона по

безопасности можно использовать геймификацию с помощью уровней. Это поможет чемпиону по безопасности иметь то, над чем нужно работать, и отмечать свои успехи на пути к безопасности. Можно даже выделить чемпиона по безопасности как отдельную должность, чтобы мотивировать сотрудников на вступление в организацию.

♦ Измерение прогресса. У чемпионов по безопасности могут быть цели и ключевые результаты (OKR), которые необходимо достичь в области безопасности. Таким результатом может быть, например, выявленный процент критических уязвимостей, количество мероприятий по моделированию угроз, пройденные модули обучения по безопасности.

Обучение

Большая часть чемпионов безопасности приходит из отдела разработки. Их необходимо обучать тем вопросам, в которых безопасность нуждается в дополнительной помощи. Как минимум для них должно быть приоритетным обучение безопасному кодированию на более высоком уровне помимо того, которое требуется для всех разработчиков. Повышению их квалификации может способствовать участие в отраслевых мероприятиях.

В некоторых организациях, успешно реализующих программы подготовки чемпионов по безопасности, существуют формализованные уровни. Например, в Adobe имеется учебный план и официальная сертификация в виде цветных поясов, как в боевых искусствах. Получение зелёного пояса относительно просто, открыто для любого сотрудника и достигается с помощью электронных курсов. Сертификация на коричневый и чёрный пояса требует от сотрудников выполнения «одного или нескольких проектов в области безопасности, приносящих непосредственную пользу компании и клиентам» и накопления баллов для получения каждого пояса.

ЧТО МОЖЕТ ПОЙТИ НЕ ТАК

Кажется логичным повысить чемпионам зарплату, ведь эти люди приносят больше пользы, чем другие члены

команды, выполняют больше обязанностей и принимают на себя ответственность. К сожалению, у такого решения могут быть неприятные последствия: высокая зарплата может привлечь любителей лёгких денег. Если у них окажется поддержка в руководстве и прокачанные навыки офисных интриг, велика вероятность, что в чемпионы попадут совсем не те люди, которые нужны компании.

Ещё одна ошибочная практика — назначить ответственных за безопасность приказом и успокоиться, рассчитывая, что они справятся сами. К сожалению, пользы такое решение не приносит.

Пример из жизни. Около 15 лет назад в одном из трёх крупнейших российских банков возникла проблема: информационных систем и ресурсов стало слишком много, так что ИБ-подразделения головной конторы и филиалов перестали справляться с бумажной работой. Чтобы помочь ИБ, решили в каждом отделе назначить специального человека — администратора ИБ-подразделения, АИБа. В обязанности АИБов входило оформление заявок на подключение новых сотрудников к системам, доступов к различным ресурсам, блокировки учётных записей на время отпуска, на отключение уволенных, согласование этих заявок с ИБ, инвентаризация доступов и даже инструктаж коллег по вопросам ИБ.

Никакого обучения АИБов не проводили. Мотивация была только в виде наказаний. Результат не заставил себя долго ждать. Очередной внутренний аудит выявил многочисленные нарушения ИБ-регламентов: АИБы не оформляли заявки на отключение уволенных или ушедших в декрет сотрудников, не делали инвентаризацию прав доступа, потому что не понимали, что это такое и как её проводить.

В итоге полезная идея была уничтожена её неграмотной реализацией.

РЕЗЮМЕ

Культура кибербезопасности должна стать неотъемлемой частью процессов всех организаций независимо от сферы их деятельности. Для

компаний, которые занимаются разработкой программных продуктов, это особенно важно, поскольку напрямую отражается на эффективности бизнеса: устранение проблем безопасности в готовом продукте обходится намного дороже, чем «прививка от уязвимостей» на этапе проектирования.

Реализовать принцип Shift-Left Security, переместив заботу о безопасности софта как можно ближе к началу жизненного цикла, мешают следующие факторы:

♦ разработчики не изучают вопросы безопасности, потому что воспринимают их как что-то постороннее, а времени и так не хватает;

♦ у безопасников не хватает квалифицированных специалистов, чтобы внедрить принципы безопасной разработки в продуктовых командах и обучить разработчиков.

Выход из ситуации состоит в том, чтобы выявить в продуктовых командах приверженцев принципов безопасной разработки ПО, обладающих необходимыми компетенциями и готовых продвигать этот подход среди коллег, чемпионов безопасности. Эти люди обеспечивают коммуникацию между ИБ и продуктовыми подразделениями, выступая в роли носителей культуры кибербезопасности.

Поскольку эта деятельность требует дополнительных усилий, нужна адекватная мотивация, чтобы чемпионы чувствовали, что их работа оценивается по достоинству. Простая прибавка к зарплате не слишком эффективна, поскольку может привлечь некомпетентных людей, заинтересованных исключительно в увеличении своего дохода. Лучшие результаты показывают такие методы, как оплата участия чемпионов в профильных ИБ-конференциях, направление на обучение, а также публичное признание заслуг.

Помочь оценить уровень знаний потенциальных чемпионов безопасности можно с помощью специализированных тестов. Результаты тестов могут стать стимулом для повышения ИБ-компетенций участников продуктовых команд и элементом геймификации.

МОШЕННИЧЕСТВО НА САЙТАХ ЗНАКОМСТВ

КАК РАСПОЗНАТЬ «СПЕКТАКЛЬ»



Роман ЖУРАВЛЁВ
специалист отдела
аудита защиты
приложений ИБ VK

Хотя многие продолжают опасаться дейтинговых сервисов, считая, что там их ждёт не любовь, а мошенник, популярность российских приложений и сайтов знакомств продолжает расти на фоне ухода зарубежных конкурентов. Опросы показывают, что россияне искренне верят, что могут найти пару в любом возрасте и современные технологии помогут им в этом. Появление новых дейтинг-стартапов с

альтернативными механиками по поиску вторых половинок доказывает популярность этого сегмента рынка.

Киберпреступники, естественно, используют самые популярные площадки для реализации своих мошеннических схем. И хотя известные сервисы внедряют различные технологические барьеры для злоумышленников, последние успевают моментально адаптироваться. Находят жертв с помощью методов социальной инженерии, с лёгкостью применяют свои схемы среди ищущих отношений, ведь нет ничего проще ввести в заблуждение тех, кто только и ищет повода кому-то довериться.

СХЕМЫ ЗЛОУМЫШЛЕННИКОВ

Работа с фокус-группами «жертв интернет-мошенничества» на дейтинговых платформах показала, что мошенники продолжают использовать конструктор схем, в котором они лишь меняют некоторые детали

в зависимости от контекста и ограничений платформы.

Например, недавно эксперты по информационной безопасности обнаружили огромное количество поддельных сайтов популярных театров, музеев и даже ресторанов. Схема мошенников выстроена грамотно: в приложении для знакомств жертва начинает общаться с девушкой или юношей, после недолгого диалога они решают встретиться, и удача — именно завтра в популярном театре города будет классный спектакль, куда новый знакомый как раз уже купил билет. Инициативный собеседник сразу предлагает уточнить, есть ли ещё билеты. Далее жертва получает от собеседника ссылку или даже QR-код на оплату билетов, и надо спешить скорее, потому что это билет на соседнее место и его кто-то может моментально выкупить. После перехода по ссылке и оформления покупки происходит переадресация на поддельную форму оплаты. Настоящая функциональность такой формы — P2P-перевод. P2P-перевод (peer-to-peer или person-to-person) — денежный перевод от одного пользователя к другому, без участия банка или других посредников. Понятно, что после списания денег со счёта общение с новым знакомым вдруг прерывается навсегда.

Этот вид мошенничества прошёл небольшую эволюцию с расцвета дейтинговых сервисов в 2010-х годах, когда можно было обнаружить целые фейковые сайты. Тогда основными предложениями для выманивания денег были покупка билетов (нужны деньги, чтобы приехать и встретиться лично), мобильного интернета (заканчиваются деньги и нужно срочно пополнить счёт), размещения по приезду (потерялся багаж с деньгами).

Креативность киберпреступников не имеет границ — как в придумывании поводов, так и в техническом исполнении. Порой только опытные специалисты смогут отличить фейк от оригинала. Многие жертвы преступников спустя время осознают всю странность разграниченной ситуации и тот факт, что они могли бы не переводить деньги, поддавшись желанию «успеть», «помочь» или «получить». Эта игра на чувствах и азарте продолжает реализовываться изо дня в день, накапливая на счетах преступников миллионы даже за счёт маленьких взносов — оплатить такси, билет на поезд, купить лекарства и т.д. Такие схемы чаще используются мошенниками-дилетантами, более опытные же играют по-крупному или выуживают конфиденциальную информацию для реализации более сложных мошеннических схем.

Например, мужчина хочет отправить подарок, поэтому нужно прислать адрес или просто ввести на сайте службы доставки (фишинговая ссылка с поддельной формой). Или же собеседник отправляет жертве фишинговую ссылку, прося проголосовать или посмотреть товар, а после перехода по ссылке автоматически запускается бот для атаки на аккаунт в мессенджере или соцсетях. А в специализированных приложениях 18+ популярны иные способы мошенничества. Собеседник может попросить жертву сделать интимное фото так, чтобы было видно лицо, с целью удостовериться в подлинности собеседника. После отправки таких фото запускается схема по шантажу и вымогательству крупных сумм. Кроме того, пользователи могут столкнуться и с реальными преследованиями: по данным «Лаборатории Касперского», каждый пятый россиянин сталкивался со stalkingом и угрозами о сливе личной информации.

Также киберпреступники пользуются фидами разработчиков дейтинговых сервисов, используя их инструменты рекламы и платной функциональности в своих целях. Например, мастерски копируя:

- ◆ подарки, которые «выделят тебя из сотен лайков»;
- ◆ подписки на дополнительные функции:
 - просмотр лайков, когда пользователь видит, кто поставил ему лайк, если такая функциональность не предусмотрена по умолчанию;
 - приоритетные лайки или анкета в топе, когда показывают анкету пользователя одной из первых в предлагаемых для других пользователей;
 - напиши первым, когда пользователь получает возможность написать сообщение другому пользователю до того, как случится метч.

КАК ПРИЛОЖЕНИЯ ЗАЩИЩАЮТ СВОИХ ПОЛЬЗОВАТЕЛЕЙ?

Сейчас разработчики сервисов для знакомств уделяют всё больше внимания безопасности пользователей, внедряя дополнительные способы проверки и аутентификации.

◆ Привязка профиля к email или номеру телефона. Привязка к номеру телефона более зрелая с точки зрения безопасности, хотя оба варианта не предотвращают мультиаккаунтинг.

◆ Верификация профиля с помощью отправки селфи в самом приложении по заданным правилам: с определённым жестом или ракурсом. Далее приложение сравнивает фото в анкете и фото, которое загружает

К сожалению, ни один сервис не сможет полноценно обеспечить безопасность пользователей, если они сами не будут предпринимать шаги для защиты самих себя

пользователь. Но этот способ не защищает на 100%, потому что злоумышленники могут попросить кого-то создать верифицированный профиль за награждение и передать им логин и пароль.

- ◆ Запрет скриншотов диалогов, анкет, фото и видео в диалогах.

- ◆ Предупреждение о том, что переход в любую другую соцсеть с собеседником не гарантирует безопасность.

- ◆ Запрет на вставку текста в набираемое сообщение и использование ссылок.

- ◆ Блокировка аккаунтов при упоминании слов «деньги», «оплата» и прочих в диалогах.

- ◆ Исчезающие фото и видео, когда внедрены ограничения на доступ к собеседнику и просмотру по времени и количеству раз.

Но, к сожалению, ни один сервис не сможет полноценно обеспечить безопасность пользователей, если они сами не будут предпринимать шаги для защиты самих себя.

КАК ЗАЩИТИТЬ СЕБЯ?

Каждый пользователь несёт персональную ответственность за свою безопасность, регистрируясь в дейтинг-приложении. Поэтому всегда критично относитесь к получаемой информации и оценивайте риски: насколько опасна для меня публикация каких-либо данных? Вот несколько базовых рекомендаций, которые будут полезны в общении не только в дейтинг-сервисах, но и в социальных сетях в целом.

- ◆ Обращайте внимание, насколько подробно вы делитесь своей персональной информацией на страницах в социальных сетях и профилях ваших мессенджеров. Овершеринг помогает злоумышленникам точнее составить ваш психологический портрет и подобрать нужные рычаги воздействия. Даже на основе фразы «успех — победа» злоумышленник сможет сложить мнение о вас и предложить, например, инвестицию в интересный проект за пару тысяч рублей.

- ◆ Изучите профиль собеседника, ведь интернет помнит всё. А далее, если решите

продолжить общение на альтернативной площадке, также придерживайтесь рекомендаций безопасности, которые внедрены в сервис. Например, социальные сети научились предупреждать о «подозрительном собеседнике», то есть, если специальные алгоритмы заметили подозрительную активность профиля, они автоматически пришлют оповещение. Далее вы уже сможете отправить жалобу на собеседника и внести его в чёрный список одной кнопкой.

- ◆ Старайтесь обращать внимание на верифицированные профили: шансов, что по ту сторону окажется мошенник, будет меньше. Ведь совокупность подтверждённого фото, имени, телефона и другой информации — персональные данные. Значит, сузить круг поиска до конкретного человека гораздо легче. Особенно благодаря таким инструментам, как нейросети и телеграм-боты.

- ◆ С осторожностью относитесь к любым неожиданным сообщениям, которые сулят вам невероятную выгоду. Чаще всего под благовидным предлогом вас мотивируют перейти по фишинговой ссылке и ввести персональные данные. Несмотря на все усилия ИБ-сообщества, у пользователей сохраняется тенденция использовать один пароль для входа на многие ресурсы. Получив ваши данные, мошенник может получить доступ к вашим личным кабинетам на многих легитимных ресурсах.

- ◆ Всегда обращайте внимание на стиль общения и письма. Большинство людей не готовы на внезапные и быстрые встречи после пары сообщений. Обычные пользователи испытывают такой же страх встретить мошенника, как и вы.

- ◆ Встречайтесь на нейтральных территориях и выбирайте для встречи людные места, в которых в первую очередь можно разговаривать.

- ◆ Не забывайте о цели общения в сервисах знакомств и не поддавайтесь эмоциям. Если вы ищете отношения, а вам предлагают интимную встречу или бизнес-проект — как бы ни было велико желание, помните: такое предложение может поступить любому.

- ◆ Кроме того, стоит сразу же насторожиться, если ваш собеседник настойчиво переводит общение в любой мессенджер или социальную сеть, объясняя это привычкой и удобством функциональности других платформ. Это может быть знаком того, что мошенники хотят реализовать схему, которую не пропустят ограничения безопасности дейтинг-сервиса.



Российский стек ПО для создания ИТ-инфраструктур любого масштаба



Сервер. Десктоп. Мобайл.
Защищенная ОС



Система
для управления
службой каталогов



Развертывание
решений
по клику



Облачная
виртуализация



Серверная
виртуализация



Всесторонняя
помощь
при проектах
миграции



Инфраструктура
виртуальных
рабочих мест



Платформа
для биллинга
облачных
сервисов



СУБД и
платформа для
администри-
рования
и мониторинга



Корпоративная
почта



Средство
резервного
копирования



Платформа
для управления
физической
инфраструктурой



Мобильное
рабочее место



Провайдер
технологических
продуктов для
обучения и развития
сотрудников



Сервис для
разработчиков со
всеми инструментами
для организаций и
частных пользователей

- широкая экосистема совместимых программных и аппаратных решений
- безопасная разработка
- стабильность и защита ИТ-инфраструктур
- инструменты автоматизации и механизмы миграции
- быстрое и легкое развертывание ПО
- комплексное сопровождение проектов внедрения
- круглосуточная техническая поддержка

Более 2,5 млн
инсталляций
ОС Astra Linux



Российские
ИТ-решения
gk-astra.ru
8(495) 369-48-16
info@astralinux.ru

Реклама

ПО СЛЕДАМ ПРЕСТУПЛЕНИЙ

КТО И КАК ДОЛЖЕН ПОМОЧЬ СЛЕДСТВИЮ?



**Василий
ОКУЛЕССКИЙ**
к. т. н., вице-президент
по информационной
безопасности
ЦМРБанка

Существует множество способов отъёма денег у честных граждан. Банковские безопасники привычно называют их мошенничеством, коллеги из правоохранительных структур — кражами. А как правильно? Вопрос не праздный, поскольку и то и другое — это разные статьи Уголовного кодекса со всеми вытекающими последствиями. Но прежде чем классифицировать преступление, преступника надо поймать. И тут очень многое зависит от поведения жертвы.

На первый взгляд, схема действий пострадавшего проста: звонить в банк, заблокировать карту, сообщать о несогласии с проведёнными операциями, и сразу в полицию — писать заявление в отношении неустановленных лиц.

И всё же, чтобы дела открывались и расследовались быстрее, пока ещё след не остыл, потерпевшему надо максимально сохранить, «закрепить» и предъявить улики. Попробуем разобраться, что в таких ситуациях является существенным и как граждане должны поступать, чтобы помочь следствию.

ЭТАПЫ АТАКИ

Рассмотрим классические «технические» схемы интернет-мошенничеств, при которых злоумышленники, используя вредоносное ПО, получают либо удалённый доступ к компьютеру жертвы и проводят мошеннические операции непосредственно с её компьютера, либо, используя удалённый токен, проводят операции со своего компьютера. В таких схемах могут быть особенности, например, деньги сначала переводятся на транзитный счёт,

а с него уже на мошеннический. Транзитный счёт может быть непричастным к преступлению, но всё же скомпрометированным.

Разобьём «техническую» схему на этапы.

Этап 1. Разведка. «Охотники» начинают поиск жертвы. В простом варианте они покупают в даркнете информацию о скомпрометированных учётных записях клиентов, данные бот-сетей, в более продвинутом — собирают открытую информацию в интернете.

Этап 2. Предварительные «танцы». Получив установочные данные для атаки, «охотник» ищет доступ к компьютеру жертвы. Инструменты этого этапа очень разные, не будем на них останавливаться, нам важен результат: на компьютере жертвы устанавливается вредоносное ПО, позволяющее видеть всё, что происходит на ПК, и совершать в нём противоправные действия.

