



18>

Анатолий АКСАКОВ
Государственная дума РФ
**Законодатели идут
в ногу со временем**

31>

Екатерина КАЛИНИНА
SWIFT
С точки зрения SWIFT



40>

Алексей РАЕВСКИЙ
Zecurion
Идеальная DLP-система



72>

Андрей ЧАПЧАЕВ
ИнфоТекС
ИнфоТекСу — 30 лет!

108>

Марина БРОДСКАЯ
BIS Journal
**Это Cyber EdTech,
детки!**

128>

Александр БОДРИК
Cyberlands.io API Penetration
Testing Company
**Топ-12 мер
безопасности для API**

УЧИТЕЛЯ ГОДА: ЗУМБОМБЕРЫ И КИБЕРХУЛИГАНЫ



Проекты Медиа Группы «Авангард»

Онлайн и офлайн-мероприятия

Отраслевой журнал BIS Journal

Интернет-телекомпания BIS TV

Энциклопедия безопасника

ib-bank.ru



**Окупись в мир
информационной
безопасности!**



АВАНГАРД



Артём ЗУБКОВ
генеральный директор
Медиа Группы «Авангард»

Дорогие наши читатели, коллеги-безопасники, спешу разделить с вами радость по поводу того, что весна в разгаре и COVID-19 идёт на спад. Худо-бедно, но идёт... Собственно в этом и заключается главный весенний тренд.

Но это в эмоциональном плане. Рациональный тренд, который красной нитью проходит через весь новый номер BIS Journal — это осмысление полученного опыта. Что было? Что стало? Что со всем этим делать?

Вот, например, для клиентов банков мир стал, безусловно, более удобным. Пандемия привела к увеличению лимитов на переводы, расширению возможностей дистанционной идентификации и упрощению подтверждения операций.

В то же время и мошенничество расцвело новыми цветами. Если год назад клиент рисковал только деньгами во вкладах, то сегодня на вас могут оформить кредит в любом банке и украсть даже то, чего у вас нет. Легко! При этом риски, связанные с удобством управления деньгами, полностью перекадываются на клиентов. Основной причиной роста мошенничества объявляется низкий уровень киберграмотности населения. Конечно, очень удобно при росте разбоев заявить, что всё дело в населении — боксом не занимаются, ходят без оружия...

Во время пандемии многие действия и риски были оправданы, но сейчас (с наступлением весны) логично позаботиться и о защите прав потребителей. А именно, исключить навязывание дополнительных финансовых сервисов, обеспечить надёжную идентификацию и аутентификацию, остановить, наконец, социальную инженерию... Ну, хотя бы исключить возможность подмены злоумышленниками официальных банковских телефонных номеров! И, конечно, многое другое, включая утечки данных и неотвратимость наказания за мошенничество.

Как это сделать? Очень просто: надо думать и обсуждать. Объединять усилия и снова думать, и снова обсуждать. Более эффективной методики принятия правильных решений история, простите за каламбур, ещё не придумала. И хочу напомнить, именно для этого в нашей отрасли существует Медиа Группа «Авангард» — как инструмент активизации коллективного отраслевого мышления. BIS Journal, BIS TV, форумы, онлайн- и офлайн-конференции — всё это разные формы масштабного отраслевого мозгового штурма. Формы управления стихией рационального и эмоционального интеллекта.

Все вопросы решаемы. Нужно только крепко подумать. Подумать вместе.

Переверните страницу нового номера BIS Journal и начинайте... думать вместе со всеми.

ОБЩЕСТВЕННЫЙ РЕДАКЦИОННЫЙ СОВЕТ

Войлуков А.А. — вице-президент Ассоциации банков России
Емельянов Г.В. — член-корреспондент Академии криптографии РФ, действительный государственный советник РФ 3 класса
Сычёв А.М. — Первый заместитель директора Департамента информационной безопасности Банка России, доктор технических наук
Шипилов В.В. — исполнительный директор Ассоциации российских банков, кандидат технических наук

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Былевский П.Г. — шеф-редактор, 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. — специалист Службы информационной безопасности КБ Максима (ООО)
Вихорев С.В. — советник генерального директора по информационной безопасности IT Expertise
Воробьёва А.А. — руководитель интернет-проектов
Дзержинский Ф.Я. — главный эксперт — координатор системной экспертизы ООО «ТехноСофт»
Зубков А.Н. — генеральный директор ООО «Медиа Групп» «Авангард», директор Фонда содействия развитию безопасных информационных технологий (ФСРБИТ)
Курило А.П. — заведующий кафедрой международной информационной безопасности МГЛУ, кандидат технических наук
Левинов Д.О. — председатель Совета НП «Партнёрство специалистов по информационной безопасности»
Мельников С.Ю. — заместитель генерального директора ООО «Лингвистические и информационные технологии», кандидат физико-математических наук
Некрасов И.В. — главный редактор журнала
Одувалов М.В. — руководитель службы Управления по обеспечению ИБ Банка ВТБ (ПАО)
Окулесский В.А. — заместитель начальника службы ИБ банка «Возрождение», кандидат технических наук
Пазизин С.В. — заместитель начальника Управления по обеспечению ИБ Банка ВТБ (ПАО), кандидат физико-математических наук
Рачкова Е.В. — заместитель начальника Управления по обеспечению ИБ Банка ВТБ (ПАО)
Филиппчук А.А. — технический директор ГК ЦРТ
Шумский Л.С. — CISO в Ассоциации «Финтех»
Янсон И.А. — бизнес-партнер по информационной безопасности, Департамент безопасности ПАО «Сбербанк России», кандидат физико-математических наук

ЭКСПЕРТНАЯ ГРУППА

Баранов А.П. — заведующий кафедрой комплексной безопасности критически важных объектов в Университете нефти и газа им. И.М. Губкина, доктор физико-математических наук, академик Академии криптографии РФ
Батранков Д.В. — консультант по информационной безопасности Palo Alto Networks
Гадарь Д.А. — вице-президент — директор департамента информационной безопасности, Tinkoff.ru
Калемберг Д.А. — генеральный директор ООО «СэйфТек»
Лукацкий А.В. — бизнес-консультант по безопасности Cisco Systems
Сабанов А.Г. — заместитель генерального директора ЗАО «Аладдин РД»
Сумманен К.Т. — директор по управлению проектами — вице-президент, Банк ВТБ (ПАО), кандидат физико-математических наук
Хайретдинов Р.Н. — директор по росту компании BIZONE

РЕДАКЦИЯ ЖУРНАЛА

Главный редактор: **Некрасов И.В.**
Шеф-редактор: **Былевский П.Г.**
Директор по развитию: **Минаков А.В.**
Арт-директор: **Мельников Н.С.**
Руководитель интернет-проектов: **Воробьёва А.А.**
Ответственный редактор: **Седов О.В.**
Обозреватели, корреспонденты: **Куликов В.А., Бродская М.А., к.т.н.**
Иллюстрация на 1-й обложке: **Viktor Miller-Gausa**
Фото в номере: **DepositPhotos, Виталий Вилкин**
Цветокорректор: **Науменко М.Б.**

УЧРЕДИТЕЛЬ-ИЗДАТЕЛЬ

ООО «Медиа Групп» «Авангард»
Адрес: 127473, Россия, Москва, 3-й Самотечный переулок, д.21
Тел.: +7 499 271-70-85
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). Свидетельство ПИ № ФС 77-61378 от 10 апреля 2015 г.

Все права на материалы, опубликованные в номере, принадлежат журналу «BIS Journal — Информационная безопасность банков». 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.

Подписан в печать 20.04.2021. Тираж 5000 экз. Заказ № 562021.
Цена договорная. Отпечатан в типографии «Московский Печатный Двор», 123298, г. Москва, 3-я Хорошевская 18, корп. 1, офис 201А

© BIS Journal, 2021



НОВОСТИ

5 В России, в мире, криминал



ТЕМА НОМЕРА: БАНК ДАННЫХ УГРОЗ

- 8 Сергей Вихорев (ИТ-Экспертиза)
Блеск и нищета... БДУ
- 11 Артём Калашников (BIS Journal)
Главное — ущерб!
- 12 Василий Окулесский (BIS Journal)
Тусклый блеск... «науки в жизнь»
- 14 Юрий Язов (Воронежский
государственный технический
университет)
Нищета... знаний о БДУ



РЕГУЛЯТОРЫ

- 18 **Законотворчество**
Анатолий Аксаков (Государственная дума)
Законодатели идут в ногу со временем
- 22 **Киберполигон**
Павел Былевский (BIS Journal)
В России создаётся Национальный киберполигон
- 25 **Тенденции**
Артём Сычёв (Банк России)
В перекрестье прицела «кибербригады»



БАНКИ

- 28 **Вредные советы**
Екатерина Рачкова (Банк ВТБ)
Проверка по 716-П. Разберитесь в себе
- 31 **Платёжные системы**
Екатерина Калинина (SWIFT)
С точки зрения SWIFT
- 34 **Аудит**
Валерия Мещерякова (BIS Journal)
От хаоса к порядку
- 37 **Новые технологии**
Денис Батранков (BIS Journal)
Что такое SASE

УГРОЗЫ И РЕШЕНИЯ

- 40 DLP**
Алексей Раевский (Zecurion)
Выбор идеальной DLP-системы
- 44 DLP**
Артём Киселёв (StaffCop)
Версия 4.9. Теперь действительно больше!
- 47 DLP**
Дмитрий Горлянский (Гарда Технологии)
Тотальный перехват
- 50 DLP**
Алексей Парфентьев (СёрчИнформ)
Не все DLP «одинаково полезны»
- 54 Импортзамещение**
Дмитрий Курашёв (UserGate)
Превосходство российского решения
- 56 Аутентификация**
Илья Осадчий (Тайгер Оптикс),
Виктор Сердюк (ДиалогНаука)
Silverfort защищает... незащищаемое
- 60 Периметр**
Алексей Кузнецов (BI.ZONE)
Управление поверхностью атаки
- 62 Квантовая криптография**
Елена Верещагина
(СМАРТС-Кванттелеком)
Другое шифрование
- 65 ИТ-инфраструктура**
Батр Альчинов (АМТ-ГРУП)
Управляем сетевым доступом быстрее и эффективнее
- 68 КИИ**
Максим Темнов (СТИ)
Простая логика
- 70 Аудит**
Роман Косичкин (ГК «ЦИБИТ»)
Аудит — не отчёт!





ИНФРАСТРУКТУРА

- 72 Юбилей**
Андрей Чапчаев (ИнфоТеКС)
ИнфоТеКСу — 30 лет!
- 77 Юбилей**
Александр Виноградов (КБ Максима),
Владимир Голованов (ИнфоТеКС)
ТК 122 / ПК 1 — 10 лет!
- 80 Деловые мероприятия**
Кибербезопасность — наши дни.
Промышленные технологии — 2021
- 82 Деловые мероприятия**
Марк Новодачный (BIS Journal)
iFin 2021
- 84 Деловые мероприятия**
Виктор Вячеславов (Innostage),
Владимир Дмитриев (CyberART)
The Standoff 2021
- 86 Электронная подпись**
Иван Янсон (BIS Journal)
Закон «Об электронной подписи»:
жизнь после принятия
- 91 Аутентификация**
Всеволод Шейкин (ТК 26)
Дружелюбные пароли
- 95 ИБ и геополитика**
Денис Батранков (BIS Journal)
Кибернаёмник? Спецслужба? Хулиган?