Этап 3. Собственно атака. Злоумышленник каким-либо техническим или иным способом получает доступ к компьютеру и личным данным, включая пин на токен с электронной подписью. Затем либо устанавливает «надзор» за движением денежных средств через счёт жертвы, либо формирует ложное платёжное поручение, либо вносит изменения в реквизиты уже сформированного, но не отправленного, либо блокирует проведение важных платежей, вносит изменения в личный кабинет плательщика и т.д. и т.п. В такой ситуации все электронные сообщения злоумышленника в банке воспринимаются как отправленные самим клиентом, так как формально выполняются все признаки перевода от имени клиента: есть легитимная ЭП, IP-адрес отправителя, Fingerprint компьютера и т.д.

Этап 4. Завершение атаки на клиента. Основная цель этого этапа — скрыть следы деятельности на компьютере жертвы и оттянуть время обнаружения преступления.

ЧТО ДОЛЖЕН СДЕЛАТЬ КЛИЕНТ В ПЕРВУЮ ОЧЕРЕДЬ

На каждом этапе злоумышленники оставляют цифровые следы на компьютере клиента: изменения в реестре, данные системных

логов, данные логов приложений, изменения в программах, данных... То есть все те следы, которые могут помочь восстановить картину произошедшего. И надо помнить, что некоторые из этих следов по разным причинам сравнительно быстро исчезают.

В таких условиях самым важным действием для жертвы становится отключение питания компьютера, при котором сохраняется дамп на момент отключения. Обычно современные накопители, особенно SSD, легко переносят такое издевательство. Операция не гарантирует сохранности системы и приложений, нормальной работы компьютера после включения и также не гарантирует 100% сохранения цифровых следов, однако с высокой долей вероятности эта процедура позволит максимально их сохранить. При этом важно помнить, что непосредственное исследование самого накопителя обязательно приведёт к потере или части следов, или их всех. Поэтому самостоятельное исследование крайне не рекомендуется. В специальных лабораториях в таких случаях делают побитные копии накопителя, которые затем и подвергают исследованиям без риска потерять первичную информацию.

Ещё один нюанс: при снятии накопителя с компьютера необходимо обеспечить целостность накопителя и отсутствие постороннего доступа, а также зафиксировать время снятия.

Соблюдение этих нехитрых правил поведения при выявлении признаков несанкционированного доступа к компьютеру или данным на нём поможет сохранить важнейшую улику при выявлении и задержании злоумышленника. А триггером поимки преступника станет скорейшее обращение в банк для блокировки дальнейших платежей и возврата денежных средств, переведённых без согласия клиента, и написание заявления в полицию о совершённом преступлении.

КУДА ОБРАЩАТЬСЯ ПОТЕРПЕВШЕМУ

В общем случае необходимо немедленно обратиться:

- ♦ в службу технической поддержки банка или платёжной системы, осуществляющей переводы денежных средств, чтобы заблокировать счёт;
- ♦ в полицию по месту проживания;
- ♦ получить консультацию можно по телефону горячей линии 8 800 222 74 47 или на сайте Министерства внутренних дел РФ;
- ♦ в Роскомнадзор, осуществляющий контроль за деятельностью организаций по

оказанию услуг в области электронных технологий.

Если есть контакты, надо обратиться в территориальное отделение специализированного подразделения МВД. Правонарушениями в сфере компьютерной информации занимается специализированное подразделение МВД России – управление «К».

При обращении в полицию с заявлением необходимо сообщать как можно более полную информацию о злоумышленниках, в частности, их адрес сайта, расчётный счёт, адрес электронной почты, номера телефонов, электронных кошельков и т.д. И вот здесь очень пригодится накопитель, снятый с компьютера.

Заявление пишется, как правило, по установленной форме. Из документов для написания заявления требуется лишь паспорт гражданина РФ. По правилам коллеги из МВД в течение 3 рабочих дней должны принять соответствующее решение. Понятно, что чем быстрее начнётся производство, тем больше шансов поймать злоумышленников.

Их действия могут квалифицироваться Уголовным кодексом либо как кража (ст. 158 УК РФ), либо как мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путём ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей по п. 1 ст. 159.6 УК РФ. Что именно можно указать в самом заявлении, надо уточнять в полиции.

ДОПОЛНИТЕЛЬНЫЕ СЛЕДЫ

Не стоит забывать, что кроме вышеназванных есть ещё следы, которые помогут найти «охотников». Они появляются там, где злоумышленники будут пытаться вывести похищенные деньги, — в банкоматах, интернет-магазинах, мобильных приложениях при переводе в крипту... Поиск и фиксация этих следов — это уже домашнее задание для соответствующих подразделений Банка России, банков, платёжных систем, операторов платёжных систем, т.е. всех тех организаций, через которые бегают электроны, перенося информацию о переводах денежных средств. Эта сфера должна регулироваться и координироваться совместно Банком России и МВД.

Жизнь такую задачу поставила. Что дальше?

ПРЕСТУПЛЕНИЕ БЕЗ НАКАЗАНИЯ

НАБРОСОК КОММЕНТАРИЕВ К СТАТЬЯМ 159 УК РФ



Сергей ВИХОРЕВ
советник генерального
директора
по информационной
безопасности
IT Expertise

Кража или мошенничество? Да, действительно, вопрос не праздный. И думается, к тому моменту, когда преступник будет пойман, правильно было бы с этим вопросом определиться. В связи с этим хочу поделиться соображениями по поводу юридического казуса.

ИНФОРМАЦИЯ — НЕ СОБСТВЕННОСТЬ

Итак, статья 159.6 УК РФ. Мошенничество в сфере компьютерной информации:

«1. Мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путём ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей...»

Комментарии юристов к этой статье, на мой взгляд, не всегда правильны. Например, есть такой комментарий: «Согласно ст. 6 Федерального закона от 27.07.2006 №149-ФЗ „Об информации, информатизации и о защите информации“ информационные ресурсы находятся в собственности юридических и физических лиц, включаются в состав их имущества, на них распространяется действие гражданского законодательства»¹.

Этот тезис уже в самом начале содержит фактическую ошибку: информация здесь приравнивается к имуществу, а также говорится,

что она находится в собственности. Но это далеко не так, это было бы справедливо до 2006 года, когда информация упоминалась в ст. 128 ГК РФ как объект гражданского права. Сегодня такая ошибка может иметь существенные последствия.

Согласно ст. 128 ГК РФ «Объекты гражданских прав», «К объектам гражданских прав относятся вещи (включая наличные деньги и документарные ценные бумаги), иное имущество, в том числе имущественные права (включая безналичные денежные средства, бездокументарные ценные бумаги, цифровые права); результаты работ и оказание услуг; охраняемые результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации (интеллектуальная собственность); нематериальные блага». Обратите внимание, в действующей редакции ГК РФ информация выведена из числа объектов гражданского права. Объяснения, почему это так, есть в интернете², и насколько это справедливо, не мне судить, хотя я не могу полностью с этим согласиться. Между тем будем опираться на действующий закон.

СОБСТВЕННИК — НЕ ОБЛАДАТЕЛЬ

Понятия «собственник» и «обладатель» не идентичны.

Собственнику принадлежат права владения, пользования и распоряжения своим имуществом³. Право собственности — наиболее важное вещное право. Оно является исключительным и абсолютным, так как точно известен собственник (управомоченное лицо), все остальные лица по отношению к собственнику выступают в качестве обязанных. Право собственности — закреплённая законом возможность лица по своему усмотрению владеть, пользоваться и распоряжаться принадлежащим ему имуществом, одновременно принимая на себя бремя и риск его

¹ Источник: <https://stykrf.ru/159-6>.

² Проблема отнесения информации к категории объектов гражданского права — Объекты гражданских прав (vuzlit.com)

³ ГК РФ, ст. 209, ч. 1.

содержания⁴. Речь идёт об имуществе, которое имеется в наличии на время существования права собственности и которое может быть индивидуализировано и присвоено собственником с исключением всех других лиц от обладания им.

Вместе с тем обладателем информации признаётся лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам⁵. То есть если собственник всегда один и только один, то обладателей информации может быть сколь угодно много, если информация получена на законных основаниях.

Пример на яблоках: я купил в магазине диск с любимым исполнителем музыки. Я стал обладателем информации, записанной на этом диске, но и автор, и исполнитель также остаются обладателями...

Следовательно, информация не может находиться в собственности ни юридических, ни физических лиц и не может быть отнесена к имуществу. Гражданский оборот информации, по всей видимости, регулируется другими правами, например интеллектуальным правом.

Что из этого следует? То, что ст. 159.6 действует только и только тогда, когда мошеннические действия привели к хищению именно чужого имущества или приобретения права на чужое имущество, а не информации.

Пример на яблоках: Некто Имярек путём вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации получил доступ к чужому аккаунту и узнал чужой пароль доступа к личному компьютеру, где хранились данные о кредитной карте жертвы и её пин-коде. Следуя дефиниции ст. 159.6 УК РФ, такое деяние не может считаться преступлением, так как хищения чужого имущества или приобретения права на чужое имущество в результате его действий не произошло (пароль, как информация, не является имуществом). Применить в этом случае дефиницию ст. 272 КУ РФ также не получится, так как, хотя и произошёл неправомерный доступ к компьютерной информации, но, к сожалению, повторюсь, пароль не является информацией, охраняемой по закону.

Теперь попробуем развить ситуацию. Этот самый Имярек, который узнал чужой пароль,

посредством даркнета продал эту информацию другому лицу, назовём его Имярек-2. В рамках законодательства Имярек, конечно, поступил плохо, разгласив информацию, которую можно отнести к частной и личной тайне (разглашение персональных данных в диспозиции ст. 13.11 КоАП РФ здесь неприменимо, так как она касается оператора персональных данных). Однако, к сожалению, законодательные нормы и положения определения частной, личной и семейной тайны не дают и не раскрывают их содержание. Что порой затрудняет отнесение некоторой категории сведений к таковым, а также делает невозможной адекватную защиту такой информации средствами уголовного судопроизводства.

Так вот, Имярек-2 использовал полученную от Имярека информацию и произвёл некоторую транзакцию, сняв деньги жертвы через банкомат. Казалось бы, здесь вполне можно применить ст. 159.3. УК РФ «Мошенничество с использованием электронных средств платежа»⁶. Но эту статью нельзя рассматривать автономно от ст. 159 УК РФ, где даётся определение понятия «мошенничество» как хищения чужого имущества или приобретения права на чужое имущество путём обмана или злоупотребления доверием. Но обман предусматривает сознательное введение потерпевшего в заблуждение. То есть, согласно диспозиции ст. 159.3, необходимо обязательно ввести в заблуждение жертву. Но Имярек-2 даже может и не знать жертву. И кого в данном случае он обманул? Получается, что банковскую систему, хотя и это не факт, ведь информация была введена правильная, да и такая система сама по себе не может быть «потерпевшей».

В действиях Имярек-2 нет обмана и, следовательно, нет мошенничества, и ст. 159.3 УК РФ в данном случае неприменима. Получается казус: преступление в виде хищения денег есть, а наказать нельзя. Именно поэтому я считаю, что такие преступления необходимо квалифицировать по ст. 158 УК РФ и, более того, по части 2б: с незаконным проникновением в помещение либо иное хранилище.

⁶ В соответствии с Законом о национальной платёжной системе электронное средство платежа – это средство и/или способ, которые позволяют клиенту оператора по переводу денежных средств составлять/удостоверять/передавать распоряжения для перевода денежных средств в рамках применяемых форм безналичных расчётов с использованием информационно-коммуникационных технологий, электронных носителей информации (в том числе платёжных карт), а также других технических устройств (ч. 19 ст. 3 Федерального закона от 27.06.2011 №161-ФЗ).

⁴ Гражданское право: Учебник. 2-е изд., перераб. и доп. / Отв. ред. Е. А. Суханов. М. : Волтерс Клувер, 2003. Т. 1

⁵ ФЗ-149, ст. 2, п. 5.

РЕГУЛЯТОРЫ ВСЕХ СТРАН, УЖЕСТОЧАЙТЕСЬ!

НОРМАТИВНЫЕ ТРЕБОВАНИЯ В СФЕРЕ КИБЕР-
БЕЗОПАСНОСТИ СТРЕМЯТСЯ К ЗАЩИТЕ КИИ, СУЛЯТ
ОГРОМНЫЕ ШТРАФЫ И УГОЛОВНЫЕ НАКАЗАНИЯ

Марина БРОДСКАЯ
обозреватель BIS Journal

КЛАССИФИКАЦИЯ ИНЦИДЕНТОВ И КАРАТЕЛЬНЫЕ МЕРЫ

В декабре 2023 года Администрация киберпространства Китая (САС) опубликовала для обсуждения проект требований по формированию отчётности об инцидентах кибербезопасности. В проекте указывается, что кража информации о национальной безопасности должна быть признана серьёзным инцидентом, а сокрытие такого происшествия будет строго караться, пишет портал Global Times.

По данным САС, документ призван стандартизировать отчётность об инцидентах кибербезопасности и сократить потери и ущерб, причиняемые киберинцидентами.

В документе уточняется, что операторы должны оперативно инициировать планы реагирования на чрезвычайные ситуации для устранения инцидентов. Согласно рекомендациям, о крупных, серьёзных или чрезвычайно серьёзных инцидентах следует сообщать в течение одного часа.

Инцидент сетевой безопасности считается чрезвычайно серьёзным, если приводит к отказу системы и потере возможности обработки бизнес-процессов.

В классификацию инцидентов также включены ситуации, при которых информация, содержащая государственную тайну, конфиденциальные сведения и данные, теряется, украдена или сфальсифицирована. Такой инцидент представляет особо серьёзную угрозу национальной безопасности и социальной стабильности.

Другие события, определённые как чрезвычайно серьёзные инциденты, определяются по следующим признакам:

- ♦ недоступность веб-сайтов партийных и правительственных порталов государственного, регионального или местного уровня, ключевых новостных порталов более 24 часов;
- ♦ недоступность или перерыв в работе КИИ более чем на шесть часов или отказ в работе их основных функций более чем на 24 часа;
- ♦ события, которые затрагивают работу и жизнь более 30 % населения в одном административном районе провинциального уровня или затрагивают вопросы обеспечения водой, электричеством, газом, маслом, отоплением или транспортом более 10 млн человек;
- ♦ утечки персональных данных более 100 млн человек или прямые экономические потери на сумму более 100 млн юаней (\$ 14 млн).

Проект документа показывает, что для Управления сетевой безопасностью Китая начинается новый этап развития, считают китайские должностные лица. Классификация инцидентов по уровням серьёзности является главной особенностью документа, поскольку позволяет распределить происшествия на основе их срочности и важности, устраняет путаницу, возникающую в критических ситуациях.

По мнению САС, если оператор задерживает отчётность, искажает или скрывает инцидент, приводящий к серьёзным последствиям, то ответственные лица должны быть наказаны в соответствии с законом. Реализация карательных мер имеет решающее значение для обеспечения эффективного исполнения законов и защиты национальной безопасности, считают китайские эксперты.

При обнаружении инцидента оператор должен сообщить название подразделения, где произошла кибератака, и основную информацию о задействованных объектах, системах и платформах, а также время, место, тип события, степень воздействия и причиненный вред. В отчете должны быть отражены принятые меры и их эффективность, тенденция развития ситуации, возможные дальнейшие последствия и вред, а также предварительный анализ причин инцидента.

НЕ УЛОЖИЛИСЬ В СРОКИ

По данным Управления подотчетности правительства США (GAO), 20 из 23 федеральных департаментов и агентств США не уложились в установленные законом сроки для внедрения возможностей реагирования на инциденты, связанные с киберугрозами. Новый отчет GAO показал, что по состоянию на август 2023 года только три из 23 федеральных подразделений соответствовали требуемым стандартам регистрации событий, предусмотренным Приказом Президента США (№ 14028 от 2021 года, «Требования к реагированию на инциденты кибербезопасности и статус завершения»). Согласно этому документу, Управление по управлению и бюджету США (OMB) требует, чтобы все федеральные агентства США достигли «третьего уровня» организации мониторинга киберинцидентов, на котором надлежащим образом ведутся и хранятся журналы мониторинга на всех уровнях критичности.

Несмотря на то что большинство агентств делают шаги по стандартизации планов реагирования и несколько улучшили свои возможности обнаружения, анализа и обработки инцидентов, только три из них достигли продвинутого — третьего — уровня. Из оставшихся двадцати три находятся на первом, базовом, уровне, а 17 — на неэффективном нулевом уровне, пишет портал Cyber Security Hub.

«До тех пор пока все агентства не внедрят требования к регистрации событий, способность федерального правительства в полной мере обнаруживать, расследовать и устранять киберугрозы будет ограничена», — говорится в отчете GAO. Среди агентств, которые не смогли достичь третьего уровня, — Госдеп США, Министерства торговли и юстиции.

Федеральные агентства США сообщают о многочисленных проблемах реагирования на инциденты в области кибербезопасности. Для решения проблем агентства используют различные инструменты и услуги, которые предоставляются Агентством по кибербезопасности и инфраструктурной безопасности

(CISA) и сторонними компаниями, привлекают к работе квалифицированный персонал и выделяют финансирование. При этом агентства сталкиваются с тремя ключевыми проблемами, которые препятствуют в полной мере подготовиться к реагированию на инциденты кибербезопасности:

- ♦ нехватка персонала;
- ♦ технические проблемы с регистрацией событий;
- ♦ ограничения в обмене информацией о киберугрозах.

Для решения этих вопросов федеральные органы власти принимают усилия, которые включают помощь CISA, семинары, рекомендации и усовершенствование платформы обмена информацией о киберугрозах. В долгосрочной перспективе запланированы реализация Национальной стратегии в области трудовых ресурсов и образования и внедрение новой платформы для анализа угроз, создаваемой с участием CISA. Первый этап внедрения платформы в федеральных департаментах и агентствах ожидается в 2024 финансовом году, говорится в отчете.

ЮРИДИЧЕСКИЙ СПОР ПРИВЁЛ К КИБЕРАТАКАМ

В марте 2023 года Агентство по охране окружающей среды США (EPA) выпустило уведомление, предупреждающее компании о росте кибератак на муниципальные системы водоснабжения. По данным EPA, эти атаки могут привести к отключению или загрязнению путей доставки питьевой воды. И хотя некоторые государственные управляющие компании приняли шаги для повышения кибербезопасности своих систем водоснабжения, многие организации не смогли внедрить современные базовые методы ИБ и подвергаются высокому риску киберугроз. В числе таких компаний есть и финансируемые государством, утверждает EPA.

В соответствии с федеральным «Законом о безопасной питьевой воде» штаты обязаны

По состоянию на август 2023 года только 3 из 23 федеральных департаментов и агентств США соответствовали требуемым стандартам регистрации событий, предусмотренным Приказом Президента США

проводить регулярное, каждые 3–5 лет, обследование местных систем водоснабжения, чтобы оценить состояние систем, источников и эксплуатацию, а также качество питьевой воды. Все выявленные в ходе обследования недостатки должны быть устранены в соответствии с требованиями. Согласно мартовскому уведомлению, в список оборудования для проверки включены электронные системы, например промышленные системы управления. Должна проводиться и проверка кибербезопасности любой используемой операционной технологии, которая может повлиять на водоснабжение и качество поставляемой потребителям воды. В меморандуме изложены различные подходы, с помощью которых штаты могут соблюдать требования ЕРА, включая самооценку водной системы, оценку третьей стороной, прямую государственную оценку и пр. В сопроводительном документе Агентство привело контрольный список вопросов по кибербезопасности, который могут использовать штаты для оценки ИБ.

Однако новые требования вызвали неприятие в ряде штатов и у Ассоциации водопроводных предприятий США и Национальной ассоциации сельского водоснабжения. Они обратились в суд с требованием о приостановке уведомления ЕРА в связи с превышением полномочий последней. В июле 2023 г. суд Восьмого округа удовлетворил ходатайство истцов о приостановке действия меморандума до вынесения ходатайства на рассмотрение. В октябре ЕРА отозвало уведомление, сославшись на судебный процесс.

Осенью 2023 года ФБР, Агентство кибербезопасности и безопасности инфраструктуры (CISA), АНБ, Национальное управление кибербезопасности Израиля и ЕРА выпустили предупреждение, что как минимум с 22 ноября 2023 г. хакеры иранского Корпуса стражей исламской революции активно эксплуатируют уязвимости, найденные в системах водоснабжения и водоотведения США. В числе скомпрометированных устройств — программируемые логические контроллеры Unitronics израильского производства. В рядах пострадавших — система водоснабжения г. Аликвиппа (шт. Пенсильвания), взломанная иранской группировкой CyberAv3ngers.

Агентства рекомендуют (после судебного решения они не могут требовать) выполнить три условия, чтобы водоснабжающие организации могли предотвратить или смягчить последствия кибератак: установить многофакторную аутентификацию, использовать уникальные пароли и проверить установленное оборудование на наличие паролей по

умолчанию. Эти пункты идентичны трём из четырёх, которые были в списке контрольных вопросов из уведомления ЕРА. Как показало расследование инцидента в Пенсильвании, хакеры используют те слабые стороны, которые вызвали негодование эксплуатирующих организаций и на которые ранее обратило внимание Агентство.

После кибератак Ассоциация водопроводных предприятий призвала федеральное правительство законодательно установить режим регулирования для систем водоснабжения и канализации, создать частную отраслевую компанию, которая будет разрабатывать требования кибербезопасности и обеспечивать их соблюдение при непосредственном участии ЕРА. Аналогичный подход давно действует в электроэнергетике, однако до сих пор не реализован в виде закона.

Как отмечают юристы, бюрократия и враждебность судов к федеральному регулированию замедляют усилия Администрации Байдена по принятию правил кибербезопасности для всех секторов экономики. Белый дом продолжает искать способы усилить безопасность критически важной инфраструктуры, пока конгресс США сопротивляется принятию новых регуляторных требований. Так, Департамент здравоохранения и социальных служб США (HHS) опубликовал план по реализации мер кибербезопасности для больниц, получающих выплаты Medicare и Medicaid.

ПОМОГИ СЕБЕ САМ

Невозможность получить неотложную медицинскую помощь из-за кибератаки — это не страшная сказка, а реальность, с которой всё чаще сталкиваются пациенты в Северной Америке. Сфера здравоохранения — на всех этапах оказания медицинской помощи, от больниц до врачебной практики, — является основной мишенью для кибератак из-за её зависимости от сложных ИТ-систем и хранения персональных данных.

Осенью 2023 года две крупные кибератаки нарушили работу медицинских компаний. 26 ноября компания Ardent Health Services подверглась атаке программы-вымогателя, которая нарушила работу 30 больниц и закрыла отделения неотложной помощи как минимум в трёх штатах. Ardent не смогла восстановить доступ к системе электронных медицинских карт и основным клиническим и бизнес-системам до 6 декабря.

В декабре диализная группа Fresenius Medical Care (ФРГ) сообщила о взломе американской дочерней компании Cardioglass

Consultants. Злоумышленник получил доступ к медицинским записям и личной информации 500 тыс. пациентов и их поручителей. Были скомпрометированы персональные данные 200 сотрудников.

Управление по гражданским правам США (OCR) зафиксировало увеличение количества утечек данных на 93 % в период 2018–2022 гг., а медицинские компании сообщили OCR о 536 утечках данных только в течение 2023 г. Согласно исследованию 2021 г., проведённому Proofpoint и Ponemon Institute, во время атак программ-вымогателей наблюдается рост смертности пациентов в госпиталях. Кибератаки вынуждают больницы отменять плановые процедуры и срывают проведение экстренных операций.

Учитывая тенденции, Департамент здравоохранения и социальных служб США (HHS) разработал и опубликовал для обсуждения план по реализации мер ИБ, который позволит использовать существующие полномочия ведомства для установления требований кибербезопасности для больниц, получающих выплаты Medicare и Medicaid. Этот план является частью усилий по реализации Федеральной стратегии кибербезопасности. В документе основное внимание уделяется четырём основным целям.

- ♦ Добровольность принятия мер в области кибербезопасности для сектора здравоохранения. Цели эффективной кибербезопасности (Cybersecurity Performance Goals, CPG) будут включать основополагающие методы ИБ и поощрение внедрения передовых методов.

- ♦ Предоставление ресурсов для стимулирования и внедрения методов кибербезопасности. HHS будет реализовывать программы инвестиций и стимулирования.

- ♦ Внедрение общенациональной стратегии HHS для поддержки строгого правоприменения и подотчётности. Цель HHS — включить CPG в существующие правила и программы, в том числе через Центры услуг Medicare и Medicaid (CMS). Кроме того, OCR дополнит правило безопасности Закона о переносимости и подотчётности медицинского страхования (HIPAA) дополнительными требованиями кибербезопасности.

- ♦ Создание и развитие единого центра кибербезопасности для установления тесной связи между организациями, предоставляющими медицинские услуги, и Управлением стратегической готовности и реагирования HHS (ASPR) — агентством, имеющим опыт обеспечения готовности к чрезвычайным ситуациям в сфере здравоохранения.

После публикации этого документа HHS заключило мировое соглашение с медицинской группой Lafourche Medical Group (LMG) из Луизианы в отношении фишинговой атаки 2021 г., которая привела к нарушениям HIPAA и утечке медицинских данных почти 35 тыс. человек. LMG согласилась выплатить OCR \$ 480 тыс. и принять меры по внедрению мер безопасности, соответствующих требованиям HIPAA, и провести обучение персонала основам ИБ.

В октябре 2023 г. HHS заключило соглашение со службой управления врачами (DMS) в связи с атакой программы-вымогателя, в результате которой в 2017 г. были скомпрометированы данные почти 207 тыс. человек. DMS согласилась выплатить OCR \$ 100 тыс., принять меры для устранения нарушений HIPAA и улучшить меры безопасности.

Эти соглашения показывают, что HHS расширяет свои правоприменительные полномочия и уделяет особое внимание усилиям по обеспечению отрасли здравоохранения надёжными и эффективными программами кибербезопасности.

Аналогичным образом Департамент финансовых услуг Нью-Йорка (DFS) внёс поправки в свои правила кибербезопасности. Они расширяют требования к безопасности финансовых учреждений и применяются к любой организации, действующей или обязанной действовать в соответствии с Законом о банковской деятельности, Законом о страховании или Законом о финансовых услугах. Таким образом, под действие этих правил попадают страховые компании, менеджеры по льготам в аптеках и аналогичные организации. Правила кибербезопасности в Нью-Йорке потребуют от больниц внедрения мер кибербезопасности для улучшения защиты систем и сетей, используемых для оказания помощи пациентам. Правила были рассмотрены Советом по общественному здравоохранению и планированию здравоохранения и прошли общественные обсуждения до 5 февраля 2024 г. Если правила будут доработаны и приняты, больницам предоставят один год до начала соблюдения требований.

Во Флориде компания CommunityHealth IT (CommHIT) выделила два федеральных гранта для учреждений здравоохранения и общественного здравоохранения в сельских, недостаточно обслуживаемых и отдалённых районах. Гранты предназначены для оказания помощи этим учреждениям в реализации мер кибербезопасности и обучения персонала.

ОДКБ. РЕСПУБЛИКА КАЗАХСТАН

**Александр
ВИНОГРАДОВ**
ФГУП «ЦНИИХМ»

Сергей МЕНЬШИКОВ
основатель Belarusian
InfoSecurity Community

Андрей СИТНОВ
независимый
эксперт

Валерий СОКОЛЕНКО
заместитель начальника
службы информационной
безопасности ICBC в г. Алматы

Продолжаем серию материалов по анализу законодательства в области информационной безопасности (далее – ИБ) стран. На этот раз рассматриваем законодательство Республики Казахстан.

ТАЙНЫ

Тайны, определённые законодательством Республики Казахстан:

Коммерческая тайна

В РК в отличие от большинства стран нет специального закона, регулирующего охрану коммерческой тайны. Более того, законодательство РК не даёт исчерпывающего определения термину «коммерческая тайна». Нормы, посвящённые коммерческой тайне, дифференцированы по различным нормативно-правовым актам, что доставляет некоторые неудобства при определении границ коммерческой тайны.

Согласно п. 1 ст. 126 и п. 1 ст. 1017 Гражданского кодекса (далее – ГК РК) к коммерческой тайне относится ценная информация, включающая в себя секреты производства (ноу-хау), технологию производства, управленческую модель, а также способы и методы для увеличения прибыли.

При этом предприятие не может включать любую информацию в перечень объектов коммерческой тайны. Необходимо соблюдать три главных критерия в выборе:

- ♦ сведения должны иметь для предприятия действительную или потенциальную коммерческую ценность;
- ♦ сведения должны быть неизвестными третьим лицам;
- ♦ в отношении сведений должен быть установлен режим коммерческой тайны.

К объектам коммерческой тайны можно отнести сведения о субъектах предпринимательства и сферах их деятельности, а также производственную, управленческую, научно-техническую и финансово-хозяйственную информацию о деятельности компании. Однако стоит отметить, что в казахстанском законодательстве нет определённого перечня объектов, которые нельзя относить к коммерческой тайне.

Банковская тайна

Понятие «Банковская тайна» определено в Законе Республики Казахстан от 31.08.1995 № 2444 «О банках и банковской деятельности в Республике Казахстан»:

«Банковская тайна включает в себя сведения о клиентах и корреспондентах банков, их операциях и взаимоотношениях с банками, связанных с получением банковских услуг, в том числе без ограничения: информации о наличии, владельцах и номерах банковских счетов и корреспондентов банков, остатках и движении денег на этих счетах и счетах самого банка, ограничениях на перечисленных счетах (решениях и (или) распоряжениях государственных органов о приостановлении расходных операций, арестах, залогах), операциях клиентов и корреспондентов и самого банка (за исключением общих условий проведения банковских операций), а также наличии, владельцах, характере и стоимости имущества клиентов, находящегося на хранении в сейфовых ящиках, шкафах и помещениях банка, информацию о получении клиентами кредитов, проведении операций по платежам и (или) переводам денег, в том числе выполненным без открытия банковского счёта».



ОБЩИЕ СВЕДЕНИЯ

Республика Казахстан (РК) — государство в центре Евразии, граничащее на севере и западе с Россией, на востоке с Китаем, на юге с государствами Центральной Азии (Киргизия, Узбекистан и Туркменистан). Столица — Астана. Государственный язык — казахский, но наравне с ним официально употребляется и русский.

После распада СССР между нашими странами сложились тесные дружеские отношения. Казахстан и Россия — участники ОДКБ, ЕАЭС, СНГ и ряда других союзов.

Органы, утверждающие законы и подзаконные акты в области ИБ в Казахстане: Президент Республики Казахстан, Правительство Республики Казахстан, Комитет национальной безопасности Республики Казахстан (далее — КНБ РК), Министерство цифрового развития, инноваций и аэрокосмической промышленности Казахстана (далее — МЦРИАП РК), Агентство Республики Казахстан по регулированию и развитию финансового рынка (далее — АРРФР РК), Национальный Банк Республики Казахстан (далее — НБ РК) и другие отраслевые ведомства.

Все документы, которые будут рассмотрены ниже, имеют общереспубликанское значение и применяются для организации и обеспечения информационной и кибербезопасности. НБ РК, АРРФР РК, МЦРИАП РК, КНБ РК и другие отраслевые ведомства дополняют и детализируют ИБ в части специфичных отраслевых процессов.

Персональные данные

Понятие «Персональные данные» определено в Законе Республики Казахстан от 21.05.2013 № 94-V «О персональных данных и их защите»:

«персональные данные — сведения, относящиеся к определённому или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе».

ВЫСОКОУРОВНЕВЫЕ ДОКУМЕНТЫ

Концептуальными документами, охватывающими вопросы информационной безопасности, являются:

Концепция кибербезопасности («Киберщит Казахстана») (утверждена постановлением Правительства Республики Казахстан от 30.06.2017 № 407).

Концепция определяет основные направления реализации государственной политики в сфере защиты электронных информационных ресурсов, информационных систем и сетей телекоммуникаций, обеспечения безопасного использования информационно-коммуникационных технологий. Она призвана обеспечить единство подходов к мониторингу обеспечения информационной безопасности государственных органов, физических и юридических лиц, а также выработку механизмов предупреждения и оперативного реагирования на инциденты информационной безопасности, в том числе в условиях чрезвычайных ситуаций социального, природного и техногенного характера, введения чрезвычайного или военного положения.

ЗАКОНЫ

Законы — нормативные правовые акты, которые регулируют важнейшие общественные отношения, устанавливают основополагающие принципы и нормы, предусмотренные Конституцией Республики Казахстан. Основными законами в области ИБ являются:

Закон РК от 6.01.2012 № 527-IV «О национальной безопасности»

Данный Закон регулирует правовые отношения в области национальной безопасности Республики Казахстан и определяет содержание и принципы обеспечения безопасности человека и гражданина, общества и государства, систему, цели и направления обеспечения национальной безопасности Республики Казахстан.

Закон РК от 24.11.2015 № 418-V «Об информатизации»

Данный Закон позволяет регулировать общественные отношения в сфере информатизации, возникающие на территории Республики Казахстан между государственными органами, физическими и юридическими лицами при создании, развитии и эксплуатации объектов информатизации, а также при государственной поддержке развития отрасли информационно-коммуникационных технологий.

Закон РК от 15.03.1999 № 349-1 «О государственных секретах»

Закон определяет правовые основы и единую систему защиты государственных секретов в интересах обеспечения национальной безопасности Республики Казахстан, регулирует общественные отношения, возникающие в связи с отнесением сведений к государственным секретам, их засекречиванием,

распоряжением, защитой и рассекречиванием.

Закон РК от 21.05.2013 № 94-V «О персональных данных и их защите»

Закон позволяет регулировать общественные отношения в сфере персональных данных, а также определяет цель, принципы и правовые основы деятельности, связанные со сбором, обработкой и защитой персональных данных.

Закон РК от 7.01.2003 № 370 «Об электронном документе и электронной цифровой подписи»

Закон направлен на регулирование отношений, возникающих при создании и использовании электронных документов, удостоверенных посредством электронных цифровых подписей, предусматривающих установление, изменение или прекращение правоотношений, а также прав и обязанностей участников правоотношений, возникающих в сфере обращения электронных документов, включая совершение гражданско-правовых сделок.

Закон РК от 5.07.2004 № 567 «О связи»

Закон устанавливает правовые основы деятельности в области связи на территории Республики Казахстан, определяет полномочия государственных органов по регулированию данной деятельности, права и обязанности физических и юридических лиц, оказывающих услуги связи или пользующихся ими.

Закон РК от 31.08.1995 № 2444 «О банках и банковской деятельности в Республике Казахстан»

Закон регламентирует банковскую деятельность.

ПРИКАЗЫ И ПОСТАНОВЛЕНИЯ

Постановления Правительства РК:

Постановление Правительства РК от 20.12.2016 № 832 «Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности»

Указанные требования разработаны в соответствии с подпунктом 3 статьи 6 Закона РК «Об информатизации» и определяют требования в области информационно-коммуникационных технологий и обеспечения ИБ.

Постановление Правительства РК от 9.08.2018 № 488 «Об утверждении Национального антикризисного плана реагирования на инциденты информационной безопасности»

Национальный антикризисный план реагирования на инциденты ИБ определяет

порядок действий субъектов системы (государственные органы, уполномоченные на решение вопросов ИБ или реагирования на инциденты ИБ, НКЦИБ, Оперативный штаб, владельцы объектов информатизации «электронного правительства», владельцы объектов КИИ, оперативные центры информационной безопасности (далее – ОЦИБ), службы реагирования на инциденты информационной безопасности) по снижению влияния инцидентов ИБ на состояние информационной безопасности с одновременным сведением к минимуму нарушений их работы.

Приказы и постановления государственных органов РК:

Приказ Министра оборонной и аэрокосмической промышленности РК от 28.03.2018 № 52/НК «Об утверждении Правил проведения мониторинга обеспечения информационной безопасности объектов информатизации «электронного правительства» и критически важных объектов информационно-коммуникационной инфраструктуры»

Данные правила разработаны в соответствии с подпунктом 7 статьи 7-1 Закона РК «Об информатизации» и определяют порядок проведения мониторинга обеспечения информационной безопасности объектов информатизации «электронного правительства» и критически важных объектов информационно-коммуникационной инфраструктуры.