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

- 98 Обучение персонала**
Ольга Лимонова, Андрей Жаркевич
(ООО «Антифишинг»)
Как пробудить движущую силу
- 103 Фишинг**
Виталия Демехина (ООО «Антифишинг»)
Обмануть, чтобы защитить
- 106 Антифрод**
Игорь Шульга (Информзащита)
«Серебряная пуля» против
мошенничества

ОБРАЗОВАНИЕ И КАРЬЕРА

- 108 Обзор иноСМИ**
Марина Бродская (BIS Journal)
Это Cyber EdTech, детки!
- 111 Обзор**
Марина Бродская (BIS Journal)
Абитуриент-2021
- 113 Соцопрос**
Анастасия Московкина, Дарья Чуб (МГЛУ)
Юзеры против хакеров

СУБЪЕКТЫ

- 118 История**
Борис Столпаков (историк криптографии)
Гигант математической мысли и дела
- 123 История**
Борис Столпаков (историк криптографии)
В начале столетнего пути
- 128 Заметки безопасника**
Александр Бодрик (Cyberlands.io)
Топ-12 мер безопасности для API

ПЕРВЫЙ В РОССИИ... БЛОКЧЕЙН-ОПЕРАТОР

Участники Ассоциации ФинТех (АФТ) — ВТБ, Газпромбанк, ПСБ, Национальная система платежных карт, Московская биржа и сама АФТ — учредили первого в России блокчейн-оператора: ООО «Системы распределенного реестра».

С момента основания АФТ изучала потенциал распределенных реестров для финансового рынка. Результатом стали новые финансовые сервисы на блокчейн-платформе Мастерчейн. На сегодня Мастерчейн — единственная блокчейн-платформа в России, прошедшая сертификацию на применение российских стандартов криптографии. Сервисы, созданные и пропилотированные на платформе Мастерчейн (для учета залоговых и выпуска цифровых банковских гарантий), продемонстрировали свою востребованность и стали основой для дальнейшего развития сервисов в рамках ООО.

Участники АФТ приняли решение о выделении блокчейн-направления в отдельную юридическую структуру для развития российских ИТ-сервисов и технологий, как с использованием Мастерчейн, так и других блокчейн-платформ в дальнейшем. ООО станет одним из центров компетенций по применению технологии распределенных реестров на российском финансовом рынке.



POSITIVE HACK DAYS «СТРЕЛЯЕТ» ДУПЛЕТОМ

Культовый форум «Positive Hack Days 10: Начало» откроет свои двери 20–21 мая 2021 года в Центре Международной Торговли, а за два дня до этого стартует его «младший брат» — The Standoff. Оба мероприятия все желающие смогут посетить онлайн.

На PHDays выступят российские и зарубежные разработчики, представители государственной власти, CIO

и CISO крупнейших отечественных и международных компаний, ведущие специалисты банков, телекоммуникационных, нефте- и газодобывающих, промышленных и ИТ-компаний. Запланированы десятки докладов, мастер-классов, круглых столов и пр. Форум традиционно наполнится масштабной конкурсной программой.

В 2020 году киберполигон The Standoff отделился от PHDays и стал самостоятельным направлением. The Standoff — это цифровой двойник современного мегаполиса, превращенный в поле битвы для «хакеров» и «защитников» и наглядно демонстрирующий, насколько важно бизнесу иметь риск-ориентированную ИБ-стратегию.

PHDays в этом году пройдет в гибридном формате: часть участников посетит площадку лично, часть — в онлайн-формате. The Standoff будет доступен зрителям только онлайн.



«ОБНАЛИЧКУ» СНОВА ПРИЖАЛИ

Банк России ужесточил требования к кредитным организациям по контролю за обналичиванием и отмыванием денег: вдвое снизил порог, за которым банк считается причастным к сомнительным операциям.

Теперь банк будет считаться причастным к сомнительным действиям, если сумма таких операций за квартал превысит 500 млн руб. (сегодня порог — 1 млрд руб.). Требования к максимально допустимой доле сомнительных операций клиентов остаются прежними: их удельный вес в обороте не должен превышать 2% в квартал.

По данным регулятора, в период 2016–2020 гг. объем вывода денег за рубеж по сомнительным операциям сократился в четыре раза (до 52 млрд руб.), а «обналичка» — в семь раз (до 78 млрд руб.).

В ЦБ РФ также отметили, что банки в целом соблюдают установленные ограничения.

APPLIST



Рекомендуемые приложения

ВСЕ СВОИ

Минцифры разработало и запустило приложение App List — каталог всех отечественных приложений.

«App List — каталог лучших приложений для смартфонов и планшетов на русском языке. Все приложения бесплатны и безопасны. Мы знаем, где искать свежие новости, заказывать вкусную еду и учиться новым профессиям», — гласит описание приложения. Внутри App List можно увидеть категории «На каждый день» (33 приложения), «Медиа и СМИ» (32 приложения), «Культура» (17 приложений), «Государственные приложения» (14 приложений), «Общение и коммуникации» (19 приложений), «Еда и продукты» (4 приложения), «Товары и услуги» (23 приложения), «Авто» (3 приложения), «Образование» (15 приложений), «Работа» (4 приложения) и «Спорт» (5 приложений).

«ГОСДОКИ». УЖЕ В ЭТОМ ГОДУ?

Для замены бумажных документов электронными уже в этом году будет разработано приложение «Госдоки». Беспрецедентная разработка заявлена в рамках проекта «Цифровой профиль гражданина» (ЦПГ), за который отвечает рабочая группа «Национальная инновационная система» во главе с вице-премьером Дмитрием Чернышенко.

«Госдоки» переведут в электронный вид СНИЛС, ОМС, ИНН, водительское удостоверение и другие документы (всего 30 видов). При этом, по задумке авторов, бумажные аналоги (кроме паспорта) выдавать больше не будут. Это позволит сэкономить ресурсы на печати 5 млрд бумажных документов в год.

Новый софт могут запустить уже в этом году. Разработка оценивается в 1,3 млрд рублей. Разработчик пока неизвестен.

И СНОВА... ГОСДЕП США

Киберпреступники похитили тысячи официальных электронных писем Государственного департамента США. Они получили доступ к переписке Бюро по делам Европы и Евразии, а также Бюро по делам Восточной Азии Госдепа. Это уже второе за шесть лет проникновение на почтовые серверы ведомства, приписываемое русским хакерам.

«Департамент серьезно относится к своей ответственности по охране информации и постоянно принимает меры по обеспечению её защиты. Из сообщений безопасности в настоящее время мы не можем обсуждать природу или масштабы каких-либо предполагаемых инцидентов», — сообщили в пресс-службе Госдепа.

Скомпрометированные бюро работают над вопросами, касающимися союзников США, в том числе НАТО, а также европейских и индо-тихоокеанских партнёров.

СБП ИДЕТ НА ЗАПАД

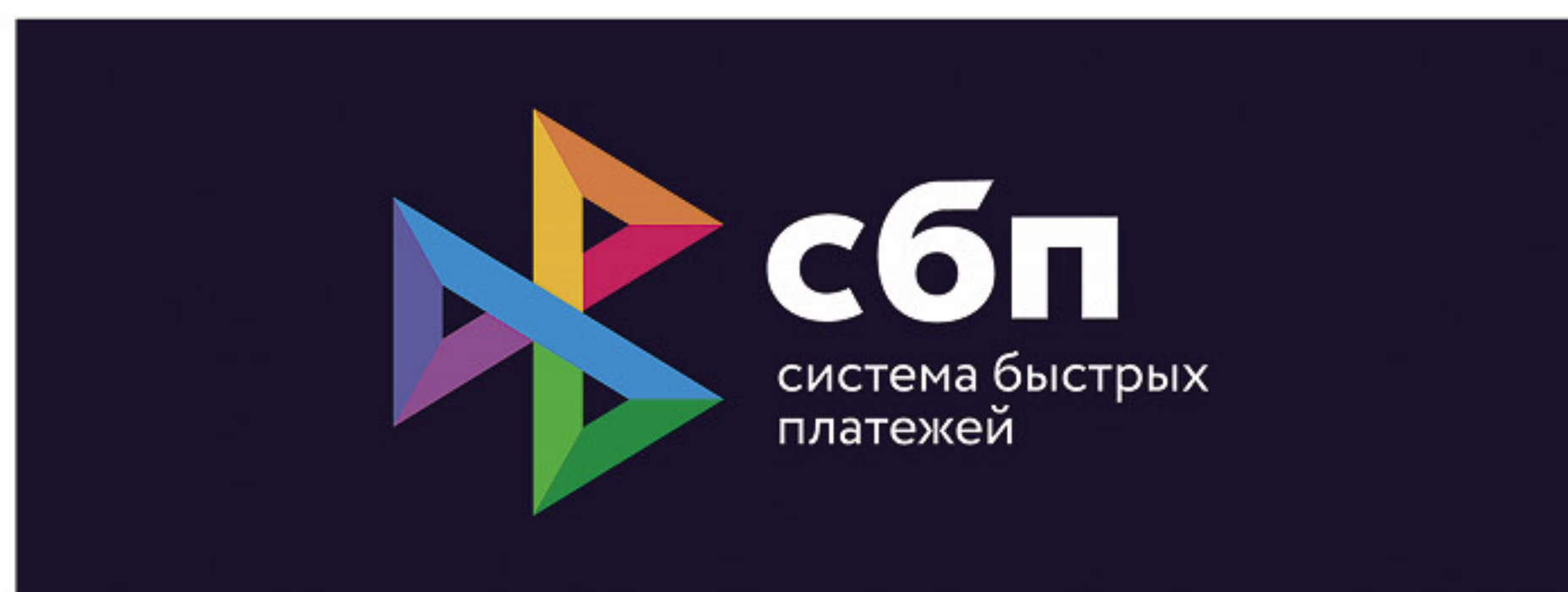
Белоруссия станет первой страной, в которую россияне смогут — к концу следующего года — переводить деньги через Систему быстрых платежей, сообщила директор Департамента национальной платёжной системы Банка России Алла Бакина.

О планах внедрить переводы через СБП за рубеж стало известно ещё в 2019 году. Чтобы люди быстро и дёшево переводили средства в другие страны не по карте, а со счёта на счёт, Национальная система платёжных карт, обрабатывающая

межбанковские переводы через СБП, подписала соглашение с Mastercard.

14 апреля ЦБ РФ представил стратегию развития национальной платёжной системы (НПС) до 2023 года. Её цель — создать условия для оказания удобных и доступных платёжных услуг гражданам, бизнесу и государству.

Так, в течение ближайших двух лет регулятор собирается расширить сотрудничество в сегменте быстрых платежей между банками ЕАЭС (в Армении, Белоруссии, Казахстана, Киргизии и России).



ИРЛАНДИЯ ВЗЯЛАСЬ ЗА FACEBOOK

Ирландская Комиссия по защите данных проверяет сведения об утечке из Facebook базы с информацией о 533 млн пользователей социальной сети, заявил замглавы регулятора Грэм Дойл.

В Facebook утверждают, что подразумевается тот же массив данных, об утечке которого стало известно ещё в 2019 году.

«После появившихся в СМИ сообщений [о распространении БД на хакерском форуме] мы изучаем ситуацию, чтобы установить, идёт ли речь о том же массиве данных», — сообщил Дойл. И добавил, что эта конкретная утечка произошла до вступления в силу европейского закона о защите персональных данных, что «станет серьёзным осложнением при попытке привлечь соцсеть к ответственности за недостаточно надёжное хранение данных граждан ЕС».

Головной офис европейского представительства Facebook расположен в Ирландии, поэтому именно ирландский регулятор должен следить за соблюдением компанией европейского закона о защите персональных данных.



ОПАСНЫЕ ОТВЕТЫ

В Москве отмечены случаи записи и последующего использования злоумышленниками голосов клиентов для оформления кредитов или иных финпродуктов.