Приказ и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 16.08.2019 № 199/НК «Об утверждении Правил проведения мониторинга событий информационной безопасности объектов информатизации государственных органов»

Правила разработаны в соответствии с подпунктом 5-1 статьи 7-1 Закона РК «Об информатизации» и определяют порядок проведения мониторинга событий информационной безопасности объектов информатизации государственных органов.

Приказ Министра оборонной и аэрокосмической промышленности РК от 19.03.2018 № 48/НК. «Об утверждении Правил обмена информацией, необходимой для обеспечения информационной безопасности, между оперативными центрами обеспечения информационной безопасности и Национальным координационным центром информационной безопасности»

Правила разработаны в соответствии с подпунктом 19 статьи 7-1 Закона РК от 24.11.2015

«Об информатизации» и определяют порядок взаимодействия Национального координационного центра информационной безопасности с оперативными центрами обеспечения информационной безопасности при обмене информацией, необходимой для обеспечения информационной безопасности и реагирования на инциденты информационной безопасности.

Приказ Комитета национальной безопасности РК от 27.03.2018 № 25/нс «Об утверждении Правил функционирования системы централизованного управления сетями телекоммуникаций Республики Казахстан»

Правила разработаны в соответствии с пунктом 2 статьи 21 Закона РК «О связи» и определяют порядок функционирования системы централизованного управления сетями телекоммуникаций РК.

Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 13.10.2020 № 386/НК «Об утверждении Правил функционирования единого шлюза доступа к Интернету и единого шлюза «электронной почты электронного правительства»

Правила разработаны в соответствии со статьёй 7-1 Закона РК «Об информатизации» и определяют порядок функционирования единого шлюза доступа к интернету.

Приказ Комитета национальной безопасности РК от 27.03.2018. № 24/нс «Об утверждении Правил присоединения сетей операторов междугородной и международной связи к точкам обмена интернет-трафиком и пропуска интернет-трафиком»

Правила разработаны в соответствии с подпунктом 21-6 статьи 13 Закона РК от 21.12.1995 «Об органах национальной безопасности Республики Казахстан» и определяют порядок присоединения сетей операторов связи к точкам обмена интернет-трафиком и пропуска интернет-трафика.

Приказ Министра оборонной и аэрокосмической промышленности РК от 16.03.2018 № 44/НК «Об утверждении Правил создания и обеспечения функционирования единой национальной резервной платформы хранения электронных информационных ресурсов»

Правила разработаны в соответствии с подпунктом 17 статьи 7-1 Закона РК от 24.11.2015 «Об информатизации» и определяют порядок функционирования единой национальной резервной платформы хранения электронных

информационных ресурсов, периодичность резервного копирования электронных информационных ресурсов критически важных объектов информационно-коммуникационной инфраструктуры.

Приказ Министра обороны и аэрокосмической промышленности РК от 16.03.2018 № 45/НҚ «Об утверждении Правил передачи резервных копий электронных информационных ресурсов на единую платформу резервного хранения электронных информационных ресурсов»

Правила разработаны на основании подпункта 4 пункта 2-1 статьи 17 Закона РК «Об информатизации» и определяют порядок и сроки передачи резервных копий электронных информационных ресурсов на единую национальную резервную платформу хранения электронных информационных ресурсов.

Приказ Министра цифрового развития, обороны и аэрокосмической промышленности РК от 03.06.2019 № 111/НҚ «Об утверждении методики и правил проведения испытаний объектов информатизации «электронного правительства» и информационных систем, отнесённых к критически важным объектам информационно-коммуникационной инфраструктуры, на соответствие требованиям информационной безопасности»

Методика разработана в соответствии с подпунктом 5 статьи 7-1 Закона РК «Об информатизации».

Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 29.06.2019 № 144/НҚ «Об утверждении Правил проведения экспертизы в сфере информатизации инвестиционных предложений, финансово-экономических обоснований бюджетных инвестиций»

Правила разработаны в соответствии с подпунктом 19 статьи 7 Закона РК «Об информатизации» и устанавливают порядок проведения экспертизы в сфере информатизации (далее — экспертиза) инвестиционных предложений, финансово-экономических обоснований бюджетных инвестиций.

Постановление Правления Национального Банка Республики Казахстан от 27.03.2018 № 48 «Требования к обеспечению информационной безопасности банков, филиалов банков-нерезидентов Республики Казахстан и организаций,

осуществляющих отдельные виды банковских операций»

Требования разработаны в соответствии с пунктом 7 статьи 61-5 Закона РК «О банках и банковской деятельности в Республике Казахстан» и устанавливают требования к обеспечению информационной безопасности банков, филиалов банков-нерезидентов РК и организаций, осуществляющих отдельные виды банковских операций.

Постановление Правления Национального Банка РК от 28.01.2016 № 34 «Об утверждении Требований к безопасности и непрерывности работы информационных систем банков, филиалов банков-нерезидентов РК и организаций, осуществляющих отдельные виды банковских операций»

Требования разработаны в соответствии с подпунктом 85 части второй статьи 15 Закона РК «О Национальном Банке Республики Казахстан» и определяют требования к безопасности и непрерывности работы информационных систем банков, филиалов банков-нерезидентов РК и организаций, осуществляющих отдельные виды банковских операций, посредством которых обеспечивается оказание электронных банковских услуг.

Постановление Правления Агентства РК по регулированию и развитию финансового рынка от 12.09.2022 № 67 «Об утверждении Правил подключения и использования финансовыми организациями объекта информатизации по сбору, обработке и обмену информацией по событиям и инцидентам информационной безопасности, используемого отраслевым центром информационной безопасности финансового рынка и финансовых организаций»

Правила разработаны в соответствии с пунктом 4 статьи 7-5 Закона РК «Об информатизации» и определяют порядок подключения и использования финансовыми организациями объекта информатизации по сбору, обработке и обмену информацией по событиям и инцидентам информационной безопасности, используемого отраслевым центром информационной безопасности финансового рынка и финансовых организаций.

Постановление Правления Национального Банка РК от 30.07.2018 № 164 «Об утверждении Требований к организации безопасной работы, обеспечивающей сохранность и защиту информации от несанкционированного доступа к данным, хранящимся в страховой

(перестраховочной) организации, а также кибербезопасности страховой (перестраховочной) организации»

Требования разработаны в соответствии с Законом РК от 18.12.2000 «О страховой деятельности» и устанавливают требования к организации безопасной работы, обеспечивающей сохранность и защиту информации от несанкционированного доступа к данным, хранящимся в страховой (перестраховочной) организации, а также кибербезопасности страховой (перестраховочной) организации.

Постановление Правления Национального Банка РК от 27.09.2018 № 228 «Об утверждении Требований к использованию информационно-коммуникационных технологий и обеспечению информационной безопасности при организации деятельности кредитных бюро, поставщиков информации и получателей кредитных отчётов, являющихся банками, организациями, осуществляющими отдельные виды банковских операций, микрофинансовыми организациями и коллекторскими агентствами, а также Требований, предъявляемых кредитными бюро к поставщикам информации и получателям кредитных отчётов в соответствии с подпунктом 11) пункта 2 и подпунктом 9) пункта 3 статьи 27 Закона РК от 6 июля 2004 года «О кредитных бюро и формировании кредитных историй в РК»

Требования разработаны в соответствии с Законом РК от 6.07.2004 «О кредитных бюро и формировании кредитных историй в РК» и устанавливают требования к использованию информационно-коммуникационных технологий и обеспечению информационной безопасности при организации деятельности кредитных бюро, поставщиков информации и получателей кредитных отчётов, являющихся банками, организациями, осуществляющими отдельные виды банковских операций, микрофинансовыми организациями и коллекторскими агентствами.

Постановление Правления Национального Банка РК от 28.04.2012 № 165 «Об утверждении Требований к программно-техническим средствам и иному оборудованию, необходимым для осуществления деятельности на рынке ценных бумаг»

Требования определяют минимально необходимый функционал программно-технических средств и иного оборудования, а также набор требований к обеспечению

информационной безопасности при обработке информации, содержащей коммерческую тайну, на программно-технических средствах и ином оборудовании организаций, осуществляющих деятельность на рынке ценных бумаг.

Постановление Правления Агентства РК по регулированию и развитию финансового рынка от 21.09.2020 № 89 «Об утверждении требований к компетенциям руководителей и работников подразделений информационной безопасности, включая требования по повышению квалификации лиц, ответственных за обеспечение информационной безопасности»

Требования разработаны в соответствии с Законом РК от 4 июля 2003 года «О государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций» и устанавливают требования к компетенциям руководителей и работников подразделений информационной безопасности, включая требования по повышению квалификации лиц, ответственных за обеспечение информационной безопасности финансовых организаций РК и филиалов банков – нерезидентов РК, филиалов страховых (перестраховочных) организаций – нерезидентов РК, филиалов страховых брокеров – нерезидентов РК независимо от форм собственности.

Постановление Правления Агентства РК по регулированию и развитию финансового рынка от 21.09.2020 № 90 «Об утверждении Требований к службам реагирования на инциденты информационной безопасности, проведению внутренних расследований инцидентов информационной безопасности»

Требования разработаны в соответствии с Законом РК от 04.07.2003 «О государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций» и устанавливают требования к службам реагирования на инциденты информационной безопасности, проведению внутренних расследований инцидентов информационной безопасности банков второго уровня и филиалов банков-нерезидентов РК, организаций, осуществляющих отдельные виды банковских операций.

Постановление Правления Агентства РК по регулированию и развитию финансового рынка от 23.11.2020 № 110 «Об утверждении Правил оценки уровня защищённости от угроз информационной безопасности»

Правила разработаны в соответствии с Законом РК от 04.07.2003 «О государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций» и определяют порядок оценки уровня защищённости от угроз информационной безопасности финансовых организаций и филиалов банков – нерезидентов РК, филиалов страховых (перестраховочных) организаций – нерезидентов РК, филиалов страховых брокеров – нерезидентов РК.

Постановление Правления Агентства РК по регулированию и развитию финансового рынка от 23.11.2020 № 111 «Об утверждении методики оценки рисков информационной безопасности, включая порядок ранжирования финансовых организаций по степени подверженности рискам информационной безопасности»

Методика разработана в соответствии с Законом РК от 04.07.2003 «О государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций» и применяется в целях организации процесса оценки рисков информационной безопасности в финансовых организациях и филиалах банков – нерезидентов РК, филиалах страховых (перестраховочных) организаций – нерезидентов РК, филиалах страховых брокеров – нерезидентов РК, к которым предъявляются требования по проведению оценки рисков информационной безопасности, для определения приоритетов и оптимизации ресурсов, задействованных при обработке рисков информационной безопасности в финансовых организациях.

Постановление Правления Агентства РК по регулированию и развитию финансового рынка от 12.09.2022 № 67 «Об утверждении Правил подключения и использования финансовыми организациями объекта информатизации по сбору, обработке и обмену информацией по событиям и инцидентам информационной безопасности, используемого отраслевым центром информационной безопасности финансового рынка и финансовых организаций»

Правила разработаны в соответствии с пунктом 4 статьи 7–5 Закона РК «Об информатизации» и определяют порядок подключения и использования финансовыми организациями объекта информатизации по сбору, обработке и обмену информацией по событиям и инцидентам информационной безопасности, используемого отраслевым

центром информационной безопасности финансового рынка и финансовых организаций.

СТАНДАРТЫ

Национальные стандарты РК:

♦ СТ РК ISO/IEC 27001–2023 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования».

♦ СТ РК ISO/IEC 27002–2015 «Информационная технология. Методы и средства обеспечения безопасности. Свод правил по средствам управления информационной безопасностью».

♦ СТ РК ИСО/МЭК 13335–5–2008 «Информационная технология. Методы и средства обеспечения безопасности. Управление защитой информационных и коммуникационных технологий. Часть 5. Руководство по управлению защитой сети».

♦ СТ РК ISO/IEC 15408–1–2017 «Информационные технологии. Методы и средства обеспечения безопасности Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель».

♦ СТ РК ISO/IEC 15408–2–2017 «Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности».

♦ СТ РК ISO/IEC 15408–3–2017 «Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования к обеспечению защиты».

♦ СТ РК 1073–2007 «Средства криптографической защиты информации. Общие технические требования».

♦ СТ РК ИСО/МЭК 18028–4–2007 «Технологии информационные. Методы обеспечения защиты. Защита сети информационных технологий. Часть 4. Защита удалённого доступа».

♦ СТ РК ИСО/МЭК 27005–2022 «Информационные технологии. Методы обеспечения безопасности. Менеджмент риска информационной безопасности».

♦ СТ РК IEC 31010–2020 «Менеджмент риска. Методы оценки риска».

Надеемся, что данный материал поможет «не заблудиться» в Законодательстве Республики Казахстан. Мы постарались облегчить путь изучения и применения на практике нормативных законов и подзаконных актов в области ИБ.

ВЕРНЁМ И ВЫРАСТИМ РЕБЁНКА ЭНГЕЛЬБАРТА!

ОБ УПРАВЛЕНИИ ЗНАНИЯМИ И ТЕОРИИ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



Рустам ГУСЕЙНОВ
эксперт BIS Journal

Иногда полезно напоминать себе, что защита информации – это не только технологии и процессы, но и люди. А люди – ничто без созданных предшествующими поколениями культуры и знаний. Помнить об этом полезно не только с общегуманитарной точки зрения, но и в контексте развития отдельной организации. Когда мы сталкиваемся с уходом целых подразделений и утратой квалификации из-за корпоративных конфликтов или терпим потерю накопленных за годы работы данных из-за отсутствия резервных копий, мы буквально теряем «зрение» и «слух». Но проблема глубже – в меняющемся мире, полном новых угроз, процессов и технологий и, соответственно, в задаче непрерывной адаптации к новому, изменённому контексту. Возникает необходимость принятия быстрых решений, отделения значимого от второстепенного, встаёт задача управления приоритетами в условиях ограниченных ресурсов. И здесь на фронтире – системы управления знаниями; применение экспертных систем и искусственного интеллекта; анализ данных и прочее. Автор статьи рефлексировал генезис проблемы и рассказывает о возможных путях превращения

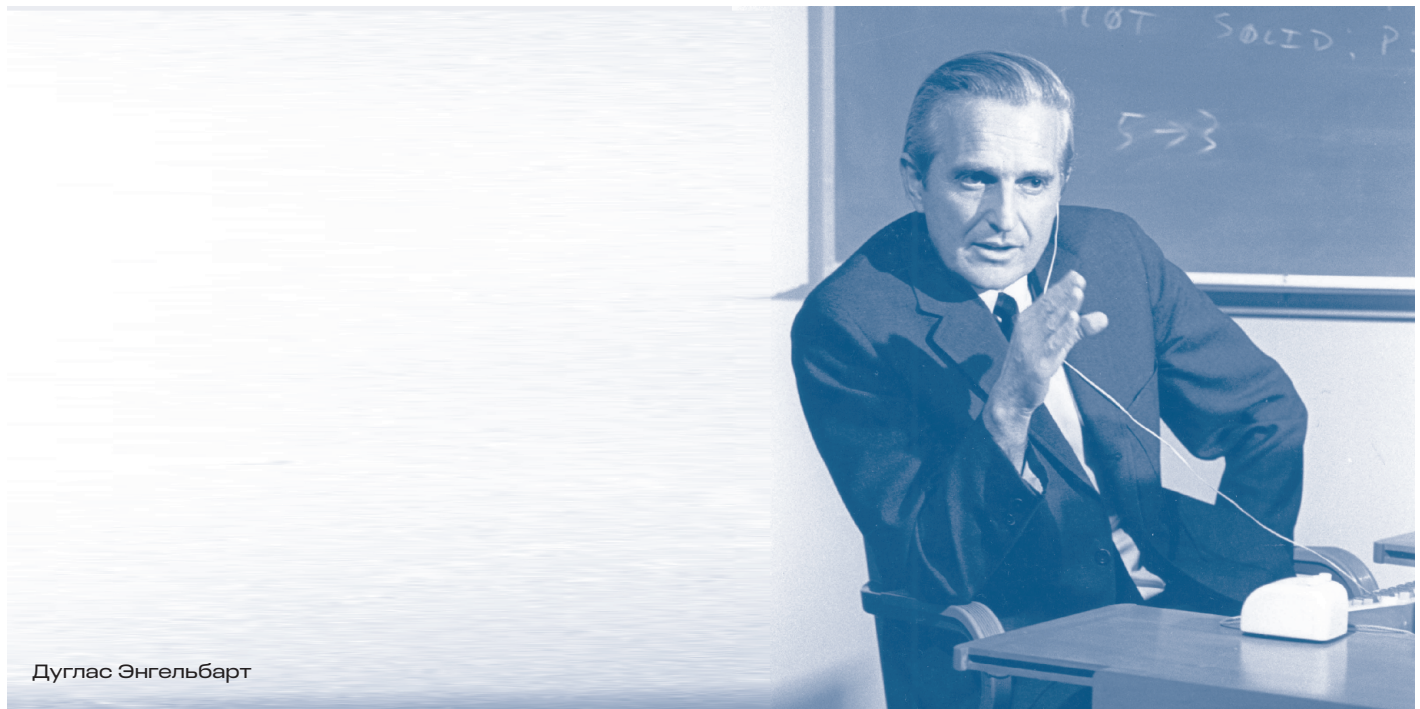
этой проблемы в понятную и масштабируемую задачу в контексте информационной безопасности и управления предприятием.

ВВЕДЕНИЕ

В не совсем далёкие времена, когда энтузиазм от победы союзников во Второй мировой не угас, а послевоенное поколение верило в возможность строительства лучшего мира, один молодой человек из США задумался над тем, как принести этому миру наибольшую пользу? Тогда он столкнулся с океаном возможностей и безграничными объёмами неструктурированной информации, разбросанной по множеству книг и журналов, хранящихся в архивах, научных институтах и библиотеках. Конечно, он мог пойти путём Дарвина или Маркса и на десятилетия уйти в мануальную проработку разрозненных материалов, чтобы через 20 лет упорной книжной работы создать собственный magnum opus и разобраться наконец в устройстве мира, понять, что же нужно делать этому миру дальше, но... нашему герою хотелось найти другие, более быстрые и современные пути. Пути, к которым обязывало ускоряющееся время.