Правоохранители рассказали, что мошенники звонят клиентам кредитных организаций и задают вопросы, требующие односложных ответов. Жертвы же узнают об оформлении кредитов, когда с их карт списываются средства.

«Зная, что некоторые банки предоставляют услугу оформления кредита по биометрическим данным, злоумышленники совершают звонки клиентам банков, использующих услугу распознавания голоса, и задают вопросы, на которые требуется отвечать только «да» или «нет». Разговор записывается, после чего мошенники используют записи ответов для оформления кредитов на своих жертв», — сообщили в московской полиции.



ТРИ ШТРАФА ЗА ДЕНЬ

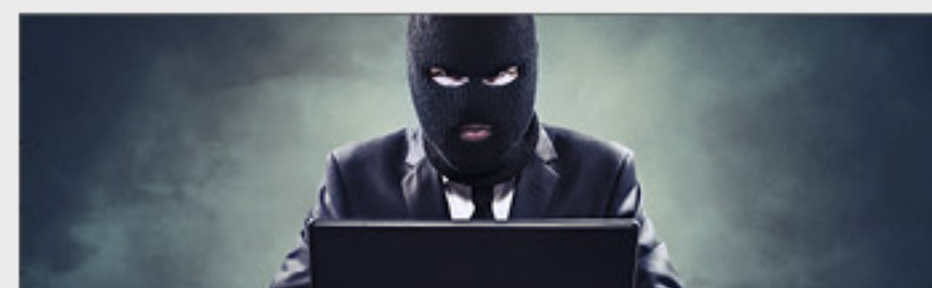
Мировой судья Таганского района Москвы оштрафовал соцсеть Twitter на общую сумму в 8,9 млн рублей за не удаление противозаконного контента.

Штрафы в 3,3 млн 3,2 млн и 2,4 млн рублей были присуждены по ч. 2 ст. 13.41. КоАП РФ («Нарушение порядка ограничения доступа к информации, доступ к которой подлежит ограничению в соответствии с законодательством РФ»). Подразумевается

неудаление твитов с призывами к подвигам выходить на несогласованные акции протеста.

Ранее Роскомнадзор в своих требованиях к Twitter заострял внимание на твитах с призывами к суициду, детской порнографией и информацией о наркотиках.

С момента вступления решения суда в силу у сервиса будет 60 суток на выплату штрафов.



ДВА РАЗА В МЕСЯЦ

В апреле на один из хак-форумов два раза подряд выложили базы с данными 500 млн пользователей соцсети LinkedIn. Это около 70% зарегистрированных там аккаунтов.

Сведения содержат ID учётных записей, имена, имейлы, телефонные номера, информацию о работе, а также ссылки на аккаунты в других соцсетях.

«Пока мы всё ещё изучаем эту проблему, но опубликованные данные, по-видимому, включают общедоступную информацию, полученную из LinkedIn, а также данные, собранные с других сайтов», — рассказал представитель площадки.

Хакеры могут использовать персональные данные для кибератак на компании через информацию о сотрудниках, прокомментировал инцидент аналитик Пол Прюдомм.

РУССКИЙ ХАКЕР РАСКАЯЛСЯ

Американский суд обязал российского киберпреступника Андрея Тюрину выплатить компенсацию потерпевшим — почти 20 млн долларов. Также его приговорили к 12 годам тюрьмы.

Судебное заключение гласит: жертвам преступлений ответчик «должен выплатить компенсацию общей суммой в 19 952 861 доллара». Приговор Тюрину был вынесен в январе, и россиянин признал себя виновным. По данным следствия, фигурант причастен к крупнейшей в истории страны краже персональных данных клиентов банков и брокерских фирм — тогда была скомпрометирована информация более чем о 80 млн клиентах JPMorgan Chase & Co, Dow Jones & Co, Fidelity Investments, E-Trade Financial и др.

В своём последнем слове подсудимый заявил, что «занимался незаконными вещами» и раскаивается в содеянном.

Хотели как лучше,
а получилось как всегда...

В. С. Черномырдин

БЛЕСК И НИЩЕТА... БДУ

О БАНКЕ ДАННЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ФСТЭК РОССИИ¹



Сергей ВИХОРЕВ
советник
генерального
директора
ООО «ИТ-Экспертиза»

О банке данных угроз безопасности информации ФСТЭК России регулярно пишут разные авторы. И меня не миновала чаша сия. Оговорюсь сразу: речь пойдёт о том разделе, который посвящён именно угрозам безопасности информации. С разделом уязвимостей более или менее всё ясно: вендор, ПО, уязвимость, идентификатор, способ применения и способ устранения. Чего не скажешь о разделе с угрозами. Мнения об этом разделе самые разные: от полного неприятия до панегириков. А истина — она, как всегда, где-то посередине. Сейчас ФСТЭК России задумался о совершенствовании своего детища. Вот и давайте посмотрим на банк угроз непредвзято, может, что-то полезное и появится...

ОБЕЩАТЬ — НЕ ЗНАЧИТ ЖЕНИТЬСЯ

К чему это я? А вот к чему. Стоит открыть любой документ ФСТЭК России, касающийся требований к мерам защиты, и мы увидим: «Требования к системе защиты информации информационной системы определяются в зависимости от... угроз безопасности информации». И далее: «В качестве исходных данных для определения угроз безопасности информации должен использоваться банк данных угроз безопасности информации» (bdu.fstec.ru).

Замечательно, продекларировали! А дальше что? А дальше — провал. Я уже как-то писал об этом². Меры защиты выбираются исходя из класса информационной системы (который, кстати, определяется совсем по другим критериям и не обращает внимания на угрозы) или требуемого уровня защищённости, но никак не отталкиваясь от угроз. Нет взаимосвязи между самими угрозами и теми мерами, которые позволяют их нейтрализовать. Получается, что в данном случае угрозы, вернее модель угроз, построенная на их основе, выступает в качестве

некоего «сферического коня в вакууме». Только не подумайте, что я против модели угроз как таковой! Нет! Может быть, повторюсь, но считаю, что сама идея — использовать модель угроз при выборе мер защиты — абсолютно верная. Однако, не отрицая важности самого процесса оценки угроз безопасности информации при выборе адекватных мер защиты, необходимо отметить, что многолетняя практика моделирования угроз для каждого конкретного объекта показывает свою НЕэффективность. Ситуация получается очень похожей на басню Крылова (правда, немного в другой коннотации): «Вертит Очками так и сяк: То к темю их прижмёт, то их на хвост нанижет, То их понюхает, то их полижет; Очки не действуют никак». И происходит это по банальной причине: нет связи между угрозами и мерами. Вот давайте посмотрим на раздел банка угроз, связанного с уязвимостями. Там есть не только привязка уязвимости к конкретному ПО и его версии, что позволяет однозначно определить необходимость принятия мер, но и такие замечательные рубрики, как «Возможные меры по устранению уязвимости» и «Способ устранения». А это уже прямое руководство к действию. Поэтому этот раздел оказывается весьма полезным в практической деятельности ибэшников. К сожалению, этого нельзя сказать про раздел угроз безопасности информации. Правда, некоторые специалисты пытаются составить таблицы соответствия угроз и мер защиты³, но, честно говоря, это всё-таки самоделки. Здесь нужен системный подход, чёткая проработка и соответствующие разделы в банке угроз. Вот тогда-то модель угроз станет действенным инструментом при выборе мер защиты и не потребует заставлять бизнес разрабатывать формальную модель угроз («документ ради документа»), он сам почувствует её необходимость, так как это будет экономить деньги. А ещё лучше, если угрозы будут увязаны не

¹ Начало дискуссии в BIS Journal № 1/2020.

² С. В. Вихорев, «Перемен! — требуют наши сердца», BIS Journal № 1/2020.

³ Связь между угрозами из БДУ ФСТЭК и мерами защиты | Про ИБ (<https://zen.me/Wslr>)

только с мерами защиты, но и с необходимыми функциями безопасности, которые реализуются средствами защиты (читай классами средств защиты). Тогда модель угроз станет бесценной.

СМЕШАЛИСЬ В КУЧУ КОНИ, ЛЮДИ...

А теперь вот о чём. Не всё, что в банке угроз названо угрозами, является таковым. Просто кое-что, отнесённое к классу угроз, не вписывается в классическое определение угроз. Частенько идёт подмена понятий. Кстати, об определении. Как сказал классик, «прежде чем объединяться и для того, чтобы объединиться, мы должны сначала решительно и определённо размежеваться». В нашем случае объединяться — это составить банк угроз, а размежеваться — чётко определить те сущности, которые мы собираемся объединять. Попробуем «размежеваться». И главное здесь, конечно, — понятие угрозы.

Глупо полагать, что обеспечением безопасности информации занимаются только для того, чтобы поддержать соответствующие службы и производителей средств защиты. Эгоизм правит миром, и поэтому любая деятельность по обеспечению безопасности информации направлена только на то, чтобы не допустить ущерба обладателю от нарушений полезных свойств информации. Поэтому примем за аксиому, что угроза — это некие негативные действия, угрожающие интересам субъекта (обладателя информации). А отсюда следует, что угроза может быть только тогда, когда есть субъект, которому может быть причинён ущерб. Поэтому «угрозы информации» быть не может в силу того, что информация является объектом отношений, а не субъектом. Может быть только «угроза безопасности информации», то есть угроза состоянию защищённости информации.

Действительно, даже если будут в силу каких-то обстоятельств нарушены полезные свойства информации (конфиденциальность, целостность, доступность), это не причинит никакого вреда, если нет субъекта, заинтересованного в обеспечении сохранности этих полезных свойств. Любые негативные действия могут быть совершены только при наличии каких-нибудь слабых мест (уязвимостей), ведь если, к примеру, кто-нибудь захочет проникнуть за кирпичную стену и будет биться в неё головой, то, скорее всего, у него ничего не получится, однако наличие в стене деревянной калитки уже значительно повышает шансы на успех его героических попыток. И уж, конечно, если есть какие-то негативные действия, то их кто-то или что-то должен совершать. И мы вроде бы пришли к классическому определению угрозы

безопасности информации — совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации⁴. Это можно выразить формулой:

$$U = f(I, F, M),$$

где: I — источник угрозы, F — фактор, обуславливающий реализацию угрозы, M — метод реализации угрозы

Но такое представление угрозы всё-таки будет не совсем точным. Обратим внимание, что в определении «условия» и «факторы» даны во множественном числе. Поэтому правильное будет так:

$$U = f(\{I \in S_I, F \in S_F, M \in S_M\}),$$

где: S_I — множество (совокупность) всех источников угроз, S_F — множество всех факторов, обуславливающих реализацию угрозы, S_M — множество всех методов реализации угрозы

Одна и та же угроза может быть реализована различными источниками угроз, различными способами и с использованием различных факторов. Совокупность условий и факторов, определяющих конкретную угрозу, будет определяться множеством всех возможных вариантов (комбинаций) реализации данной угрозы различными источниками с использованием различных методов и факторов.

Давайте посмотрим это «на яблоках». Положим, у кого-то есть сейф, в котором лежит бриллиантовое кольцо, а Некто задумал это кольцо экспроприировать. В нашем случае в качестве Некто может быть: а) тривиальный вор (внешний нарушитель), б) любимый сын (внутренний нарушитель), в) случайный сантехник (посетитель).

Этот Некто может: i) вскрыть сейф дубликатом ключа, ii) взломать его фомкой, iii) разрезать автогеном. В этом случае угрозой можно считать кражу (кольцо). Тогда источники — вор, сын, сантехник; уязвимости (факторы) — ошибки хранения, слабый сейф, тонкий металл; методы — вскрытие, взлом, резка. И всё это может быть в разных комбинациях. Получается, что угроза — одна, а реализаций — много.