Этого человека звали Дуглас Энгельбарт¹, и ему вместе с соратниками предстояло разработать всё то, без чего немыслима наша компьютеризированная жизнь. Вывод изображения на экраны мониторов, графические интерфейсы, компьютерная мышь, совместная работа с документами – всё, что многие ошибочно приписывают гению Стива Джобса, на деле является результатом новаторских работ коллектива исследователей, руководимых Энгельбартом под эгидой Стэнфордского исследовательского института. И всё это было

¹ Подробнее про Д. Энгельбарта: https://en.wikipedia.org/wiki/Douglas_Engelbart; https://youtu.be/uR_4KEFrYCCQ; T. Bordini. Bootstrapping: Douglas Engelbart, Coevolution, and the Origins of Personal Computing.



Дуглас Энгельбарт

спроектировано и реализовано в далёких 60-х лишь для того, чтобы помочь людям решить исходную задачу Энгельбарта — получить эффективные инструменты для управления информацией, качественные решения о том, на что и как следует потратить время.

Удалось ли нам достичь поставленной цели? Какое отношение управление знаниями имеет к вопросам информационной безопасности? И почему человечеству только предстоит научиться создавать цифровые двойники и моделировать защищаемые организации?

ПРОБЛЕМАТИКА УПРАВЛЕНИЯ ЗНАНИЯМИ

Технооптимисты любят утверждать, что все проблемы могут быть решены внедрением какого-то решения. Но, во-первых, решение всё равно нужно внедрять и настраивать, а во-вторых, даже у автоматизированных решений есть операторы и аналитики, которые должны с ними работать. Отсюда возникает два интересных момента.

Момент первый — даже обладая самыми совершенными инструментами, но не обладая при этом компетенциями по их рациональному и продуктивному использованию, человек может не добиться никаких положительных результатов и даже хуже — подорвать продуктивность собственной работы. Классический пример описывает Тео Компернолле в книге «Мозг освобождённый», где приводится статистика продуктивности специалистов в области интеллектуального труда, которые не отключают уведомления на сотовых телефонах и электронной почте, в результате чего каждые 5–10 минут отвлекаются на очередные «входящие».

Казалось бы, в чём проблема? Отлично, что люди включены в задачи 24 на 7 на 365, давайте ещё и ещё повысим продуктивность! Но проблема, оказывается, в том, что для освоения нового и продуктивной работы над сложными задачами мозг человека должен сконцентрироваться на контексте. А эта концентрация занимает от 10 до 20 минут и требует удержания в оперативной памяти актуальных для данной задачи элементов и перехода в режим сложного ассоциативного мышления над параллельными элементами единого целого. Гиперподключённость же оказывается несовместима с подобной «глубокой работой» над информацией и творческим подходом — в результате человек занимается потоковой обработкой входящих и принятием поверхностных, шаблонных решений. Обучение и понимание сути изучаемого материала страдает. Глубина и потенциал создаваемых знаний не соответствует возможному уровню — творческих прорывов не происходит.

Момент второй — система должна уметь адаптироваться к изменяющемуся контексту, а значит, требует сопровождения. И не только интеграции внутри предприятия с новыми или старыми объектами. Но и адаптации к лучшим практикам, к фронтиру соответствующей науки или технологий, к актуальным нормативным требованиям, к возникающим в обществе и отрасли вызовам. Это значит, что практически все новые решения в каком-то смысле обречены на вечное улучшение, и когда мы забываем об этом, например, продолжаем использовать IBM Lotus Notes в 2023 году или игнорируем основной ресурс SIEM — обучение персонала и выделенные кадры на администрирование подключения и настройки источников, то допускаем фатальную ошибку.

Но и это не главное, а главное заключается в том, что современные подходы к описаниям знаний страдают от той проблемы, которую хотел решить Энгельбарт. Ведь подойдя к вопросу повышения продуктивности работы с информацией, он не только придумал графические и механические интерфейсы, но и задумался над тем, каким должен быть сам процесс работы и как должны быть устроены приложения и пользовательский опыт, чтобы люди не тонули в потоке неструктурированных данных, не запутывались в плохо сортированных гиперссылках, а действительно занимались познанием мира и формированием конструктивных решений о том, как с этим миром взаимодействовать. В этом смысле компьютер Энгельбарта был прямой противоположностью того, во что вылилась цифровизация. Не машина захвата внимания и удовлетворения потребностей человека в «легкодоступных данных», не мыслительный фастфуд, а система добровольно-принудительного усиления интеллекта, направленная на помощь пользователю при переходе в режим «глубокой творческой проработки» любого вопроса.

Современное же ИТ, восприняв часть находок Стэнфордского исследовательского института, забыло о самой важной их части. Выплеснуло с водой ребёнка. Реализовав первый этап планов Энгельбарта, оно остановилось и вот уже 50 с лишним лет стоит на месте. В результате мы получили проблему, которой боялись ещё авторы Энциклопедии²: огромный объём удобно индексируемых знаний из-за особенностей человеческого восприятия плохо усваивается в голове читателя и потому не формирует единой картины мира. Как результат, в головах формируются разрозненные островки знаний без целостной картины и понимания происходящего. Качество принимаемых решений и глубина проработки вопросов страдает. И люди в целом перестают стремиться к системному познанию мира. Сегодня они скорее жонглируют отдельными вопросами и задачами, как фокусники, постоянно переключая своё внимание.

ВОЗМОЖНОЕ РЕШЕНИЕ ПРОБЛЕМЫ

Но всё ли так страшно? И неужели из сложившейся ситуации нет выхода? Конечно же, выход есть. И здесь стоит вспомнить другую книгу — «Всеми своё место». Её авторка Джудит Фландерс рассказывает о том, как люди придумывали письменность с пробелами между словами и алфавитным порядком и как потребовались буквально сотни лет, чтобы реализовать то, что воспринимается нынешними поколениями как само собой разумеющееся. С учётом того, что «фундаментальное

открытие» важности располагать слова или разделы по алфавиту потребовало более 500 лет, не удивительно, что такая новая отрасль, как ИТ, и ещё более молодая ИБ всё ещё страдают от некоторого хаоса и плохой структурированности информации. А в практике многих специалистов, управленцев и организаций преобладает подход к тушению пожара вместо систематического, методичного и аккуратного решения приходящих задач, по аналогии с методологией GTD Дэвида Аллена³.

Уже сейчас мы ощущаем нехватку строгой теории информационной безопасности, которая бы интегрировала в себе различные, пока изолированные, домены ИБ (от безопасной разработки до требований к защите персональных данных), — по аналогии с синтезом, какой в своё время осуществила физика или совсем недавно история — в рамках развития клиодинамических моделей⁴. С другой стороны, накоплен огромный массив стандартов, сделаны первые попытки создания формальных универсальных языков, позволяющих исследовать защищённость систем и определять степень доверия к ним (например, Common Criteria / ГОСТ Р ИСО/МЭК 15408), активно внедряются и пилотируются GRC-системы, ведутся работы над созданием экспертных систем, основанных на технологиях нейронных сетей и т.д. и т.п. Гипотетически стык этих направлений может породить синтез разрозненных знаний, необходимый для выработки «единой теории информационной безопасности» и создания инструментов, стимулирующих продуктивную работу с получаемыми данными, как завещал нам Дуглас Энгельбарт.

И здесь полезно вспомнить опыт создания новых отраслей, например, в области ракетостроения и космических исследований в СССР, ведь сами по себе знания и технологии не существуют. А значит, придётся заранее готовить людей, способных освоить результаты такого синтеза и умеющих работать в соответствующем инструментарии. Это потребует изменения подходов в образовании — возврата к деятельностному и практико-ориентированному подходу, формирования базы молодых специалистов, для которых будет естественным фундаментальное восприятие процессов и организаций и которые будут заточены на моделирование онтологий и цифровых двойников защищаемых объектов. В основе таких подходов будет лежать проработанная теория информационной безопасности и стандартизированный стек инструментов, необходимый для выполнения соответствующих работ.

³ См. статью автора «Практики внедрения GRC, инфраструктуры как кода и систем мониторинга: четыре простых шага, с которых стоит начать» в № 3 (2023) журнала «Внутренний контроль в кредитной организации» <https://futurebanking.ru/profile/23545>

⁴ См. например, Сергей Нефедов: Факторный анализ исторического процесса. Исторический опыт традиционных обществ Востока: <https://www.labyrinth.ru/books/671979>

² Французская энциклопедия эпохи Просвещения, одно из крупнейших справочных изданий XVIII века (т. 1–35, 1751–1780), которое, как считается, подготовило почву для Великой французской революции (из материалов Википедии).

СЛОВО О КВАНТЕ

КОМПАНИЯ «ИНФОТЕКС» И МЕДИА ГРУППА «АВАНГАРД»
ПРЕДСТАВИЛИ КНИГУ О КВАНТОВЫХ ТЕХНОЛОГИЯХ

В Московской государственной картинной галерее народного художника СССР Александра Шилова прошла презентация книги «Прикладные квантовые технологии для защиты информации». Издание подготовлено компанией «ИнфоТекс». Издатель – ООО «Медиа Группа «Авангард».

Открывший мероприятие генеральный директор компании «ИнфоТекс» А. А. Чапчаев отметил, что идея написать собственную книгу на тему квантовых технологий возникла два года назад: «Мы постарались сделать ее понятной как для криптографов, которые только начинают изучать эту тему, так и для специалистов в области квантовой физики, которые начинают изучать особенности ее применения в криптографии. Мы благодарим за помощь в подготовке издания руководителя Центра квантовых технологий физического факультета МГУ имени М. В. Ломоносова профессора Сергея Кулика и старшего научного сотрудника Лаборатории волоконно-оптических систем квантовой криптографии Андрея Климова, советника ОАО «МТС» д.т.н. Павла Сундеева, Игоря Арбекова и весь коллектив «СФБ Лаб», участие которых обогатило материалы издания и сделало его полным и интересным». Главный редактор В. Л. Елисеев рассказал, что идея написать эту книгу зародилась весной 2022 года. Возникла необходимость создания печатного труда, в котором содержался бы некий образовательный акцент на квантовые технологии. В. Л. Елисеев поблагодарил всех рецензентов книги, которые прочли и дали отзывы на издание в процессе его подготовки к печати.

С приветственным словом к авторам обратился А. Ю. Битоков, член Совета по развитию цифровой экономики при Совете Федерации. Он зачитал обращение В. В. Бондарева, первого заместителя председателя Комитета Совета Федерации Федерального собрания РФ по обороне и безопасности, который отметил актуальность и своевременность издания. Сенатор пожелал коллективу авторов «не снижать темпы научной и инженерной работы по созданию, внедрению и развитию новейших средств защиты информации, удерживать достигнутые результаты, достойно противостоять противнику в киберпространстве».

В своём выступлении Д. Г. Грибков, помощник секретаря Совета безопасности РФ, отметил необходимость развития и государственного

регулирования новых технологий, в том числе квантовых коммуникаций и постквантовой криптографии. Это серьёзная тема, данное издание будет «хорошим подспорьем» для понимания вопроса. «Квантовая физика не просто существует, надо использовать её возможности, одновременно понимая угрозы и опасности, которые она несёт», – подчеркнул Д. Г. Грибков. Он выразил благодарность авторам и научным кругам за теоретические и практические работы на благо национальной безопасности страны.

Заместитель министра цифрового развития, связи и массовых коммуникаций РФ А. М. Шойтов отметил, что технологии квантовых коммуникаций – перспективное направление исследований, продолжение работ над которым планируется включить в национальный проект «Экономика данных». Квантовые коммуникации – уникальное сочетание перспективных технологий и информационной безопасности, и необходимо найти им применение не только в вопросах ИБ и телекоммуникаций, но и в экономике России в целом, подчеркнул замглавы Минцифры. «Эта книга даёт содержательное представление о сути самой технологии и её внедрении, что будет способствовать повышению ИБ нашей страны в целом», – отметил А. М. Шойтов.

В. Н. Сачков, вице-президент и действительный член Академии криптографии РФ, подчеркнул необходимость правильного академического подхода к изучению и развитию квантовых технологий. Он отметил, что ещё 10–15 лет назад понятия «квант» и «высокопроизводительные квантовые вычислительные машины» несли угрозы для специалистов-криптографов. Однако дальнейшее изучение квантовых технологий показало возможность создания квантовоустойчивых механизмов. «Трудно сказать, какие вопросы ещё надо будет решить, чтобы устройства шифрования заняли своё место. Сейчас это место очевидно в определённых пограничных областях. На наших глазах зарождается новое направление науки, раздел криптографии, касающийся оценки его стоимости. Такое происходит не так часто», – подчеркнул В. Н. Сачков. «Все основания быть оптимистами у нас есть», – отметил учёный.

Завершил презентацию С. П. Кулик, научный руководитель Центра квантовых технологий МГУ им. М. В. Ломоносова, стоявший у истоков направления квантовых технологий компании



«ИнфоТеКС». Он поздравил коллектив авторов и компанию «ИнфоТеКС» с изданием книги, которая представляет «лёгкий образец» того, как можно знакомить широкую публику с новыми технологиями. Книгу можно читать с любого места, подчеркнул С. П. Кулик, она перемежается воспоминаниями людей, которые принимали

непосредственное участие в создании новых устройств.

Как отметил Д. М. Гусев, заместитель генерального директора компании «ИнфоТеКС», в будущем книга «Прикладные квантовые технологии для защиты информации» будет дополняться и переиздаваться в новой редакции.

300 ЛЕТ НАЗАД

В РОССИИ ПОЯВИЛИСЬ ПЕРВЫЕ АКАДЕМИКИ



Борис СТОЛПАКОВ
историк криптографии

8 февраля 1724 года был оглашён указ Сената об учреждении Петербургской академии наук и художеств «с назначением на содержание оной доходов» по распоряжению императора Петра I.

ВЫБОР СДЕЛАН

В первой четверти XVIII столетия научные академии были ещё новым делом для Европы. Причиной их создания стали запросы практики, прежде всего, мореплавания и военного дела, вызванные Великими географическими открытиями, а также успехами в изучении движения небесных тел и всевозможных

приложений нового знания. Тогда потребовалась концентрация усилий по исследованию и освоению новых колониальных владений. Во второй половине XVII века Англия и Франция дали два способа систематизации и поддержки научных изысканий. Англия создала клуб любителей с регулярными взносами (в лице Лондонского королевского общества), а Франция — объединение исследователей, получающих стипендии от государства (в лице Парижской академии наук). Россия пошла по второму пути. На решение Петра I о создании Академии значительно повлияла его продолжительная поездка в Европу в 1716–1717 годах. Тогда царь покинул Россию на 21 месяц! В Париже его избрали в академики. Франция и стала ориентиром в академических делах.

Понятно, что в России предстояло решать задачи, уже поставленные реальной жизнью перед европейскими метрополиями. Требовалось изучить и описать экономические возможности российских территорий, составить их подробные карты, а также собрать материал о флоре и фауне, культуре и истории разных народов России. При этом желательно было использовать европейский опыт подобных исследований.

ВСЁ НАЧАЛОСЬ С КУНСТКАМЕРЫ

Решение о создании Академии вызревало постепенно. Сначала, в 1714 г., появилась Кунсткамера. Это немецкое слово, как известно, означает «кабинет искусств», т.е. собрание редкостей. Ещё во время своего первого продолжительного визита в Европу с «великим посольством» в 1697–1698 годах Пётр I обратил внимание на модное увлечение собиранием коллекций разных редкостей и организацией для их хранения и демонстрации особых кабинетов. Тогда же русский царь начал скупать целые коллекции и отдельные вещи: оружие, природные редкости, книги и прочее. Так в Москве появился «Государев Кабинет», позже перевезённый в новую столицу — Петербург и постоянно пополняемый. А в 1714 году коллекции разместили в палатах Летнего сада, их стали именовать Кунсткамерой. Это был первый в России естественно-научный музей. Коллекции увеличивались, и для их размещения в 1718 году началось строительство того здания, где они и ныне находятся. Позже в том же доме поместили и Петербургскую академию наук (илл. 1).

Задолго до основания Академии Российское государство приглашало западноевропейских специалистов для работы в качестве врачей, ботаников — для поиска лекарственных растений, фармацевтов — для изготовления лекарств, естествоиспытателей — для поиска минеральных вод и других полезных ископаемых. Этим занимался Аптекарский приказ в Москве, который в 1707 г. открыл своё отделение в новой столице — Аптекарскую канцелярию. Именно Аптекарская канцелярия ведала организацией экспедиций по территории России — на Северный Кавказ, в Карелию, на Урал, в Сибирь.

«ГДЕ СОШЛАСЯ АМЕРИКА С АЗИЕЮ...»

При Петре I приглашением иностранных учёных занимался его лейб-медик Р. Арескин, шотландец, член Лондонского королевского общества. Его задача облегчалась тем, что количество научных вакансий в Европе было невелико. Надо сказать, что тогда была эпоха универсальных учёных — энциклопедистов, т.е. учёных в изначальном смысле этого слова, а не узкообразованных специалистов — работников науки нашего времени.

Одного из учёных медиков, Д. Мессершмидта, царь отправил в 1718 г. в Сибирь «для изыскания всяких раритетов и аптекарских вещей». В следующем, 1719 г. геодезисты И. Евреинов и Ф. Лужин были посланы на Камчатку с заданием описать «тамошние места, где сошлася Америка с Азией...» Тогда происходило начальное освоение недавно присоединённых территорий Сибири и Дальнего Востока, и они были мало известны науке.

СИБИРСКИЙ ПУТЬ МЕССЕРШМИДТА

Начав с Тобольска, Мессершмидт в течение восьми лет исследовал огромные территории Сибири практически в одиночку, в сопровождении драгун и пленных шведов. Он побывал в Южной и Западной Сибири, в Забайкалье, доехал до границ с Китаем. Мессершмидт был настоящим учёным-энциклопедистом — определял географические координаты и составлял карты, открыл кости мамонта, исследовал животный и растительный мир, минералы, вёл метеорологические наблюдения, собирал этнографические и археологические коллекции. Учёный составил первые словники языков аборигенного населения Сибири с эквивалентами на латинском и немецком языках. На каменных изваяниях он первым открыл средневековую орхоно-енисейскую письменность, которую сумели расшифровать лишь через 150 лет.

Мессершмидт отправлял свои рапорты в столицу, и когда вернулся в 1727 г., все его документы и коллекции, которые он привёз, были переданы в Кунсткамеру. Составленные им карты сибирских регионов засекретили. В Петербурге уже действовала Академия наук, и Мессершмидту, покинувшему Россию в 1728 г., под присягой было запрещено публиковать собранные материалы.

ПЕРВЫЕ ПРЕДПРИЯТИЯ АКАДЕМИИ

Как известно, в 1725 г. в путь отправилась Первая Камчатская экспедиция В. Беринга — первая в России морская научная экспедиция, она осуществила съёмку 3500 км побережья. За ней последовала Великая Северная экспедиция 1733–1743 годов — самое значительное предприятие Академии наук в XVIII веке. В нём участвовали около 500 членов экспедиции и несколько тысяч человек вспомогательного персонала. Семь самостоятельных отрядов экспедиции впервые исследовали огромную территорию северо-востока Евразии, Камчатку, Дальний Восток, открыли и описали территорию Аляски с прилегающими островами (илл. 2).

Важной задачей Академии стало создание точных карт российских территорий. А потому в её структуре выделился крупный картографический центр — Географический департамент. Его возглавил французский астроном, академик Ж. Делиль, свою обсерваторию он разместил на башне Кунсткамеры.

Создание хороших карт — дело непростое и дорогое. Оно требовало привлечения астрономов, математиков, геодезистов, а также художников, гравёров. С 1735 г. в этой работе стал принимать участие академик Леонард Эйлер. Сотрудничество Делиля и Эйлера позволило обеспечить надёжную математическую основу карт.



Иллюстрация 2. Карта российских открытий в Северной Америке и Тихом океане

ЕЛИЗАВЕТА ПЕТРОВНА БЫЛА ПОРАЖЕНА

К сожалению, Делиль оказался человеком недобросовестным, вероятно, французским агентом. В 1747 г. он вернулся во Францию и вывез с собой подлинные и копияные карты XVII — первой половины XVIII веков, в том числе засекреченные картографические материалы Второй Камчатской и других экспедиций, путевые журналы и описания путешествий. Эти документы ныне хранятся в Департаменте карт и атласов Национальной библиотеки Франции. По королевскому приказу собрание подлинных секретных карт из России приобрела французская казна, а Делиль получил от Людовика XV пожизненную пенсию.

Понятно, что императрица Елизавета Петровна была поражена случившимся, вскоре по её указу М. В. Ломоносов возглавил Географический департамент. Он руководил картографией до конца своих дней.

Благодаря Географическому департаменту появился академический «Атлас российский». Он был издан в 1745 г. с пояснительными текстами на русском, латинском, немецком и французском языках. Первый академический атлас представлял собой общую карту Российской империи с отдельными картами губерний. После учреждения в 1762 г. Генерального штаба составление специальных карт империи перешло в его ведение.

А ЧТО БЫЛО ДО ПЕТРА I?

В России всегда было особое отношение к картографии и географии. В своё время академик А. И. Соболевский отметил: «Все лучшие труды по этой науке общего характера, явившиеся в Западной Европе в конце XVI и в XVII веках, были у нас переведены».

Переводили их в Посольском приказе. Это ведомство с самого начала играло в России более значительную роль, чем аналогичные структуры в других государствах. Можно сказать, что в XVII столетии в Посольском приказе ставились и решались многие задачи, которые затем перешли в ведение Академии наук.

В период царствования Алексея Михайловича (1645–1676) поле деятельности московских дипломатов простиралось от Мадрида до Пекина. Количество переводчиков Посольского приказа существенно не менялось (до 30 человек), но их качество заметно улучшилось. Они могли осуществлять письменный перевод более чем с 20 языков. Среди переводчиков появились выпускники европейских университетов, некоторые из них имели опыт западной дипломатической службы, как молдаванин Николай Спафарий. Последний принял участие в написании уникального исторического и художественного документа — Царского титулярника 1672 года. Это был богатый иллюстрированный рукописный официальный справочник,

содержащий информацию дипломатического характера — сведения по русской истории, о родословии и титулах зарубежных государей, гербах и печатях (илл. 3). Н. Спафарий известен как глава российского посольства в Китай 1675–1678 годов и автор первого подробного описания Сибири с указанием географических координат.

Интересно заметить, что один из российских потомков Н. Спафария — Илья Ильич Мечников — стал нобелевским лауреатом по медицине в 1908 году.

«ВЕСТИ-КУРАНТЫ»

Посольский приказ начиная с 1631 года уже постоянно выписывал около двух десятков иностранных газет, журналов и ведомостей. С 1620 года в приказе стали выпускать «вести-курранты», прообраз первой русской газеты. Это были объёмные рукописные обзоры зарубежной периодической печати, предназначенные для царя и правительства — боярской думы; сначала 3–6 номеров в год, затем до 20.

Исследователи отметили важное обстоятельство, связанное с «вестями-куррантами»: несмотря на обилие географических названий, исторических фактов и новых для русского читателя слов иностранного происхождения, в обзорах редко встречаются пояснения. Это свидетельствует о довольно высоком уровне образованности русского правящего слоя. Новые слова, такие как кавалер, прапорщик, маршал, монарх, резидент, президент, студент, миллион, галера, обычно связываемые с началом XVIII века, вошли в русский язык намного раньше — ранее 40-х годов XVII столетия.

ВЗАИМОВЫГОДНЫЙ ОБМЕН

В Москве придавали большое значение тому, как воспринимали в Западной Европе и само государство, и политику Московского правительства. Поэтому Московское государство вошло в число стран-агентов голландского издательского центра, снабжавших Европу информацией о происходящих событиях и получавших взамен соответствующие материалы.

Представители московского правительства, в том числе и иностранцы, занимались в Европе сбором информации, организацией необходимых публикаций, вербовкой тысяч военных и гражданских специалистов для работы в России, закупкой необходимых товаров. Агенты и царские посланники должны были приглашать на работу в Россию лучших специалистов — «инженеров таких, что во всей Еуроппи других таких не будет».

В КОЖАНОМ ПЕРЕПЛЁТЕ, ТИСНЁНОМ ЗОЛОТОМ

Архивы и музеи хранят яркие примеры информационной деятельности Посольского приказа, связанные с экономикой и математикой. Так, в Государственном Эрмитаже имеется

математическая рукописная книга, изготовленная в Посольском приказе в конце 1640-х годов. Эта книга в кожаном переплёте, тиснёном золотом, состоит из двух частей. Её первая часть — «книга сошному письму», т.е. практическое руководство по расчётам, связанным с налогообложением, в 250 страниц. Вторая часть — практическое пособие по математике объёмом в 78 страниц. Привлекает внимание, что рукопись содержит много рисунков, иллюстрирующих «дош-

ный счёт», т.е. расчёты на замечательном древнерусском арифмометре — «дошице счётной». Представление об этом приборе дают знакомые многим большие школьные счёты (станок).

Интересно, что книга была изготовлена для далёкого Кожеезерского монастыря близ Белого моря и долгое время находилась там и использовалась. Монастырь получил книгу как вклад от начальника Посольского приказа думного дьяка Григория Васильевича Львова.

Г. В. Львов, видимо, выступил и в роли заказчика, и в роли редактора. Чёткое и ясное изложение подкрепляется в книге множеством расчётных примеров, хорошо иллюстрированных (илл. 4).

По существу, это оригинальное пособие по вычислительной математике с приложением к денежным расчётам, т.е. к экономике. Г. В. Львов трудился в Посольском приказе 30 лет, до самой своей смерти в 1646 году. В 1633 году патриарх Филарет выбрал хорошо образованного и толкового подьячего Г. В. Львова в учителя своему внуку — царевичу Алексею Михайловичу. Учитель был произведён в дьяки после того, как выучил царевича письму, в том числе и тайнописи.

МЕДИКИ БЫЛИ В ПРИОРИТЕТЕ

Создание Академии наук открыло новые возможности для развития в России и экономики, и математики, и шифровой деятельности. Поначалу, исходя из государственных потребностей, медики были в явном приоритете среди академиков. И первым президентом Академии стал лейб-медик Лаврентий Блюментрост. Между прочим, уже знаменитого физика и математика Даниила Бернулли и двадцатилетнего Леонарда Эйлера пригласили в Академию именно как медиков на кафедру физиологии.



Иллюстрация 3. Царь Иоанн IV, из титулярника 1672 года

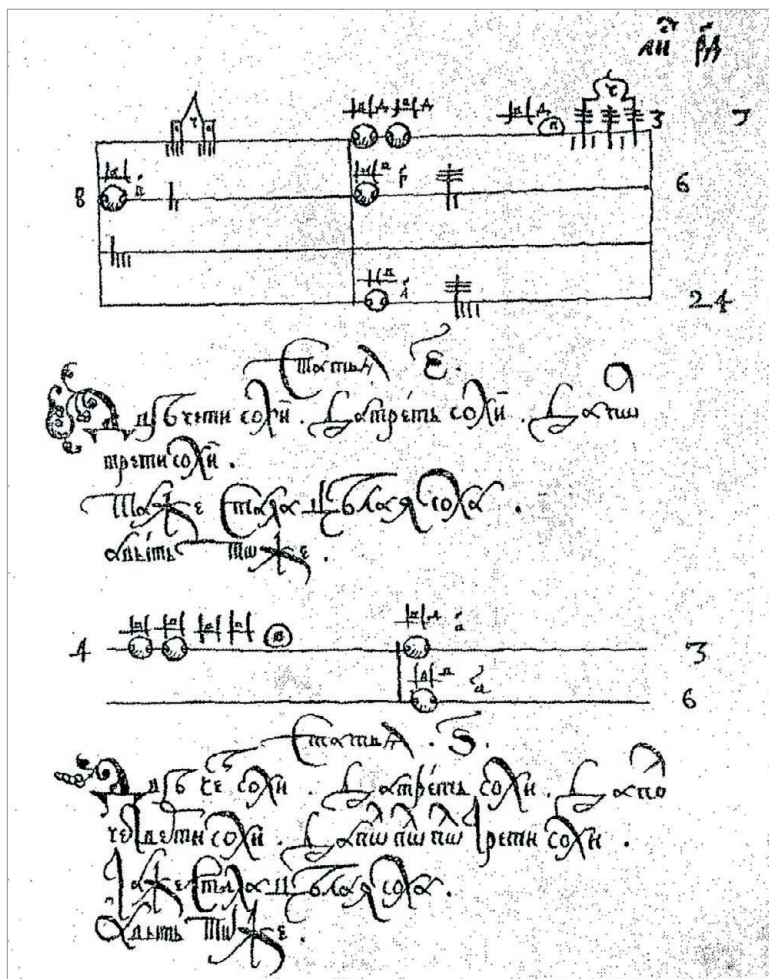


Иллюстрация 4. Страница из книги Г.В.Львова

НЕЗАМЕНИМЫЙ ПОМОЩНИК

Как известно, 1725–1741 годы стали особенно тяжёлыми и для России, и для Академии наук, тогда быстро сменили друг друга шесть императоров и императриц вместе со своим окружением. Академики потянулись в более спокойные и хлебные места Европы. В 1740–1741 годах президентом Академии был Карл Бреверн, до того трудившийся секретарём Коллегии иностранных дел и Кабинета министров. От прежнего руководителя Академии Бреверну в наследство достался толковый помощник президента академик Христиан Гольдбах. Тот быстро заслужил авторитет у своего нового начальника тем, что вполне заменял его на академических собраниях. Когда в конце 1741 г. на императорский престол взошла Елизавета Петровна, К. Бреверн вместе с А. П. Бестужевым-Рюминым возглавили Коллегию иностранных дел и толковый помощник не был забыт. Правда, Бреверн вскоре умер, но способности Гольдбаха уже успел оценить знаменитый организатор российской дипломатии Алексей Петрович Бестужев-Рюмин. Опыт и интуиция подсказали ему, что именно Гольдбах может надёжно обеспечить важную и хлопотную работу с секретной перепиской. Императорским указом

от 18 марта 1742 г. Х. Гольдбах был определён «на особливую должность» в Коллегию иностранных дел.

Надо сказать, что Гольдбах давно стремился избавиться от административной работы и заняться исследовательскими трудами. Таким образом, в свои 52 года он с энтузиазмом стал осваивать новое поприще. Конечно, поначалу потребовалось войти в курс дела. Но уже скоро от него поступили удачные предложения по усилению российских дипломатических шифров. И тогда Бестужев-Рюмин решил проверить возможности Гольбаха на разборе иностранных шифров по материалам перлюстрации, т.е. почтового досмотра в «чёрном кабинете». Как известно, за июль-декабрь 1743 г. академик Х. Гольдбах сумел дешифровать 61 письмо представителей Пруссии и Франции в Петербурге. Эффект был громкий. С той поры враждебные интриги иностранных послов перестали быть тайной для российской власти. Х. Гольдбах возглавлял шифровальную службу до своей кончины в 1764 г.

БЛАГОДАРЯ АКАДЕМИИ

Вспоминая первых петербургских академиков, необходимо заметить, что создание Петром I Академии наук позволило появиться и утвердиться в России величайшему из математиков и одному из крупнейших учёных XVIII столетия Леонарду Эйлеру и его потомкам.

Л. Эйлер приехал в 1727 г. в Россию как медик и сначала проходил как адъюнкт по кафедре физиологии, возглавляемой Д. Бернулли, но вскоре был переведён на кафедру математики. Как известно, с Петербургом связаны два периода жизни Эйлера – 1727–1741 и 1766–1783 годы, там он и упокоился в 1783 г. В промежуток между этими периодами вклинились годы жизни в Берлине, наполненные трудами по организации Берлинской академии наук и руководству ею.

В Петербурге Эйлер очень скоро изучил русский язык и быстро завоевал научную известность и авторитет. В 26 лет женился на своей ровеснице — дочери академического художника. Но уже в 1735 г. в результате кровоизлияния он ослеп на один глаз.

Значение работы в русской академии для себя лично Эйлер так оценил в письме из Германии в 1749 г.: «Что собственно до меня касается, то при отсутствии такого превосходного обстоятельства я бы вынужден был, главным образом, обратиться к другим занятиям, в которых, по всем признакам, мог бы заниматься только крохоборством. Когда его королевское величество (Фридрих II Прусский) недавно меня спросил, где я изучал то, что знаю, я, согласно истине, ответил, что всем обязан своему пребыванию в Петербургской академии».

БЕРЛИНСКАЯ КОМАНДИРОВКА

За 25 лет пребывания в Берлине Эйлер подготовил около 300 работ, причём почти половину из них

впервые опубликовал в трудах Петербургской Академии, где он продолжал оставаться почётным академиком и редактировал математический отдел академических трудов.

Эйлер деятельно участвовал в подготовке кадров для России: в Берлин были командированы для занятий под его руководством будущие академики Котельников, Румовский и Софронов. Эйлер приобретал для академии литературу и оборудование, вёл переговоры с кандидатами на должности в академии. В 1757 г. по его рекомендации в Петербургскую академию приехал из Берлина Франц Эпинус, впоследствии с 1764 по 1797 год возглавлявший Криптографическую службу России.

Эйлер состоял в дружеской и научной переписке с другим, уже активно действовавшим криптографом — Гольдбахом. Как известно, в одном из писем Эйлеру тот сформулировал свою знаменитую проблему, получившую впоследствии наименование проблемы Гольдбаха. У самого Эйлера среди его многообразных занятий не выявлено заметного интереса к криптографии.

«ЧИТАЙТЕ ЭЙЛЕРА, ОН — НАШ ОБЩИЙ УЧИТЕЛЬ»

В 1766 г. Эйлер вернулся в Петербург в окружении 17 членов семьи и родственников. Каждый из них стал специалистом в какой-либо сфере деятельности, и все они пригодились в России. У Эйлера с супругой всего было 13 детей, но выжили лишь три сына и две дочери. Старший сын Иван (Иоганн) к моменту возвращения был уже признанным математиком, членом Берлинской и Петербургской академий.

К сожалению, довольно скоро Эйлер потерял зрение полностью. В это трудно поверить, но его трудоспособность ещё выросла. Благодаря феноменальной памяти и помощи учеников за 17 лет второго периода жизни в Петербурге Эйлер подготовил около 400 работ и 10 книг — итоговых трудов. Это около половины всего его творческого наследия.

Учеников Эйлера назвать очень легко. Мы все являемся его учениками. Хотя бы потому, что важные школьные темы «тригонометрия» и «логарифмы» до сих пор излагаются по Эйлеру. Именно с него началось ясное и доступное изложение математических понятий. По мнению академика Н. Н. Лузина, в середине XX века вузовские учебники высшей математики наполовину состояли из фактов, впервые открытых Эйлером. И ныне ничуть не устарел завет Лапласа: «Читайте Эйлера, он — наш общий учитель».

РОССИЙСКОЕ НАСЛЕДИЕ ЭЙЛЕРА

Леонтий Эйлер, так его вместо Леонарда звали в Петербурге, стал хорошим учителем и мудрым воспитателем, прежде всего, для своих детей. Его старший сын Иван Леонтьевич (1734–1808) известен своими трудами по математике, физике, астрономии



Иллюстрация 5. Леонард Эйлер на почтовой марке

и механике, много лет был секретарём Академии наук. Потрудился он и на поприще криптографии. Так, Т. А. Соболевой удалось найти документы, подтверждающие, что Иван Эйлер работал в секретной экспедиции Коллегии иностранных дел и составлял шифры. На некоторых из них сохранилось его имя. Второй сын, Карл Леонтьевич (1740–1790), стал доктором медицины, придворным врачом.