В существующем банке угроз, к сожалению, всё смешано в кучу: и угрозы, и их реализации. Описать угрозы — можно, это всегда конечный перечень. Описать все возможные реализации угроз — задача благородная, но практически не реализуемая в силу большого разнообразия сущностей, её составляющих.

⁴ ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения», п. 2.6.1.

Ну а если ещё идёт смешение сущностей — получается «Бородино». Нужна какая-то система. И тут на сцену выходит дедушка Карл Николиус Линней со своей таксономией⁵.

КАРЛ ЛИННЕЙ — ЭТО ЗАЧЕМ?

И чем так привлекателен для нас «отец систематики» Карл Линней? Наверное, самое важное — это то, что он нашёл тот самый критерий или признак, который, с одной стороны, является общим для всех систематизируемых сущностей, а с другой — индивидуален для каждой такой сущности. Тычинка! Вернее, их количество — вот что объединяет и в то же время разъединяет сущности, и это самое главное открытие Линнея в деле систематизации по признакам их сходств и различий. И в результате получилась иерархическая, чётко ранжированная структура, состоящая из отдельных групп — таксонов⁶: класс — отряд — семейство — род — вид — подвид — разновидность.

В деле систематизации угроз безопасности — на опыте «отца систематики» — надо прежде всего найти такой критерий. На первый взгляд, ответ лежит на поверхности: таким критерием должно выступать полезное свойство информации, которое надо защищать (конфиденциальность, целостность, доступность). Но не всё так просто. Я уже отмечал, что эти свойства в принципе весьма субъективны и зависят от заинтересованности субъекта в обеспечении сохранности этих полезных свойств. А брать за критерий

⁵ Таксономия — это теория систематизации сложноорганизованных областей действительности и знания, имеющих иерархическое строение (объекты тех или иных областей знания, дисциплин и так далее).

⁶ Таксон — группа в классификации, состоящая из дискретных объектов, объединяемых на основании общих свойств и признаков.

систематизации заведомо субъективный критерий — обречь её на неудачу. Кроме того, нарушение таких свойств информации не всегда понятно бизнесу (а именно он даёт деньги на обеспечение безопасности информации), он, бизнес, мыслит немного другими категориями, ему ближе рискованная модель. Действительно, если бизнесу сказать, что в результате компьютерной атаки будет реализована возможность несанкционированного доступа к базе данных АСУ управления движением поездов, он задаст вопрос: ну и что? А вот если бизнесу сказать, что в результате такой атаки 35 вагонов не будут поданы к погрузке, что приведёт к такому-то финансовому ущербу, то мозги у него повернутся в нужную сторону.

Мне кажется, что ФСТЭК России сейчас взял правильный вектор в этом направлении. Если посмотреть недавно утверждённый новый вариант Методики оценки угроз безопасности информации, то можно увидеть, что одной из основных задач при оценке угроз безопасности информации является определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации. Вот это уже близко к риск-ориентированной модели! Это как раз и может стать критерием классификации угроз, вернее, первой ступенью в иерархии систематизации угроз. И за основу можно взять те угрозы, которые приведены в методике:

- ◆ ущерб физическому лицу;
- ◆ ущерб юридическому лицу, связанный с хозяйственной деятельностью;
- ◆ ущерб государству в области обороны страны и безопасности;
- ◆ ущерб в социальной, экономической, политической, экологической сферах.

Кстати, если уж мы заговорили об ущербе. Ущерб — это всегда нарушение прав субъекта, то есть совершение какого-то правонарушения, а это уже категория юридическая. То есть в качестве признака первого таксона в классификации угроз безопасности информации можно использовать составы преступлений и правонарушений, приведённые в уголовном и административном кодексах. И, самое главное, такие составы правонарушений легко увязываются с полезными свойствами самой информации и исключают их смешение. Да и бизнесу они будут понятны (рис. 1).

Ну, это мы только первый таксон нашли. А дальше можно в качестве признака второго таксона использовать возможные типовые негативные последствия, приведённые в методике ФСТЭК России. Дальше — глубже. Здесь уже можно и на более «технократическом» языке говорить. Деление угроз (вернее, их возможных

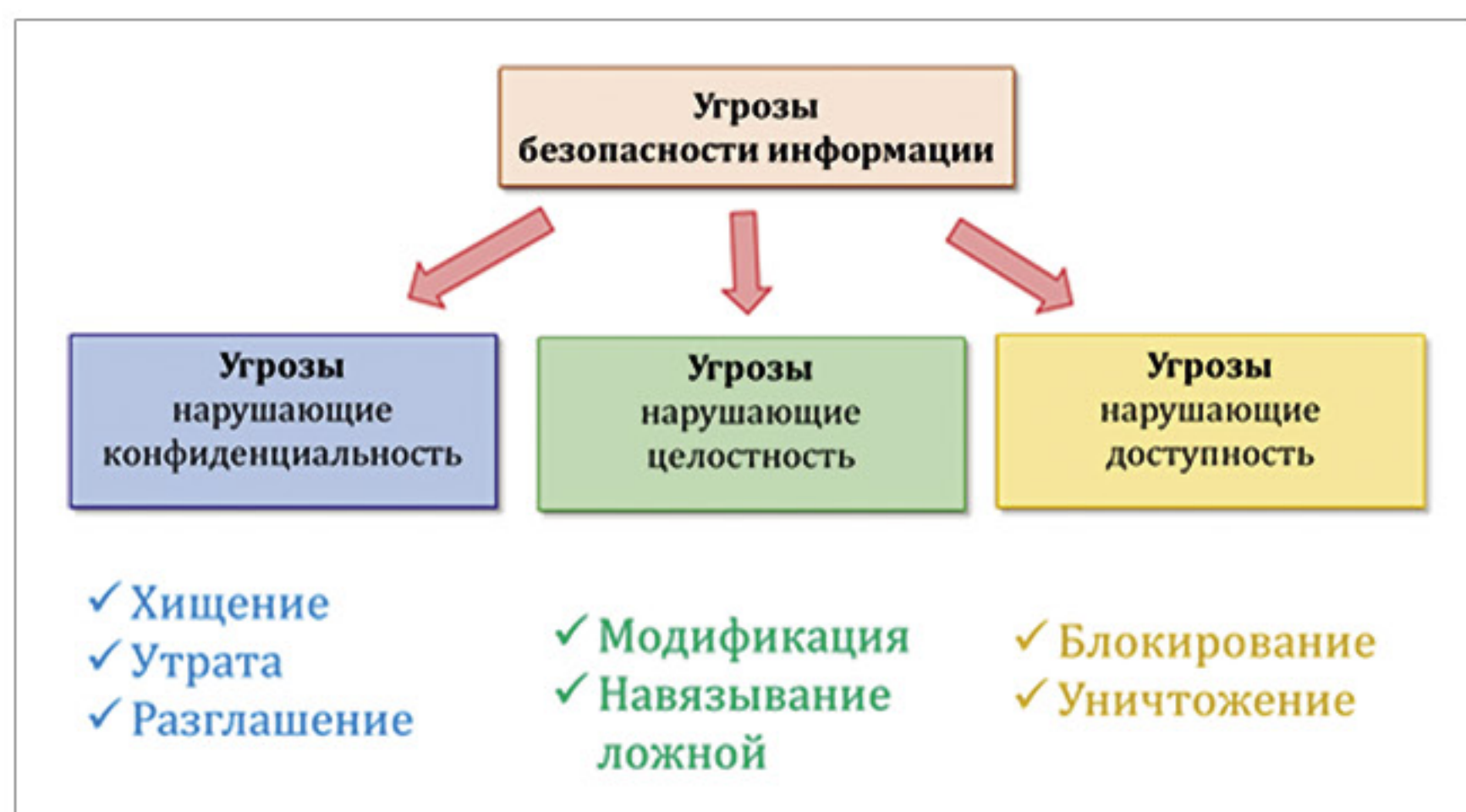


Рисунок 1. Примерный вариант классификации угроз безопасности информации на основе первого таксона

реализаций) по видам их воздействия на элементы инфраструктуры, которые могут привести к негативным последствиям. Здесь уже проглядывается прямая связь угроз и возможных уязвимостей. И так можно идти дальше. Главное, не зарыться слишком глубоко. Надо найти определённый баланс между глубиной описания угроз безопасности и возможностями банка угроз. Естественно предположить, что бизнес-процессы в разных организациях будут разные и последствия от их нарушений — тоже. Предусмотреть и рассчитать все последствия в общей модели невозможно. Да и не надо, это дело конкретных субъектов. Это как раз и должно делаться при составлении модели угроз на базе банка угроз. Вот и оставим эту часть им...

В завершение хотел бы вернуться к заглавной теме. Как бы мы хорошо ни построили банк угроз, как бы мы чётко ни сформули-

ровали критерии (признаки) таксонов, банк данных работать не будет, если не будет соответствия между самой угрозой и методами её устранения. Кстати, невооружённым глазом видно, что увязать угрозы с уязвимостями — задача реальная, а уж там недалеко и до методов устранения угроз. И ещё, не будем забывать, что угроза безопасности информации не зависит от степени важности (степени секретности) информации и определяется объективными факторами и уровнем развития науки и технологий. К объективным факторам, обуславливающим возможность (условия) реализации угроз, относятся структурно-функциональные характеристики информационной системы, а также нахождение относительно неё субъекта, совершающего противоправные действия. Поэтому в силу своей объективности условия реализации угрозы могут служить критерием выбора необходимых мер защиты.



Артём КАЛАШНИКОВ
эксперт BIS Journal

ГЛАВНОЕ — УЩЕРБ!

Статья, в общем, верная, хотя, конечно, фанатично углубляться в классификации не стоит, так как стремление описать вообще все существующие угрозы, их методы и источники неизбежно приведёт к путанице, а в условиях стремительных изменений в мире — так и к серьёзным упущениям. Я лично склоняюсь к описанной базовой модели классификации. Но в ней, на мой взгляд, не хватает одной составляющей. Она упоминается, даже с определением термина, но не присутствует, например, в подсчёте реализации. А ведь именно от неё зависит выбор параметров. Речь идёт об ущербе.

В подавляющем большинстве случаев атак, прежде чем их осуществить, злоумышленник соизмеряет предстоящие затраты с прибылью от успешной реализации атаки. Исходя из этого соотношения, он выбирает и цель, и метод, и инструмент. Это одна сторона этой составляющей. Другая — выбор инструментов защиты от атаки. Логично, что за ущерб в 200 руб. (условно) нет смысла возводить форты за 10 млн руб.

(условно). Но может быть и косвенный ущерб, который не всегда получается подсчитать.

В любом случае в разговоре с бизнесом в отношении обеспечения ИБ необходимо оперировать категориями ущерба, прежде всего цифрами. А классификация источников, угроз, методов — это лишь теоретическая основа для подсчётов. В таком контексте в расчётных формулах присутствие разных категорий ущерба необходимо.

Поясню почему. Например, атакующий получил доступ к процессингу организации. Вопрос: сколько он успеет вывести средств со счетов? Вот сколько успеет — это прямой ущерб, его можно показать в конкретных цифрах. Но после того как средства будут выведены, об этом может узнать общественность. Что, в свою очередь, приведёт к репутационным рискам. В какую цифру будет оценён ущерб от потери репутации?

Подобный пример применим и в отношении АСУ ТП. Тут методы и угрозы те же, хотя цели могут и отличаться. Но, так или иначе, раньше или позже эффект от успешной атаки будет монетизирован, а ущерб станет очевидным. Любым способом: прямые выплаты, падение или рост акций на бирже и т.д.

Вероятно, при таком подходе к классификации мы уйдём в N-мерные массивы, но от этого никуда не деться. Тем более что средства для обработки такого количества информации уже созданы и все возможные цепочки-комбинации вполне можно просчитать. И выбрать из них наиболее вероятные. А исходя из этого, уже определять комбинацию: источник — метод — ущерб. И соответственно, стратегию защиты.

BIS-КОММЕНТАРИЙ



Василий
ОКУЛЕССКИЙ
эксперт BIS Journal

ТУСКЛЫЙ БЛЕСК... «НАУКИ В ЖИЗНЬ»

ЖИВЁМ С ТЕМ НЕ ЗНАЕМ ЧЕМ...
ЗАЩИЩАЕМ ТО НЕ ЗНАЕМ ЧТО...

Не хочу доводить до логического завершения название статьи уважаемого и почитаемого мной С.В. Вихорева, а то получится, что эта самая БДУ подобна женщине с пониженной социальной ответственностью. Хотя сама статья очень даже ответственная и выводит на свет одну из фундаментальных проблем построения систем защиты информации. Таких проблем, конечно, множество. С одной стороны, это говорит о том, что информационная безопасность — живой, развивающийся организм, с другой — мы мастерски обманываем себя и других в вопросах о том, что, как и зачем надо делать. И подводим под этот обман почти научную базу.

Кстати, о научности тезисов. Аплодисменты автору — простая и всеобъемлющая формула

$$U = f(\{I \in S_I, F \in S_F, M \in S_M\}),$$

где: S_I — множество (совокупность) всех источников угроз, S_F — множество всех факторов, обуславливающих реализацию угрозы, S_M — множество всех методов реализации угрозы

прекрасно иллюстрирует принцип, по которому необходимо классифицировать те самые угрозы, и дедушка Карл Николиус Линней может подсказать принципы классификации на основе таксономии и таксонов.

Но, если уж мы заговорили об основах, давайте и начнём сначала: вспомним о предмете, который мы защищаем.

Итак, *информация* — результат и отражение в человеческом сознании, многообразие внутреннего и окружающего миров (сведения об окружающих человека предметах, явлениях, действиях других людей).

То есть предмет защиты находится у нас в голове? Тогда, может, это к психиатру? Или всё-таки во ФСТЭК?

Заглянем с другой стороны — в Энциклопедический словарь под редакцией А.М. Прохорова:

Информация (от латинского *informatio* — разъяснение, изложение) — с середины XX века общенаучное понятие, включающее обмен сведениями между людьми, человеком и автоматом,

автоматом и автоматом, обмен сигналами в животном и растительном мире, передачу признаков от клетки к клетке, от организма к организму.

Красиво! Но беда в том, что это определение натягивается только на все виды обмена «информацией» и совершенно игнорирует то, о чём говорит предыдущее определение. Мысль о монтаже в соответствии с этим определением становится информацией только в самый момент организации охоты на него при обмене мнениями о процессе охоты.

Идём дальше. Самый главный документ — Федеральный закон ФЗ-149 «Об информации, информационных технологиях и защите информации». Читаем там:

Информация — сведения (сообщения, данные) независимо от формы их представления.

Для практических задач, скорее всего, это определение подходит лучше предыдущих. Используя заложенный в нём подход, можно попробовать построить некоторую сильно упрощённую модель взаимоотношений в информационной сфере (рис. 1).

Тем не менее даже это определение не даёт исчерпывающего ответа на поставленный вопрос.

В итоге, раз ответа на вопрос о том, что же такое информация, нет, у каждого, прикоснувшегося к этой тематике, есть возможность внести свой вклад в науку. А как это можно делать, показал нам уважаемый автор, надо только определиться с таксонами.

Продолжим.

Так и не получив ответ на почти риторический вопрос, что такое информация, я попробовал посмотреть, а что же такое защита информации? Может, с этим вопросом больше порядка? Обратился к разным первоисточникам — стандартам, методическим рекомендациям и т.д. Нашёл 77 определений, связанных с понятиями «защита информации» и «безопасность информации», сбился со счёта и перестал искать...

Ближе к моим внутренним понятиям оказалось следующее определение:

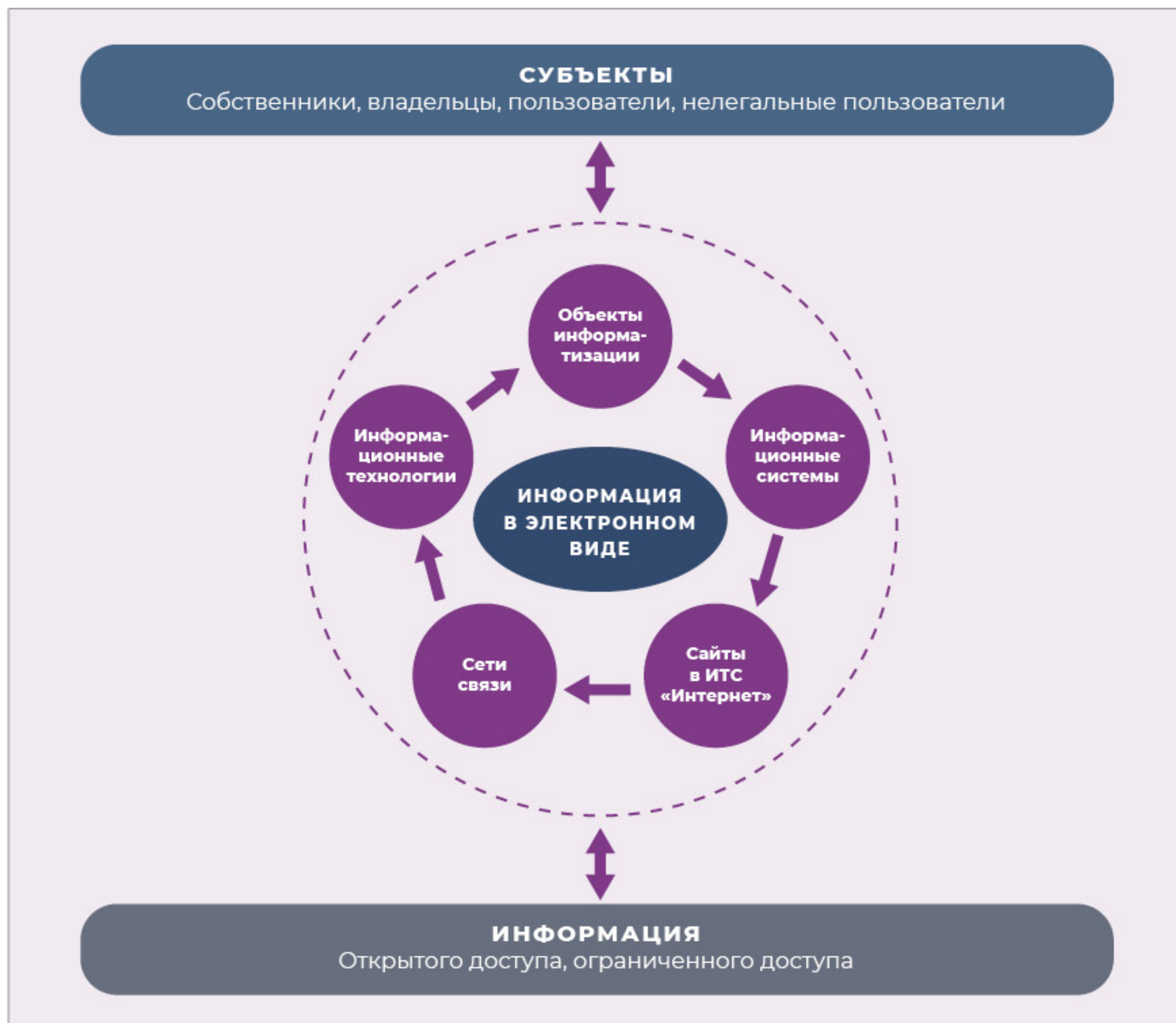


Рисунок 1. Информационная сфера

Информационная безопасность — это состояние защищённости информационных ресурсов Организации, выраженное в способности противостоять или противодействовать случайным или преднамеренным деструктивным воздействиям естественного или искусственного характера на нормальный процесс функционирования автоматизированных систем, способным нанести ущерб владельцам и пользователям информации и поддерживающей инфраструктуре.

Ключевой момент здесь в том, что мы не говорим о защите собственно информации, а говорим о защищённости информационных ресурсов. Попробуем уточнить это определение и вернёмся к нашей модельке.

И что мы видим? Мы защищаем информационные активы — информацию в электронном виде и средства её обработки, в том числе преобразования в тот вид, в котором она становится понятной субъектам этих отношений. А где уверенность в том, что собственно информация и есть то, что мы защищаем, а следовательно, рассматриваемые угрозы именно угрозы информации?

Замечательный пример с сейфом поднимает ещё одну проблему — связки безопасности физической и информационной. Следствие, на мой взгляд, красивое — не бывает информационной безопасности как таковой, её всегда надо увязывать с реальными процессами, тогда и ЗАЩИТА становится не информационной, а защита, в общем случае, бизнеса.

В таком контексте сочетание понятий уязвимости и угрозы, а ещё и меры защиты к ним, становится крайне запутанным и неопределённым.

Ну, и, наконец, вишенка на торт.

Допустим, я офицер безопасности и решаю вполне конкретную задачу — внедрение системы контроля доступа к базам данных. Вполне себе хорошая техническая мера, которая решает массу задач, в том числе контроля несанкционированного доступа к этим самым данным. У системы есть предельные технические возможности, граница которых определяется уровнем деградации основных процессов работы с базами данных. Как мне помогут все эти теоретические изыски в области защиты информации? Не знаю...



Юрий ЯРОВ
профессор
кафедры «Системы
информационной
безопасности»
Воронежского
государственного
технического
университета,
доктор технических
наук

НИЩЕТА... ЗНАНИЙ О БДУ

ОТВЕТ НА ЭССЕ С. В. ВИХОРЕВА

Статья Вихорева С. В. — одна из многих статей о банке данных угроз ФСТЭК России (далее БДУ), о котором сегодня пишут по разным поводам. Характерно то, что в этих публикациях часто путают назначение БДУ с назначением модели угроз безопасности информации. Чтобы разобраться в этом, давайте проведём небольшой экскурс в историю.

В конце 90-х годов прошлого века после появления первого терминологического стандарта (ГОСТ Р 50922–1996) и термина «защита информации» возникла задача описания тех «утечек информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию», упоминаемых в определении этого термина. В результате появилось понятие «угроза безопасности информации» как «совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации», закреплённое позже в ГОСТ 50922–2006 г. Однако приведённое определение оказалось настолько общим, что из него невозможно было определить, что за условия и факторы должны учитываться при описании угрозы. То, что их нужно описывать, чтобы знать, от чего защищаться, ни у кого не вызывало сомнения.

В самом начале 2000-х годов были развёрнуты широкие исследования (по заказам Гостехкомиссии России, Постоянного комитета Союзного государства и др.) по описанию угроз безопасности информации. Тогда и появилось понятие «модель угроз» как «физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации». Идея состояла в том, чтобы создать сначала некую модель, содержащую описание типовых угроз безопасности информации для некоторой совокупности информационных систем (например, для государственных информационных систем органов власти), которую называли базовой моделью угроз, а затем на её основе формировать модели угроз для конкретных информационных систем. И такие базовые модели предполагалось создать для определённых отраслей (энергетики, транспорта,

промышленности и т.д.) и для определённых видов и классов информационных систем в этих отраслях. Основное предназначение базовых моделей состояло в том, чтобы систематизировать сведения о возможных угрозах для информационных систем, дать единые представления о том, что должно содержать описание каждой угрозы, и исключить полный «разнобой» в таких описаниях, что наблюдалось тогда сплошь и рядом. Такие базовые модели позволяли по «единой схеме» формировать так называемые частные модели угроз, то есть модели угроз в конкретных информационных системах.