Третий, младший сын Христофор Леонтьевич (1743–1808), выбрал военное поприще. Он служил в артиллерии, заведовал постройкой Сестрорецких оружейных заводов и руководил ими. Участвовал в войне со Швецией 1788–1790 годов, достиг чина генерал-лейтенанта и заслужил орден Св. Георгия 4-й степени. Христофор Леонтьевич положил начало воинскому служению российской ветви Эйлеров. Его сыновья Фёдор, Александр и Павел заслужили боевые награды в Отечественной войне 1812 г. Подполковник Фёдор Христофорович Эйлер, как и его отец, стал кавалером ордена Св. Георгия 4-й степени. Александр и Павел дослужились до генеральских званий. Впрочем, на военном поприще отличились потомки и других сыновей Л. Эйлера. Один из них, мичман Дмитрий Павлович Эйлер, стал участником подвига крейсера «Варяг» в 1904 г. и тоже удостоился ордена Св. Георгия 4-й степени.

Потомки Л. Эйлера в течение столетия принимали прямое участие в руководстве Академией наук. К 1917 г. среди его потомков насчитывалось много учёных, инженеров, дипломатов, врачей и военных. По подсчётам историков, перед 1991 г. в СССР проживали около 200 потомков Л. Эйлера. Таков его вклад в человеческий капитал нашего Отечества.

Академия наук, начало которой было положено Петром I, пустила корни в России и за 300 лет глубоко проросла в её почву.

«ТАК СОШЛИСЬ ЗВЁЗДЫ — Я И POSITIVE TECHNOLOGIES...»

РАЗГОВОР BIS JOURNAL С АЛЕКСЕЕМ ЛУКАЦКИМ — БРЕНДОМ И ЧЕЛОВЕКОМ

ЗВЁЗДНАЯ СИТУАЦИЯ

— Сегодня словосочетание «Алексей Лукацкий» — это бренд. На конференциях модераторы давно уже не представляют вас по должности или званию. Просто Алексей Лукацкий. Популярность не утомляет?

— Я не так популярен, как звёзды шоу-бизнеса, к которым на сцену прорываются фанатки или подкарауливают у дома и пишат на тротуаре белой краской: «Лёша, я хочу от тебя сына!» Так что пока терпимо...

— Вы звезда по жизни, характеру или это вынужденная ситуация?

— Я следую принципу «не сотвори себе кумира» и не очень понимаю, что значит «звезда» применительно к сфере ИБ. Известный человек? Да, возможно. Но не более. Прекрати писать или выступать, и тебя забудут через год, как это происходило со многими.

ИСТОКИ

— Мне кажется, что со школьных времён вы не очень-то изменились. Так и вижу такого мальчишку-знайку, маленький танк, с которым не поспоришь. А как было на самом деле? Каким вы были в школьные годы?

— Это было так давно, что я уже и не помню, я ведь учился ещё в советской школе. Помню, что меня называли лучшим математиком класса, помню, что не пошёл служить в КГБ, когда в выпускном классе меня туда пригласили, ну и помню, как разбил стекло в актовом зале на выпускном...

— С какими мыслями, ожиданиями, настроениями вы поступали в МИРЭА? И почему именно в МИРЭА?

— Тут как раз всё было просто. Изначально я поступал на мехмат МГУ, на котором экзамены проходили на пару недель раньше, чем в остальных вузах. Я сдал вступительные экзамены, но не был уверен, что прохожу по баллам. Решил подстраховаться, а МИРЭА был на той же ветке метро, всего в трёх станциях от «Университета». Так что я просто подал документы в институт, в котором в итоге и проучился пять с половиной лет. Потом я

уже узнал, что прошёл бы на мехмат по баллам, но кто знает, кем бы я стал в этом случае.

— Кто и как повлиял на выбор специальности: родители, учителя, друзья, случайные связи?

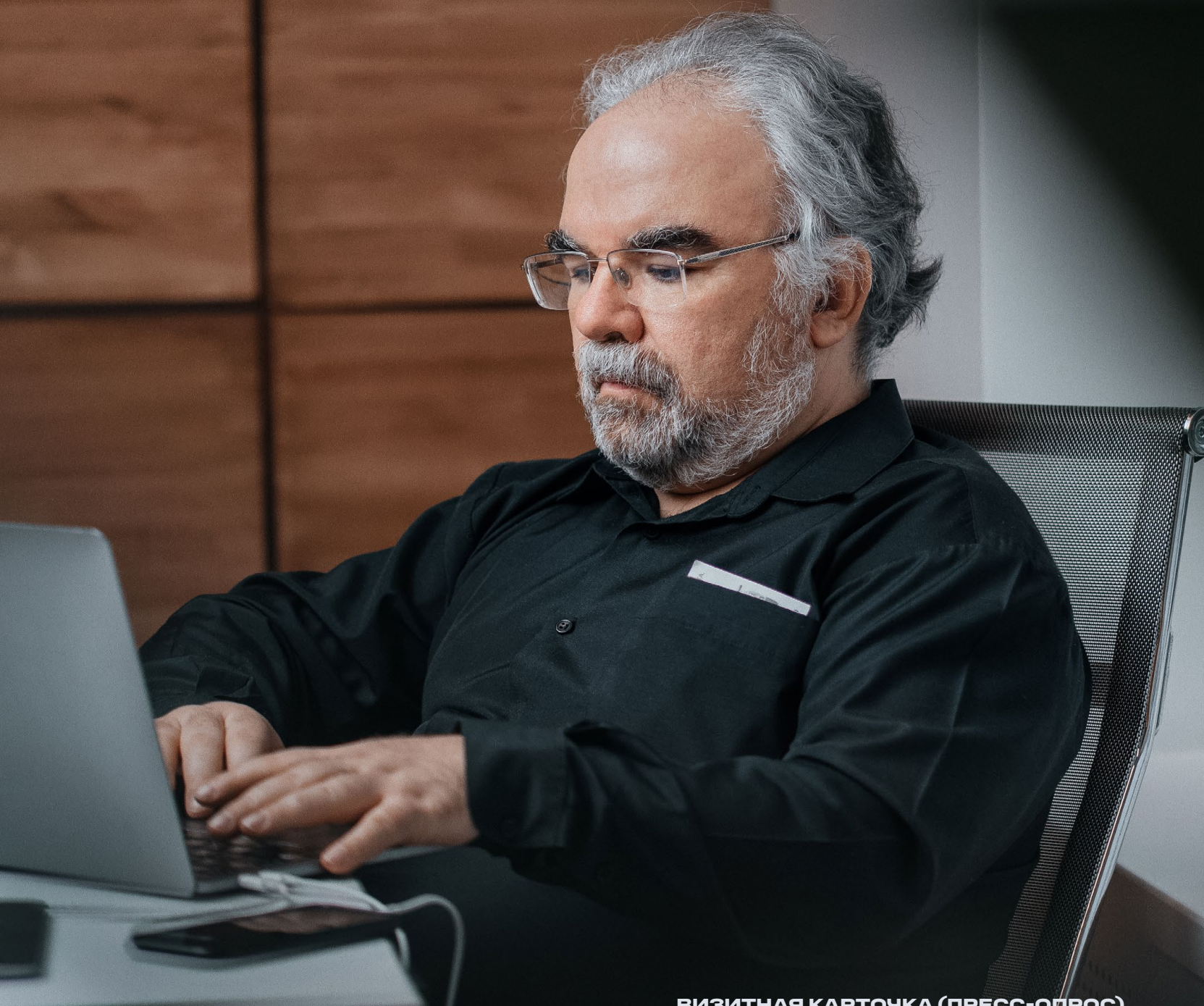
— Я учился в математическом классе, и мне нравилась информатика, где мы писали программы, учились создавать алгоритмы и вот это вот всё. Преподавал у нас выпускник мехмата, так что мой первоначальный выбор был сделан скорее под влиянием учителя информатики. А прикладную математику я выбрал потому, что на ней была самая большая в Советском Союзе стипендия — 75 рублей против 55 у остальных, даже айтишных специальностей.

МИРЭА

— Какую роль в вашей жизни сыграл вуз? Чему научил? Если вернуться в прошлое с сегодняшним опытом, куда бы вы поступали?

— Честно говоря, я вряд ли смогу сформулировать, чему меня научил вуз. Можно, конечно, сказать, что школа дала мне социализацию, а институт научил учиться и самостоятельно искать информацию, но это было бы слишком просто. Я точно не использую большую часть из тех предметов, что учил в МИРЭА. Ни матан, ни функан, ни компьютерную графику, ни проектирование процессов или создание грамматик языка, ни распознавание образов или теорию графов. Даже знание методов спецслужб иностранных государств мне не пригодилось, так как в реальности всё было немного не так, как нас учили. Возможно, что-то из этого и пригодилось бы, но не в информационной безопасности. Но я могу сказать, что в ИБ я попал именно благодаря МИРЭА, так как по распределению со второго курса стал один день в неделю трудиться в одном московском «ящике», как раз в отделе защиты информации. Это и предопределило моё будущее. Так что выбор профессии для меня — это вопрос случая, а не спланированная акция.

И вернись я в прошлое, я вряд ли бы что-то изменил. Всё-таки в семнадцать лет молодёжь не способна осознанно выбирать свою профессию, о чём говорит и опыт моих однокурсников, — мало кто из них пошёл трудиться по специальности.



ВИЗИТНАЯ КАРТОЧКА (ПРЕСС-ОПРОС)

Ваше кредо? Всегда!

Ваши цели? Везде!

Ваши кумиры? Не сотворил.

В чём смысл жизни? Быть полезным и не стыдиться смотреть людям в глаза.

Считаете ли, что состоялись в жизни?
У меня всё впереди — я пока не собираюсь уходить на пенсию.

Чего вам не хватает? Времени!

Какие планы на будущее, лет 10–15?
Дописать начатые книги.

Ваши любимые:

Времяпровождение? Камин, коньяк, сигара, загородный дом.

Блюда? Коньяк, морковь и солёные огурцы.

Книги? Когда-то их было немало. Но со временем понимаешь, что не может быть одной любимой книги. В разные периоды заходит что-то своё, чего раньше не понимал.

Фильмы? «Собачье сердце», «Семнадцать мгновений весны».

Города? Лондон, Сан-Франциско, Торжок, Суздаль.

Анекдоты? Не запоминаю.

— Исходя из опыта, подсказываете своим детям, куда пойти учиться, или даёте свободу выбора?

— Дети должны сами выбирать своё будущее, а родители не должны через них реализовывать свои несбывшиеся мечты. Поэтому мой сын самостоятельно выбирал себе и специальность, и вуз. А дочери ещё пока рано об этом думать — ей бы школу сначала окончить.

— Какие вузы сегодня, на ваш взгляд, готовы лучших ибэшников?

— Никакие. Мы просрали высшее образование в области ИБ, и те, кто стоит сейчас у руля отечественного ИБ-образования, только загоняют нас в... ещё глубже. Это боль, и обсуждать эту тему тяжело. Будь моя воля, я бы разогнал всех старпёров, которые утверждают ФГОСы по ИБ, заседают в учёных советах, пишут бессмысленные учебники и выбирают себе гранты. Они как кандалы на ногах отечественной ИБ — не дают ей нормально развиваться.

Нам вообще не нужно столько ибэшников с высшим образованием. Лучше развивать СПО в этой области, а то и вовсе заниматься профпереподготовкой в рамках корпоративных университетов. Фундаментальное образование по ИБ нам нужно для формирования прослойки методологов, архитекторов, специалистов по общению с бизнесом, но их вузы сегодня не готовят, так как там просто некому готовить таких экспертов.

ПРО НАУКУ

— Вы могли пойти в науку, но в своей официальной биографии пишете, что кандидата технических наук Лукацкого не случилось по причине наличия плагиата в работах будущих научных руководителей. Не отдаёт ли это юношеским максимализмом?

— Конечно, отдаёт. Когда я был молод, я не понимал, почему какой-то завкафедрой моей аспирантуры должен присваивать результаты моего труда, к которому он не имеет никакого отношения и вообще «пороха не нюхал». Примерно так же сегодня думает молодёжь обо мне (правда, я ни у кого не ворую контент, прекрасно понимая ценность чужого творчества). Я тогда предал огласке этот случай, но никакого эффекта это не возымело. Сейчас эти люди продолжают учить будущих ибэшников, и для меня остаётся загадкой, как могут учить защищать информацию те, кто её же ворует.

Второй раз мне предложили получить «кандидата» при условии, что я напишу книгу по ИБ и возьму в соавторы своего потенциального научного руководителя. За это мне обещали «защиту без проблем». И этого старпёра я послал в пешее эротическое путешествие. Третий раз в эту «реку» я входить уже не захотел.

— Нет ли сегодня желания всё-таки сказать своё слово в науке: повторить попытку и за-

щитить кандидатскую, докторскую? Вам, безусловно, есть что сказать. О чём вы хотели бы написать сегодня?

— А зачем? Когда ты молод, ты гоняешься за заветными тремя буквами (к. т. н.) на визитке. А сейчас мне не надо доказывать своим родителям, что их сын чего-то стоит. Тратить своё время на защиту диссертации я сейчас уже не вижу никакого смысла — всё, что я хочу сказать, я говорю на мероприятиях, в блоге, в курсах, в телеграм-канале. Это гораздо ценнее для людей, чем пылящаяся в библиотеке диссертация, которую никто не будет читать или, ещё хуже, будут троллить в интернете.

НАЧАЛО В ПРОФЕССИИ

— Как вы пришли в информационную безопасность?

— В МИРЭА была практика отправлять студентов в поля, в места будущей работы. Так я попал в один московский «ящик», который писал для Минобороны систему защиты. Работал там четыре года, начиная со второго курса, — занимался разработкой подсистемной криптографической защиты информации. Параллельно стал активно писать в эхах FIDOnet (прообраз Интернета) RU.SECURITY и RU.CRYPT, первое из которых потом и «возглавил» как модератор. На последнем курсе нашёл себе работу администратором ИБ в ретейле, но был сокращён как самый молодой специалист, когда холдинг столкнулся с кризисом. Потом была работа в банке, после чего меня сманил к себе покойный Володя Гайкович из «Информзащиты», где, наверное, я и состоялся уже как специалист по ИБ, попробовавший себя в совершенно разных ролях — аудитора, создателя сайта, создателя ИБ-контента, продавца, маркетолога, преподавателя...

— Вы работали в ИБ с 1992 года. Какой была ИБ тогда? Кто и как ей занимался? Как представлялось будущее профессии?

— ИБ была в самом-самом зачаточном состоянии. Первые ибэшники были «бывшие» сотрудники КГБ или Гостехкомиссии, которые ушли на вольные хлеба и свои знания по борьбе с иностранными техническими разведками и защите гостайны стали применять в коммерции. Активно развивалось направление защиты от утечек по техническим каналам. Персоналки уже не были редкостью, в отличие от локальных сетей. Поэтому защита заключалась в том, что надо было бороться с вирусами, распространяющимися на пятидюймовых дискетах от компьютера до компьютера. Эпидемией считалось заражение пары десятков компьютеров за неделю-две-три. Криптография была засекреченной — я ещё застал время, когда книги по ней относились к технологиям двойного назначения и их невозможно было достать в обычных библиотеках. Гражданская ИБ только-только начала зарождаться, но, как и сейчас, у её истоков

стояли те же самые по образованию и менталитету люди. Так что если отбросить в сторону чисто технологическую сторону, то сама отрасль ИБ в России за 30 лет мало поменялась.

«НЕ ТЕМ Я ЦЕНЕН»

— Опыт практической работы руками остался в далёком прошлом, все считают вас «бумажным безопасником». А сможете сегодня самостоятельно настроить с нуля систему защиты в небольшой организации?

— Как минимум я знаю, ЧТО надо делать. КАК — это уже другой вопрос. Если меня попросить настроить Active Directory или права доступа к файлам в Linux, мне придётся поднимать мануалы, и я точно где-то ошибусь или накосячу. Но включить автоматическое обновление ОС и приложений, выбрать правильный пароль администратора, внедрить MFA, настроить условный «микротик» или «кинетик» на периметре и сконфигурировать Wi-Fi я смогу. В этом плане небольшая организация мало чем отличается от моей домашней сети с парой десятков устройств, подключённых к интернету и требующих своей защиты. Но вообще достаточно странно от меня требовать доказывать «кто я такой» за счёт настройки NGFW или поиска уязвимостей в сети; я ценен другим, как мне кажется.

CISCO

— Вы проработали в Cisco 18 лет. Как вы в неё попали?

— За давностью лет и не вспомню, но вроде это было стечение обстоятельств. В «Информзащите» мне было уже тесновато, а Cisco расширялась, и ей нужен был человек на продвижение кибербеза. Мой друг, Миша Кадер, работавший там, порекомендовал меня. Прошёл семь собеседований, и меня взяли. Так и сложилось...

— Какую роль в вашей жизни сыграла эта компания? Чему научила?

— Ответу на этот вопрос можно посвятить целую книгу. Всё-таки работа в американской компании сильно отличается от любой отечественной. Как минимум это доступ к самым современным технологиям и знаниям, которые было непросто получить в российской компании, даже во времена геополитического потепления. Это совершенно иной масштаб деятельности и, как следствие, возможность изучать ИБ в Азии, Африке, Америке, Европе, не закукливаясь внутри железного занавеса. Это сильно расширяет кругозор.

Ну и, конечно, нельзя не сказать о том, что работа в международной публичной компании, работающей в разных юрисдикциях, заставляет немного по-другому относиться и к тому, что, как и кому ты говоришь, а также видеть и чувствовать, что такое процесс с чёткими входными и понят-



ными выходными параметрами. И это касается как разработки ПО или продаж, так и маркетинга и развития бизнеса. Это то, чего пока не очень хватает российским предприятиям.

— Судя по всему, именно там и родился тот Алексей Лукацкий — человек-бренд, которого мы все знаем. Так ли это?

— Нет, не так. Началось всё, как мне кажется, с публикации книги «Обнаружение атак» в 2001 году. Cisco просто дала возможность рассказывать о кибербезе для более широкой аудитории.