Вместе с тем попытки описать все известные угрозы в компьютерных системах в рамках базовых описательных моделей угроз заведомо были обречены на неудачу по двум причинам:

- ♦ во-первых, количество информационных систем и количество угроз в них оказалось настолько велико, что описать их на бумаге хоть с какой-то приемлемой для практики детальностью для всех информационных систем оказалось невозможным;

- ♦ во-вторых, динамика изменения состава и содержания угроз оказалась настолько велика (ежегодно возникала «лавина» новых угроз), что описывать их в бумажном варианте не имело практического смысла: они быстро устаревали.

Примечание: необходимо подчеркнуть, что речь идёт лишь только об описательных (вербальных) моделях угроз, а разрабатывались (и продолжают разрабатываться) также и аналитические, и имитационные, и логические, и графовые, и иные математические (формальные) модели угроз.

Естественно, возникла идея создания электронных описательных моделей угроз, то есть в виде электронной базы данных. Первая такая модель, в разработке которой принимали непосредственное участие как автор данной статьи, так и уважаемый С. В. Вихорев, была создана в 2006 г. Однако опыт практического применения этой электронной модели показал, что такие базы нужно вести, то есть постоянно обновлять по результатам публикаций, в том числе в сети Интернет, поскольку без обновлений они быстро становятся неактуальными, однако ни

средств, ни сил для отслеживания таких публикаций тогда не было. В результате в начале второго десятилетия была поставлена и начала решаться задача создания национального банка данных угроз безопасности информации, который был создан и функционирует с 2014 г.

В БДУ содержатся сведения об угрозах безопасности информации, уже реализованных хотя бы в одной из информационных систем или возможность реализации которых подтверждена, например, экспериментальными исследованиями. И эти сведения собираются в результате ежедневного сканирования всего интернет-пространства. После обработки собранных данных в банк записываются сведения об элементах описания угроз, таких как типы информационных систем, в которых, судя по публикациям, угроза реализована, возможные источники угрозы, эксплуатируемая уязвимость или уязвимости программного обеспечения информационных систем, эксплойты, разработанные для эксплуатации уязвимостей, способы реализации, объекты воздействия и несанкционированные (деструктивные) действия в ходе реализации угроз и др. Следует отметить, что сведения об уязвимостях и связанной с ними информацией (например, эксплойтах, сайтах, авторах, опубликовавших сведения и т.д.) хранятся в отдельной базе данных, что пока действительно вызывает определённые трудности с сопоставлением уязвимостей и угроз. Сегодня уже планируется существенная переработка БДУ, в том числе в интересах устранения указанного и других выявленных в ходе эксплуатации БДУ недостатков.

Вместе с тем нужно чётко уяснить, что БДУ — это ни в коем случае не описательные модели угроз для каких-либо информационных систем, что, на мой взгляд, в какой-то мере просматривается в суждениях уважаемого С. В. Вихорева.

Зачем же нужен такой банк данных угроз?

Во-первых, банк нужен при составлении частной модели угроз для каждой конкретной информационной системы, в которой описывается весь спектр актуальных угроз для этой системы. Каким же образом можно подтвердить актуальность угроз, описания которых включаются в частную модель угроз? Напомню, что угроза относится к актуальной, если имеется возможность её реализации в конкретной информационной системе и при такой реализации может быть нанесён значимый ущерб для её обладателя. Доказать актуальность можно путём:

- ♦ использования соответствующих математических моделей оценки рисков реализации угроз, если таковые модели разработаны для рассматриваемых угроз;

- ♦ экспертных оценок последствий реализации угроз с использованием новой Методики оценки угроз, утверждённой ФСТЭК России 5 февраля 2020 г.;

- ♦ применения метода аналогий, то есть сопоставлением состава и характеристик данной информационной системы (программного обеспечения, архитектуры, топологии системы, состава применяемых средств защиты, настроек и др.) с составом и характеристиками систем, в которых в соответствии с БДУ такие угрозы уже были реализованы.

Во-вторых, БДУ нужен при изыскании способов и разработке мер и средств защиты от новых угроз, сведения о которых могут содержаться в публикациях и в этом случае собираются для БДУ.

В-третьих, БДУ нужен для прогнозирования возникновения новых угроз, реализуемых, например, путём эксплуатации так называемых уязвимостей нулевого дня, при использовании новых информационных технологий в информационных системах, а также для сбора и анализа трендов в динамике возникновения новых угроз, инцидентов безопасности, уязвимостей, эксплойтов и т.д.

В связи с изложенным вызывают недоумение сетования С. В. Вихорева по поводу того, что БДУ никак не связан с требованиями к мерам защиты. Правильно! Непосредственной связи нет и быть не может, ведь он предназначен для иного. Да, в документах ФСТЭК России написано, что «Требования к системе защиты информации информационной системы определяются в зависимости от... угроз безопасности информации» и далее «В качестве исходных данных для определения угроз безопасности информации должен использоваться банк данных угроз безопасности информации (bdu.fstec.ru)». Я уже писал об этом в статье, названной редактором почему-то «Вершина айсберга во тьме»¹, где отметил, что без модели угроз правильно выбрать адекватные меры защиты не удастся. Это подчёркивает необходимость разработки частной модели угроз для конкретной информационной системы, при этом при разработке такой модели необходимо использовать банк данных угроз (bdu.fstec.ru). Ну и где же здесь «провал»? Скорее в знаниях о том, что такое банк данных угроз?! В связи с этим отнюдь не случайно мнение уважаемого С. В. Вихорева о том, что «в существующем банке угроз, к сожалению, всё смешано в кучу: и угрозы, и их реализации». Странно, ведь описание способа реализации угрозы — это

¹ Ю. К. Язов. Вершина айсберга во тьме, BIS Journal № 1 (36) / 2020

элемент её описания, и здесь сложно что-то смешать. Здесь С. В. Вихорев имеет в виду другое: хорошо бы такие описания структурировать, возможно, по иной совокупности иных «таксонов». Против такого совершенствования никто не возражает, и это предусмотрено в разрабатываемой новой версии БДУ.

Теперь об использовании модели угроз при выборе мер защиты. Я имею в виду описательные модели угроз, о математических моделях чуть позже. Сегодня при выборе мер защиты в конкретной информационной системе (а это значит, что используется частная модель угроз) применяют только экспертные процедуры, при этом сначала определяется вся совокупность актуальных угроз, которые могут иметь место в информационной системе. Затем в зависимости от класса защиты информационной системы определяется базовый состав мер защиты, которые должны быть применены для парирования этих угроз. Далее проводится:

- ♦ адаптация базового набора мер защиты информации применительно к структурно-функциональным характеристикам информационной системы, информационным технологиям, особенностям функционирования информационной системы и т.д.;

- ♦ уточнение адаптированного базового набора мер защиты информации в интересах обеспечения «блокирования (нейтрализации) всех актуальных угроз безопасности информации, включённых в модель угроз безопасности информации»;

- ♦ дополнение уточнённого адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами.

Так что утверждение о том, что при выборе мер защиты угрозы безопасности информации оказываются ни при чём, оказывается в корне неверным.

Спрашивается, а как же в этом случае быть с самими требованиями по защите? Очень просто: требования сегодня формируются в виде перечня мер, которые должны быть применены в информационной системе в зависимости от её класса защиты, который заранее определяется в соответствии с установленными в документах правилами. Правильно ли это? Сегодня, несомненно, да, поскольку иное преимущественно связано с применением количественных или иных формальных методов обоснования требований и, значит, с применением математических (формальных) моделей, к чему «общество защитников информации» пока не готово.

Конечно, с применением математических (формальных) моделей обоснование требований и выбор нужных мер защиты были бы значительно более глубокими, с оценкой достигаемой эффективности защиты информации, с решением задач оптимизации построения системы защиты в каждой информационной системе и др. Попытки именно так решать вопрос построения систем защиты неоднократно предпринимались как в России, так и за рубежом. Были разработаны весьма многочисленные модели и методики оценки эффективности защиты информации, основанные на теории риска. Однако их применение сдерживается многими факторами, такими как:

- ♦ «проклятие размерности» множества угроз и быстрое изменение их состава и характеристик, что приводит к сложности формирования и поддержания нужного состава моделей и методик для организации и ведения защиты информации;

- ♦ сложность и даже отсутствие подходов к обоснованию требуемой эффективности защиты информации в разных классах информационных систем, отсутствие практических или экспериментальных наработок для такого обоснования;

- ♦ большие трудности, возникающие с оценкой рисков реализации угроз безопасности информации в информационных системах. Напомню, что риск — это сочетание показателя возможности (как правило, вероятности) реализации угрозы и ущерба, который может быть нанесён в результате такой реализации. Если для оценки возможности реализации угроз разработаны разнообразные модели и методики, учитывающие не только характеристики самих угроз, но и принимаемые меры защиты, фактор времени и т.д., то для оценки возможных ущербов преимущественно применяются балльные методы, в основе которых лежит аппарат нечётких множеств. При этом оказывается весьма сложно учесть влияние на размеры возможного ущерба состава и характеристик мер защиты.

Конечно, было бы здорово научиться оценивать влияние нарушений безопасности информации в системах управления движением поездов на количество не поданных под загрузку вагонов и затем пересчитать всё это на финансовые убытки. Но ведь ущерб может быть финансовым, материальным (который не всегда пересчитывается в финансовый), экологическим, ущербом здоровью людей, моральным, в том числе репутационным, и т.д. Как их оценивать и тем более суммировать? В оценке рисков

реализации угроз пока значительно больше проблем, чем успешных решений.

Да! В новой методике оценки угроз сделан шаг вперёд, но до решения проблемы в целом весьма далеко. Достаточно отметить несколько вопросов, практически не раскрытых в методике: как оценивать влияние мер защиты на возможности и последствия реализации угроз, как учитывать временной фактор, оказывающий существенное влияние на оценку возможностей и развитие последствий реализации угроз и т.д. Всё это «в автомате» приводит к необходимости применения пока только экспертных оценок, и всё возвращается «на круги своя».

Тем не менее предложенное систематизированное представление о том, как оценивать угрозы, — это несомненное продвижение в нужном направлении, а с внедрением количественных методов при сохранении предложенной структуры действий может привести к методологическому прорыву. А вот общие рассуждения (без конкретных предложений) о том, как бы хорошо было иметь ясные количественные показатели риска реализации угроз, как бы полезно было использовать таксономию для полной классификации угроз (кстати, любая классификация основана на таксономии), как бы хорошо было при классификации угроз в качестве таксона использовать юридическую оценку последствий и т.д. — это пока пустые рассуждения людей, далёких или отдаляющих себя от проблематики развития методологии оценки рисков реализации угроз безопасности информации.

Наконец, следует остановиться ещё на одном тезисе С.В. Вихорева: о понятии «угроза безопасности информации» и неправомерности понятия «угроза информации» (акцентирую: не «угроза безопасности информации»). Да, термин «угроза информации» иногда встречается в публикациях, но если вдуматься в содержание контекста, а не впадать в критический раж, то становится понятным, что чаще всего имеют в виду угрозы, направленные на информацию, то есть на нарушение таких её свойств, как конфиденциальность, целостность или доступность. Тогда указанный термин не вызывает сильного отторжения. Но всё-таки лучше, конечно, придерживаться установленных терминов и их определений. В этой связи хотелось отметить следующее.

По Вихореву, угрозы безопасности информации, направленные на выполнение одного и того же несанкционированного действия (например, копирования информации), относятся к одной и той же угрозе, при этом есть

Предложенное систематизированное представление о том, как оценивать угрозы, — это несомненное продвижение в нужном направлении

множество вариантов её реализации. Но при такой трактовке этого понятия получается, что одна и та же угроза имеет разные оценки возможности реализации и ущерба в зависимости от того, каков источник угрозы, способ её реализации, используемая при этом уязвимость, применяемый эксплойт и др. При этом уважаемый С.В. Вихорев почему-то умалчивает, как быть с объектом воздействия при реализации угрозы: если копируется разная информация или копируется разный (но перекрывающийся) набор файлов, то это разные угрозы? На мой взгляд, проще и понятнее считать, что, если угрозы отличаются друг от друга хотя бы одним элементом описания (источником, эксплуатируемой уязвимостью, способом реализации, объектом воздействия или, тем более, содержанием выполняемого несанкционированного действия или совокупности действий, например, копирования и затем уничтожения файла), то это разные угрозы, поскольку возможности и последствия их реализации различны.

* * *

Таким образом, в эссе С.В. Вихорева хоть и поднимаются важные и интересные вопросы, но по некоторым из них решения уже есть. Я далёк от утверждения, что БДУ совершен. Наоборот, в эксплуатируемой сегодня его версии очень много недостатков, устранение которых уже запланировано и даже анонсировано заместителем директора ФСТЭК России Лютиковым В.С. Предполагается значительно расширить содержание включаемой в БДУ информации, установить явную взаимосвязь описываемых угроз и эксплуатируемых при этом уязвимостей, более детально раскрыть способы реализации и варианты возможных последствий, если о них стало известно из публикаций и др. Возможно, в результате многие вопросы исчезнут. Однако нужно чётко понимать роль и место БДУ в организации и ведении защиты информации в отечественных информационных системах и не путать БДУ с моделями угроз. Надеюсь, что изложенное в данной статье поможет разобраться в этом.



Анатолий АКСАКОВ
председатель Комитета
Государственной думы РФ
по финансовому рынку

ЗАКОНОДАТЕЛИ ИДУТ В НОГУ СО ВРЕМЕНЕМ

ПРАВОВЫЕ НОВШЕСТВА
УСИЛИВАЮТ
ПРОТИВОДЕЙСТВИЕ
ЗЛОУМЫШЛЕННИКАМ
И КОНКУРЕНЦИЮ
НА ФИНАНСОВОМ РЫНКЕ

Развитие законодательства в сфере информационной безопасности финансового рынка охватывает деятельность всех субъектов отрасли: и банковских, и некредитных организаций. Законопроекты учитывают особенности их профиля, особенности угроз и рисков, а также мер, средств и инструментария обеспечения безопасности бизнес-процессов и клиентских сервисов.

СОВЕРШЕНСТВОВАНИЕ ФИНАНСОВОГО МОНИТОРИНГА

Продолжается усиление законодательного противодействия незаконному обогащению — отмыванию доходов, полученных преступным путём, и финансированию терроризма. Последние законодательные инициативы в этой сфере направлены на оптимизацию подходов к применению соответствующих мер кредитными и иными финансовыми организациями.

Федеральный закон от 13 июля 2020 года № 208-ФЗ «О внесении изменений в Федеральный закон «О противодействии

легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма» в целях совершенствования обязательного контроля» содержит следующие нормы.

Во-первых, уточняется перечень подлежащих обязательному контролю операций (сделок):

- ♦ исключает неактуальные виды операций: обмен между юридическими и физическими лицами банкнот одного достоинства на банкноты другого достоинства, перевод денежных средств за границу (из-за границы) на счёт (вклад),





открытый на анонимного владельца, переводы денежных средств, осуществляемые некредитными организациями по поручению клиента;

- ♦ уточняет, что обязательному контролю будут подлежать операции с наличными и (или) безналичными денежными средствами по сделкам с недвижимым имуществом на сумму свыше 3 млн рублей;

- ♦ в части операций, связанных с выполнением государственного оборонного заказа, снижается с 50 до 10 млн рублей пороговая сумма операций по второму и

последующему зачислению (списанию) денежных средств в рамках операций, связанных с осуществлением расчётов по государственному оборонному заказу;

- ♦ устанавливаются особенности подлежащих обязательному контролю операций (сделок) для организаций федеральной почтовой связи (почтовые переводы на сумму более 100 000 рублей), операторов связи (возврат аванса за услуги связи на сумму более 100 000 рублей), для операций по договору лизинга (операции по счёту на сумму более 600 000 рублей).

Во-вторых, для каждой конкретной организации, осуществляющей операции с денежными средствами или иным имуществом, определён исчерпывающий перечень подлежащих обязательному контролю операций (сделок), информация о совершении которых подлежит предоставлению в Росфинмониторинг.

ОБОСНОВАНИЕ ОТКАЗА В ОБСЛУЖИВАНИИ

30 января 2021 года вступил в силу Федеральный закон от 30 декабря 2020 года № 536-ФЗ «О внесении изменений в Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма».

Изменения следующим образом уточняют порядок применения кредитными организациями права на отказ в выполнении распоряжений клиентов в совершении операций:

- ♦ повышается уровень защиты интересов добросовестных клиентов финансовых организаций;
- ♦ устраняются недостатки, выявленные в национальной антиотмывочной системе по результатам четвёртого раунда взаимных оценок ФАТФ.

Основные новации таковы:

- ♦ закрепление обязанности организаций информировать клиентов о дате и причинах принятия решений об отказе в совершении операции, отказе в заключении договора банковского счёта (вклада), о расторжении договора банковского счёта (вклада);
- ♦ установление требования о том, что упомянутые решения принимаются руководителем финансовой организации или специально уполномоченным им лицом;
- ♦ введение нормы об информировании финансовыми организациями Росфинмониторинга о вынесенном судом решении об отмене принятых ими решений об отказе в совершении операции, отказе в заключении договора банковского счёта (вклада);
- ♦ закрепление для всех финансовых организаций базовой нормы об отказе в приёме клиента на обслуживание, если не проведена идентификация и не установлены сведения, предусмотренные 115-ФЗ.

ЗАМОРОЗКА ОСПАРИВАЕМЫХ ТРАНЗАКЦИЙ

Продолжается работа над законопроектами в сфере безопасности электронных финансовых сервисов. В отношении заморозки средств у получателя оспоренной финансовой транзакции закон позволяет оспаривать переводы только до зачисления средств на счёт получателя, а максимальный срок приостановки транзакции составляет пять дней.

Ассоциация банков «Россия» разработала поправки к закону о национальной платёжной системе, предусматривающие блокировку перевода средств с карты на 25 дней в случаях, когда клиент банка заподозрил получателя его денег в мошенничестве.

Чтобы реализовать это право, клиенту следует обратиться в банк с заявлением о подозрительном переводе не позднее следующего дня после его совершения. Получателю средств даётся пять дней на подтверждение транзакции. Если он за

это время не предоставит нужные документы, деньги будут возвращены отправителю средств, в противном случае — зачисляться на его счёт (если зачисление было приостановлено), но всё равно будут заблокированы на оставшийся срок.

Заморозка средств на этот срок нужна для того, чтобы плательщик, если он считает, что всё-таки стал жертвой мошенников, смог обратиться в суд. Для чего ему предлагается передавать персональные данные получателя.

Однако такие персональные данные являются банковской тайной. Поэтому Ассоциация предлагает предусмотреть в законе о национальной платёжной системе право получать информацию, составляющую банковскую тайну, для случаев, когда отправитель денежных средств оспаривает перевод. Аналогичное право арбитражного управляющего прописано в законе о банкротстве. По мнению экспертов, данный вопрос требует дополнительной юридической проработки.

Кроме того, имеются риски злоупотребления. Так, по мнению специалистов, например, человек может приобрести с рук какой-то товар и потребовать блокировку. В этом случае получатель средств не будет иметь никакой подтверждающей документации, а соответственно, автоматически станет злоумышленником.

Банк России считает, что данный законопроект требует серьёзной проработки. В настоящее время он находится на стадии согласования. Нужно дождаться окончательной редакции предлагаемого законопроекта на основе баланса интересов всех заинтересованных сторон.

ПРОВЕРКА СВЕДЕНИЙ О ВЛАДЕЛЬЦАХ SIM-KART

В настоящее время существуют мошеннические схемы, при которых злоумышленники без ведома владельца телефона меняют его сим-карту. После этого мошенники получают доступ к онлайн-банкингу, перехватывают SMS-сообщения и снимают средства со счетов законных владельцев. При этом сами владельцы далеко не сразу об этом догадываются, поскольку к ним не приходят SMS-сообщения о списании денег со счёта.

Госдума ещё 5 марта 2019 года в первом чтении приняла законопроект № 514780-7 «О внесении изменений в Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путём и финансированию терроризма» и иные законодательные акты Российской Федерации (о создании информационной системы проверки сведений об абоненте)».

Законопроект предусматривает создание единой информационной системы (ЕИС) проверки сведений об абоненте. С её помощью банки и другие финансовые организации смогут проверять сведения о владельцах сим-карт — физических лицах, индивидуальных предпринимателях и юридических лицах.

Законопроект позволит бороться с теми, кто получает услуги у финансовых организаций, используя сим-карты, полученные незаконным путём. Оператор связи будет обязан предоставить в том числе и информацию о замене SIM-карт.

И доступ к этой информации получают все без исключения банки, в случае если это касается их клиента.

Таким образом, банк сможет отследить, что номер принадлежит законному владельцу, а не злоумышленнику. Однако процесс согласования поправок ко второму чтению законопроекта оказался непростым и затянулся. Разошлись мнения заинтересованных сторон, в частности, по таким вопросам, как обязательность использования ЕИС и установление тарифов на услуги проверки сведений об абонентах.

Целый ряд замечаний, которые необходимо учесть, возник как у Правительства РФ, так и у Банка России. Есть основания полагать, что все замечания удастся проработать и законопроект будет принят в весеннюю сессию 2021 года.

ПРОТИВ ПОДМЕНЫ ТЕЛЕФОННЫХ НОМЕРОВ

Звонки с подменных банковских номеров — одна из распространённых схем мошенничества. Для того чтобы имитировать любые номера телефонов, мошенники пользуются сервисами подмены номеров, которые используют SIP-протокол интернет-телефонии. Это даёт возможность совершать звонки с браузера или мобильного телефона. У вызываемого абонента будет отображаться произвольный либо выбранный «заказчиком» номер.

Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации» № 429-ФЗ от 8 декабря 2020 года, разработанный совместно с Банком России, создал правовую основу технических и организационных мер противодействия мошенничеству с подменой абонентских номеров.

Законодательный акт затрагивает интересы многих организаций, в том числе телекоммуникационных. Поэтому он прошёл предварительное согласование в профильных ведомствах.

ВОЗРАСТАЕТ КОНКУРЕНТНОСТЬ СТРАХОВАНИЯ

Развитие законодательства не только обеспечивает противодействие новым атакам злоумышленников, но и создаёт правовую основу для совершенствования финансового рынка. Так, законопроект № 1056530–7 «О внесении изменений в отдельные законодательные акты Российской Федерации в части создания автоматизированной информационной системы страхования» нацелен на повышение эффективности оказания страховых услуг.

В настоящее время на российском страховом рынке одновременно функционируют несколько систем хранения информации по отдельным видам страхования, в отношении каждой из которых действуют свои правила. Основная проблема в нынешней организации информационных систем в сфере страхования — конфликт публичного и коммерческого интересов. Корпоративная закрытость — тормоз конкуренции, повышению эффективности страхования.