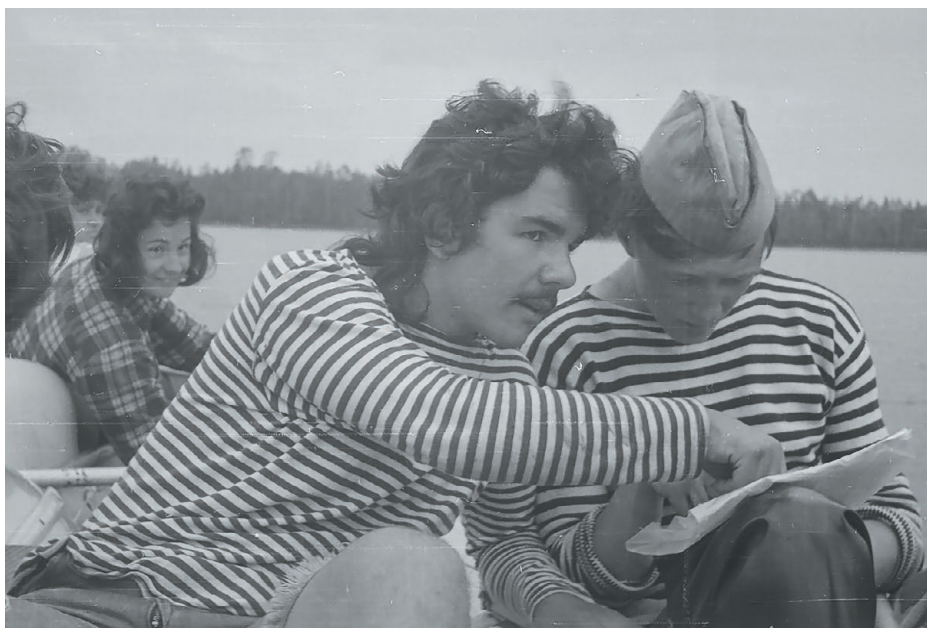
— Как пережили уход из компании? Варианты уехать из страны не рассматривали?

— Отвечу коротко: «Пережил и чувствую себя сейчас позитивно!»

POSITIVE TECHNOLOGIES

— Как попали в Positive? Чем там занимаетесь?

— Так сошлись звёзды — я и «Позитив». На самом деле вариантов было немного. Дело в том, что, несмотря на растущий рынок отечественного кибербеза, у нас не так уж много компаний, которые не погружены только в продуктовую историю, а готовы инвестировать в отрасль, заниматься её образованием, проводить различные социальные проекты и выполнять многие иные задачи, выходящие за привычную маркетинговую историю ИБ-вендора. У «Позитива» всё это было и есть. Так что тут я нашёл для себя возможность продолжать заниматься евангелизацией ИБ, комбинируя опыт, полученный в крупном международном вендоре, с возможностями, которые есть у Positive Technologies. И при этом, что мне очень импонирует, «Позитив» готов к экспериментам и нестандартным инициативам, которые невозможно себе представить в американской или европейской, очень compliance-ориентированной компании.



О СВОБОДЕ И ТВОРЧЕСТВЕ

— Насколько для вас важна свобода действий? Если условный работодатель скажет: «С завтрашнего дня быть на рабочем месте с 9 до 18, офисный стиль, делать только то, что укажут, регулярные отчёты и KPI по пятницам», — как долго протянете в таком режиме?

— Подобные вопросы я сначала задам на собеседовании, и если меня не устроит ответ, то я вряд ли устроюсь в такую компанию. Cisco научила меня, что важен не рабочий график и постоянная отчётность, а результат, который ты приносишь. Можно соблюдать трудовой распорядок, но не приносить никакой пользы. А можно быть разгильдяем, но при этом приносить половину дохода своей компании. Сейчас я уже просто не смогу работать в условиях военной дисциплины и отсут-

ствия свободы действий. Кроме того, мы забываем простую мысль, что «согласие есть продукт при полном непротивлении сторон». Не только работодатель выбирает меня, но и я работодателя. Он не может мне навязать что-то, к чему я не готов и чего не хочу. Это звучит странно, но, возможно, именно поэтому я тот, кто я есть. Я за свободу выбора, а не принуждение к работе за зарплату.

ДВУЛИКИЙ ЯНУС

— Возвращаясь к выбору профессии. Алексей Лукацкий — автор сотен отличных статей в СМИ, писатель, ведущий популярного блога. Может, стоило пойти в журналистику? Или вы придерживаетесь взглядов, что инженер может работать журналистом, а журналист инженером — нет?

— Если бы я пошёл в журналистику, мне бы не о чем было писать и пришлось вымучивать материалы согласно редакционному плану или заданию. А как специалист по ИБ я могу творить на любую тему в этой области, погружаясь на любую глубину. Бывают, конечно, и журналисты-исследователи, которые тратят много времени на какую-то тему, но, увы, в России таких не осталось. Большинство современных материалов носят оперативно-новостной характер, не подразумевающий глубокого погружения в тему.

— **Не соглашусь. Например, ведущая рубрики «Тема номера» в BIS Journal Елена Покатаева каждый раз очень глубоко погружается в тему. Но сегодня наш герой всё-таки вы, поэтому следующий вопрос. Вы человек с разносторонними интересами: с одной стороны, вы входите в профильные комитеты Федерального агентства по техническому регулированию и метрологии и ФСТЭК, занимаетесь вопросами стандартизации, законотворческими инициативами, что понятно только узкому кругу специалистов. Консультант крупного вендора. С другой — вы популяризатор кибербезопасности, который на простых и доступных примерах показывает, какую роль ИБ играет в жизни государств, отраслей, компаний и обычных граждан. Автор и ведущий интеллектуальных игр. Какая сторона деятельности вам ближе и даёт больше возможностей для самореализации?**

— Начнём с того, что больше полутора лет я уже не занимаюсь нормативкой и законотворчеством. Для меня это всегда была вынужденная деятельность, которой я занимался постольку-поскольку. А в последние годы я перестал улавливать логику в большинстве принятых законодательных инициатив, и мне просто стало неинтересно биться о стену непонимания наших карательных органов, которые пишут и принимают нормативку по ИБ. В Positive Technologies мне, к счастью, практически не нужно вовлекаться в эти задачи, и я ими занимаюсь только тогда, когда это может положительно повлиять на результативную, а не бумажную кибербезопасность. Поэтому сейчас у меня больше евангелистской деятельности для разных целевых аудиторий.

О СЕМЬЕ

— **Алексей Лукацкий в семье — какой он?**

— Мне бы хотелось уделять семье больше внимания, чем удаётся. Получается это не очень, но я безмерно ценю, что моя семья понимает это.

— **А дети? Расскажите немного о них. Оба будут безопасниками? Чем они увлекаются, к чему стремятся? Как влияют на папу?**

— Сын пошёл также на прикладную математику, как и я в своё время, но я никак не влиял на



его выбор. Будет ли он безопасником? Не знаю. Не уверен, что это будет лёгкий путь для него. Дочери ещё рано думать о своём будущем — она учится в седьмом классе. Но мне кажется, безопасником она тоже не будет: она творческий человек и ей ближе то, к чему у меня никогда не лежала душа, — музыка, рисование и т.п.

— **Есть ли у вас досуг? Какой он?**

— У японцев есть такой термин «икигай», то есть когда в одном человеке сошлось то, что он любит, то, в чём он хорош, то, что нужно миру, и то, за что ему платят деньги. Мне кажется, мне удалось найти свой «икигай» и поэтому мой досуг так или иначе связан с ИБ. В свободное время, если я не провожу его с семьёй, я пишу, делаю презентации или записываю видео.

— **В блоге вы сказали, что увлекаетесь туризмом. Когда успеваете? Где побывали? Чем гордитесь?**

— Сейчас на это времени уже не остаётся, но в своё время я прошёл или проплыл достаточно много мест в европейской части Советского Союза и России — Карелия, Кольский, Карпаты, Крым, Кавказ, Урал. В Cisco удалось поехать по США, намотав не одну и не пять тысяч километров на автомобиле. Побывал в командировках в Африке, Азии, Европе, Северной Америке, даже в Исландии. Но есть места, где моя нога ещё не ступала, и я бы хотел это осуществить. В России — это плато Путорана и Камчатка, а за её пределами — Южная Америка и, возможно, Антарктида. Но время ещё есть, и я надеюсь, что мне удастся это осуществить.

Вопросы задавала
Марина Бродская

НЕДЕКЛАРИРОВАННЫЕ ПОДАРКИ

НОВОГОДНИЕ РАЗМЫШЛЕНИЯ О ПОЛЕЗНЫХ ФУНКЦИЯХ, НЕИЗВЕСТНЫХ ДАЖЕ РАЗРАБОТЧИКАМ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИБ



Сергей ВИХОРЕВ
советник генерального
директора
ООО «ИТ-Экспертиза»

О говорюсь сразу: во-первых, отнеситесь к этому опусу немного с юмором в преддверии Нового года, но серьёзно. Во-вторых, недокументированные (недекларированные) возможности здесь я рассматриваю в частном случае, когда возможности системы, скрытые от (или неочевидные для) конечного потребителя, являются недекларированными функциями. Если классическая дефиниция ГОСТа предполагает две части: описание сущности и вызванные ею последствия (нарушения свойств информации), что и придаёт этому понятию

отрицательную коннотацию, то здесь мы ограничимся исключительно описательной частью (недокументированные возможности — это возможности технических устройств и/или программного обеспечения, не отражённые в документации) и тем самым устраним эту отрицательную коннотацию.

Дело в том, что разработчик (изобретатель) в силу своей зашоренности на решении основной задачи не задумывается над побочными функциями, которые может выполнять его детище. А иногда эти побочные функции оказываются весьма полезными и нужными. Попробую объяснить это «на яблоках». Все знают, что пресс-папье — это один из предметов письменного набора, представляющий собою полукруглый брусок с рукояткой сверху и с прикрепляемым снизу листком промокающей бумаги, который служит для промокания написанного. Здесь основная функция — это промоkanie написанного. Но, так как сейчас мало кто пользуется перьевыми ручками, потребность в промокании ушла в прошлое и пресс-папье пылится без дела на столе. Но вот если посмотреть на это устройство немного шире, то окажется, что



его можно довольно ловко использовать для колки орехов или подпорки для створки окна, чтобы оно не закрылось. Да, эти функции не описаны при продаже пресс-папье, но они существуют! И открывают эти побочные, но полезные функции не сам разработчик, а, как правило, пользователь в процессе эксплуатации. А потому они не всегда известны другим пользователям, но знание их бывает весьма полезным.

Конечно, проанализировать все продукты, которые используются для обеспечения безопасности информации, у меня не получится, к сожалению, у меня нет таких возможностей, но показать на примере наиболее знакомого мне продукта я попробую. Думаю, что это исследование подвигнет и других посмотреть на продукты немного под другим углом и обнаружить те самые полезные недокументированные функции. Буду благодарен всем, кто проведёт и обнаружит такую работу, ведь это позволит ещё эффективнее использовать средства защиты информации, и не только для её защиты.

Итак, речь пойдёт об известном многим продукте «САКУРА». Поскольку это средство мониторинга, то основное назначение этого комплекса,

заявленное разработчиком, — мониторинг рабочих мест информационной системы, регистрация событий безопасности и управление безопасностью информации. Эти функции оказались полезными для ИБшников и нашли у них свой положительный отклик.

Но давайте посмотрим, кому ещё могут быть полезны результаты мониторинга, проводимого продуктом «САКУРА». Продукт одновременно контролирует множество параметров информационной системы, в том числе фиксирует, на какие сайты «ходит» пользователь и сколько времени он там проводит. При правильном анализе такая информация может быть очень полезна для HR-службы. Можно, например, определить, какие кафе предпочитают посещать сотрудники, и организовать там корпоративный праздник. Или помочь составить топ игр, в которые играют сотрудники, и организовать своеобразные и популярные сейчас фиджитал-игры для командообразования. А может быть, выявить список наиболее популярных стран для отдыха и устроить (если, конечно, позволяют средства) там выездной семинар для партнёров и заказчиков.

Полезна и другая незаъявленная функция комплекса. «САКУРА» позволяет определить и зафиксировать, сколько времени проводит пользователь в той или иной прикладной программе или сколько времени он использует принтер. Кроме того, что это помогает администратору безопасности следить за правильностью действий пользователя, это может быть очень полезно сисадмину или офис-менеджеру. Например, компания закупила 100 лицензий для достаточно дорогого ПО по заявкам руководителей подразделений. При этом заявки подавались из расчёта всех пользователей, включая начальника, его секретаршу (на всякий случай!), помощника начальника и ещё кого-то. А по прошествии времени оказалось, что активно используют это ПО всего 5 человек. Представляете, какая экономия, если продлевать не 100, а только 5 лицензий! Так же и с принтером — можно оптимизировать закупку бумаги исходя из реальной потребности. Да и отличить, с какого компьютера выходит в сеть удалённый: «правильный» рабочий или «худой» домашний — тоже не проблема.

В общем, «недекларированных функций» может оказаться не меньше заявленных. Поэтому я и обращаюсь к другим пользователям (да и производителям!): может быть, пора провести ревизию таких «недекларированных» функций других продуктов и поделиться своими наблюдениями с обществом? Может получиться неплохой реестр! И в заключение оговорюсь ещё раз: в этой статье речь не идёт о НДС в классическом, ГОСТовом понимании, которые могут привести к нарушению защищаемых свойств информации. Наоборот, надеюсь, что продукты, которые могут быть помещены в этот реестр, будут свободны от таких классических НДС.

В ЖЕРНОВАХ ПРОЦЕССОВ

ЗАМЕТКИ БЕЗОПАСНИКА

Александр ИГОНИН
эксперт BIS Journal

Чтобы бизнес жил, необходима скоординированная работа всех трёх частей ЛПТ-триады: людей, процессов и технологий. Стоит чему-то одному чуть помалиться и начать сбивать, как итоговый результат непременно ухудшится. Но какая же из трёх ножек нашего табурета доставляет больше всего забот тем, кто пытается на нём усидеть? Ответ на этот вопрос вроде бы очевиден: конечно же, самый неустойчивый и проблемный элемент системы — люди. Однако я со временем всё сильнее склоняюсь к тому, что таким элементом являются процессы.

Процессы — это тот цемент, который связывает воедино людей и технологии, чтобы они взаимодействовали и выдавали желаемый результат. «Результат» здесь — понятие очень широкое: это и качественное оказание услуг внутренним и внешним потребителям, и обеспечение управляемости и отчётности для руководства компании, и (в контексте нашей специфики) минимизация вероятности возникновения инцидентов ИБ, и многое, многое другое. Но просто связать людей с технологиями мало: вторая, куда более сложная, задача — обеспечить предсказуемость и повторяемость действий обоих компонентов в самых разнообразных условиях. И здесь возникают две проблемы: нужно, во-первых, предусмотреть как можно больше возможных ситуаций, и... во-вторых — добиться того, чтобы и люди, и технологии функционировали так, как это установлено процессами.

Как вы, возможно, заметили, оба перечисленных пункта я поставил на первое место, и не случайно. Прописать слишком мало ситуаций — плохо, потому что это превращает работу в непрерывный

концерт художественной самодеятельности, что не очень хорошо для бизнеса. Однако в борьбе с народным

творчеством корпорации часто сваливаются в другую крайность: создание такого количества инструкций, что они вроде бы и регламентируют каждый шаг и чих сотрудников — но в реальности ни один человек в компании оказывается не в состоянии удержать их все в голове. А в особо запущенных случаях различные документы и вовсе начинают содержать взаимоисключающие требования.

Конечно, в реальной жизни между регламентами и работой «на земле» всегда будет ощутимый лаг. Тем не менее можно постараться его уменьшить, если придерживаться некоторых принципов. Я бы выделил два основных.

Первый: постоянный контроль за выполнением процессов и требование их соблюдения (что в английском языке описывается ёмким словом *enforce*). Люди всегда стремятся упростить себе жизнь, и даже технологии (как железо, так и софт) имеют тенденцию со временем ломаться. Поэтому без должного контроля любой процесс способен за несколько месяцев превратиться в труху, восстановить которую до исходного состояния обычно гораздо тяжелее, чем не допустить такой деградации.

Второй: максимальная стандартизация и автоматизация. Всё же основной «вклад» в деградацию процессов вносят именно люди, поэтому нужно стараться создать условия, при которых не следовать процессу сотрудникам будет сложнее, чем следовать. Да, это непросто и требует внедрения дополнительных технологических «прокладок»: внутренних порталов, клиентских приложений, более сложной логики хранения и доступа к данным. Но зато в финале это и снизит вероятность человеческой ошибки, и ускорит обучение сотрудников, и затруднит жизнь внутренним нарушителям ИБ, и — самое главное! — обеспечит предсказуемые и повторяемые результаты.

В одной крупной компании топ-менеджмент довольно успешно внедрил очень сильный принцип: «наши корпоративные руководящие документы либо исполняются, либо отменяются». Хотите чего-то, что запрещено политикой? Можете пообщаться с вице-президентом, который её подписал, и аргументировать, почему он неправ. Многие сотрудники были недовольны — но зато в масштабе всей компании это давало потрясающий эффект стабильности и предсказуемости. Жаль, что примеров такого волевого подхода очень мало. Хочется надеяться, что со временем их будет становиться больше.





МОСКВА, КЛАСТЕР «ЛОМОНОСОВ»

23 МАЯ 2024

ФОРУМ

ТЕХНОЛОГИИ ДОВЕРЕННОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

ОБСУЖДАЕМЫЕ ВОПРОСЫ:

- Вопросы создания доверенного искусственного интеллекта (ДИИ)
- Разработка требований к системам ДИИ и нормативно-правовых основ обработки персональных данных (включая их обезличивание)
- Безопасность данных и искусственный интеллект
- Современные математические методы интеллектуальной обработки данных
- Атаки на системы искусственного интеллекта и методы защиты
- Применение ИИ для решения задач в области безопасности
- Организация программ поиска уязвимостей (Bug Bounty) в системах ИИ

ОРГАНИЗАТОРЫ



Академия
криптографии
Российской Федерации



АНО «Национальный
технологический центр
цифровой криптографии»



Институт системного
программирования
им. В. П. Иванникова РАН

ПРИ ПОДДЕРЖКЕ



Министерство цифрового развития,
связи и массовых коммуникаций
Российской Федерации



trust-ai.ru

kaspersky

Регуляторный хаб знаний

Отраслевой навигатор
по законодательству и требованиям ИБ



regulhub.kaspersky.ru