Главная цель законопроекта — устранить это препятствие, усилить конкуренцию на страховом рынке. Одним из необходимых условий достижения этой цели является информационная прозрачность и обеспечение ценовой

доступности страхования. Ключевое требование к созданию базы данных в сфере страхования — полнота и достоверность собираемой информации по всем видам страхования.

Появление централизованной системы хранения информации на страховом рынке с прямым участием Банка России делает такую систему более эффективной. Качество информации в ней будет выше за счёт доступа к государственным информационным системам, включая системы Банка России. Предполагается, что информация в системе будет храниться не менее 10 лет со дня прекращения действия договора страхования.

ТРАНЗИТ БУДЕТ ПЛАВНЫМ

Автоматизированная информационная система (АИС) страхования будет способствовать снижению стоимости страховых продуктов, в том числе полисов ОСАГО. Будет создан отдельный портал под патронажем государственного регулятора, на котором сосредоточат информацию о страховых продуктах всех российских страховых компаний, и эти продукты тут же можно будет приобрести.

Внедрение системы позволит минимизировать издержки как потребителей, так и страховщиков. Оператором АИС предлагается сделать юридическое лицо в форме акционерного общества, 100% акций которого будут принадлежать Банку России.

Предполагается также создание комитета пользователей, состоящего из представителей страхового сообщества. К компетенции этого органа предлагается отнести правила осуществления деятельности оператора автоматизированной информационной системы страхования, тарифов на его услуги.

Для последовательного и постепенного перехода к централизованной системе хранения информации предлагается, чтобы страховщики начали предоставлять оператору системы сведения об осуществлении страхования владельцев транспортных средств и жилых помещений по истечении 12 месяцев со дня вступления норм в силу. О страховании владельцев опасного объекта за причинение вреда в результате аварии и перевозчиков за причинение вреда жизни, здоровью, имуществу пассажиров — по истечении 18 месяцев. В отношении иных видов страхования сроки предоставления информации предлагается определить Банку России.

Законопроект предусматривает достаточно длительный процесс перехода от нескольких информационных систем к единой. В течение этого времени они будут работать параллельно, транзит пройдёт плавно.

* * *

Развитие правовой базы обеспечения информационной безопасности финансовой сферы позволяет решать актуальные проблемы. Оперативное и даже опережающее реагирование на возникновение новых угроз, устранение пробелов в правовых нормах и создание новых — необходимое условие успешного противодействия и технологическим инцидентам, и злоумышленникам.

Создание и развитие киберполигона — одно из ключевых мероприятий федерального проекта «Информационная безопасность», которое поможет повысить уровень защищённости предприятий банковской сферы, энергетики, транспорта, связи и др. Учебные тренировки персонала этих компаний будут максимально приближены к реальным боевым условиям. Сотрудники, прошедшие обучение, приобретут новые профессиональные навыки и в дальнейшем смогут эффективно реагировать на угрозы информационной безопасности.

Кроме того, такие навыки смогут получить студенты ДВФУ и «Сириуса», в которых открыты специализированные классы с доступом к инфраструктуре киберполигона.

Минцифры также работает над расширением возможностей обучения навыкам реагирования на угрозы информационной безопасности для студентов других учебных заведений.

Дмитрий Реуцкий,
врио директора Департамента информационной
безопасности Минцифры России

В РОССИИ СОЗДАЁТСЯ НАЦИОНАЛЬНЫЙ КИБЕРПОЛИГОН

О САМОМ МАСШТАБНОМ ПРОЕКТЕ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТРАНЫ

В рамках федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации» была поставлена задача по созданию киберполигона — инфраструктуры для тренировки и обучения специалистов в области ИБ. Актуальность его появления связана с необходимостью противодействия новым угрозам кибербезопасности, возникающим при стремительной цифровой трансформации различных ключевых отраслей экономики.

ПОЧЕМУ ЭТО ВАЖНО?

Когда мы говорим о преимуществах цифровой экономики, важно учитывать те риски, которые она несёт. Прежде всего, речь идёт об угрозах, позволяющих киберпреступникам похитить ценную информацию, нарушить функционирование критической информационной инфраструктуры и повлиять на привычную жизнь большого количества людей.

Так, современные киберпреступники способны получить контроль над автоматизированными системами управления технологическими процессами (АСУ ТП) и парализовать производство, получить доступ к банковским системам и похитить деньги клиентов. В зависимости от сферы это может привести к значительным финансовым потерям отдельной компании и даже риску техногенной катастрофы, если речь идёт о промышленных предприятиях.

ГОСУДАРСТВЕННЫЙ ПОДХОД К ПРОБЛЕМЕ

Чтобы успешно противодействовать компьютерным атакам, нужны не только современные средства защиты информации на конкретных предприятиях. Необходимо системное развитие отрасли информационной безопасности в целом.

Государство активно участвует в решении этой задачи. В частности, в последние несколько лет были созданы Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) и Национальный координационный центр по компьютерным инцидентам (НКЦКИ). В структуре Банка России появился Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ).

В 2017 году в России был принят федеральный закон «О безопасности критической информационной инфраструктуры». К субъектам КИИ законодатели отнесли государственные органы и госучреждения, а также компании, которые работают в ключевых сферах.

Это здравоохранение, наука, транспорт, связь, энергетика, финансы, топливно-энергетический комплекс, атомная энергетика, оборонная, ракетно-космическая, горнодобывающая, металлургическая и химическая промышленность. Таким образом, регуляторы установили ряд требований по информационной безопасности для важнейших отраслей и обеспечили обмен информацией о существующих уязвимостях и угрозах.



Другой важный аспект — эффективная подготовка специалистов в области информационной безопасности и повышение квалификации существующих. По мнению экспертов, в отрасли ощущается нехватка ИБ-специалистов с практическим опытом защиты от киберугроз. Но его можно получить, тренируясь в условиях, близких к реальным, и не рискуя действующей инфраструктурой предприятий. Необходимость проведения кибертренировок закреплена в нормативных актах, в частности в приказе ФСБ № 282 от 19 июня 2019 года.

КИБЕРПОЛИГОН: ЧТО ТАКОЕ И ЗАЧЕМ НУЖЕН

Киберполигон — это масштабная площадка для тренировок специалистов по информационной безопасности. Здесь моделируются бизнес-процессы и информационные инфраструктуры типовых организаций различных отраслей. Участники киберучений с помощью предоставленных инструментов отработывают навыки противодействия кибератакам.

У Национального киберполигона две задачи. Первая — это повышение уровня практической подготовки специалистов по информационной безопасности: от студентов профильных специальностей до квалифицированных кадров российских организаций. Вторая задача — проведение стресс-тестов и анализа безопасности российских IT-решений, используемых в комплексных проектах по обеспечению информационной безопасности: средств защиты, программного обеспечения и элементов информационных систем.

Основную инфраструктуру киберполигона создаёт ПАО «Ростелеком» с привлечением экспертизы сотрудников его дочерней компании «Ростелеком-Солар», национального провайдера технологий и сервисов кибербезопасности. Размер выделяемых из бюджета средств на создание киберполигона в 2019–2020 годах составил 364,55 млн рублей, в

2021–2024 годах планируется выделить ещё 600 млн рублей. Проект реализуется при софинансировании со стороны ПАО «Ростелеком».

КАК РАБОТАЕТ КИБЕРПОЛИГОН?

Киберполигон представляет собой большую сеть из множества сегментов, которые включают каналы связи, сетевые устройства, серверы, рабочие компьютеры, технологическое оборудование и другие специфические устройства, подключённые к этой сети. В зависимости от отрасли и задач учений используется тот или иной набор средств защиты информации. В процессе обучения инфраструктуру можно менять, исследовать, взламывать, восстанавливать и т.д., то есть взаимодействовать с ней как с настоящей.

В ходе тренировок участники совершенствуют навыки оценки защищённости инфраструктуры, отражают смоделированные компьютерные атаки, проводят расследование инцидентов информационной безопасности.

Эксперты заранее прописывают цепочки сценариев нештатных ситуаций. На киберполигоне возможно использование как типовых сценариев атак, так и модифицированных под нужды конкретного предприятия.

ЧТО УЖЕ СОЗДАНО И ПЛАНЫ НА БУДУЩЕЕ

Планы по развитию киберполигона определены Правительством РФ. В соответствии с ними уже созданы два отраслевых сегмента — банковский и индустриальный (энергетический комплекс).

В 2020 году на базе индустриального сегмента киберполигона были успешно проведены закрытые отраслевые учения для одного из федеральных органов исполнительной власти. В них участвовали семь команд, было задействовано около

тысячи виртуальных машин. На 2021 год уже запланирован ещё ряд масштабных киберучений.

В 2021–2024 годах Национальный киберполигон будет дополнен следующими сегментами:

- ♦ нефтегазовый комплекс, включая инфраструктуры добычи, транспортировки и хранения нефти и газа;
- ♦ транспортная сфера, прежде всего железнодорожный транспорт;
- ♦ отрасль связи;
- ♦ горнодобывающая промышленность, включая инфраструктуры добычи и производства.

Кроме того, планируется обеспечить кросс-отраслевое взаимодействие созданных инфраструктур сегментов киберполигона, чтобы можно было проводить межотраслевые учения.

В рамках проекта будет построено несколько опорных центров Национального киберполигона в различных регионах России. Один из первых создаётся на базе ДВФУ во Владивостоке. Здесь уже дважды провели тестовые киберучения для студентов вуза. Кроме того, создан опорный центр в Научно-технологическом университете «Сириус» в Сочи.

* * *

В итоге Национальный киберполигон станет самым масштабным проектом в данном сегменте информационной безопасности и позволит повысить уровень защищённости всех ключевых отраслей экономики страны.

BIS-КОММЕНТАРИЙ

КИБЕРПОЛИГОНЫ? ПОЖАЛУЙСТА!

НЕ НУЖНО ЖДАТЬ, КОГДА ГОСУДАРСТВО ИХ ПОСТРОИТ



Александр БОДРИК
эксперт BIS Journal

Британское правительство использует методологию управления портфелями и ценностью проектов OGC Gateway. Её смысл в том, чтобы выбирать верные проекты и реализовывать их верным образом (Right projects. Done right). Проект киберполигона от государства, несомненно, очень полезен для развития индустрии и человеческого капитала в кибербезопасности страны, но такой подход всё же несколько устарел. В современном распределённом мире с независимыми игроками (предприятия, вузы, органы власти и т.д.) идея централизованного киберполигона отстала от жизни ещё до начала её реализации (которая, кстати, займёт не один год).

Вместо киберполигона гораздо удобней и выгодней использовать, например, свежий Google kCTF <https://github.com/google/kctf>, который можно запустить за час и сразу начать тренировать специалистов — хоть у себя в дата-центре, хоть в облаке (Google Cloud). И это не единственный вариант.

Запуская свой полигон на общедоступной базе, специалисты по ИБ изучат Kubernetes — multi-cloud — «инфраструктуру для поддержки приложений будущего» и, не томясь в ожидании, пока государство что-то построит, смогут создавать свои сценарии учений, а также добавят релевантные для их организаций и случаев сценарии.

ОТ РЕДАКЦИИ

Любопытно, что именно тема Национального киберполигона — достаточно предметная, почти вещественная — оказалась идеальным примером двойственности социального мира. Государственный, масштабный, тяжёловесный проект и лёгкие, быстрые, летучие тесты и тренировки на общедоступной базе — две стороны одной монеты, готовой уйти в массовый отраслевой оборот. Понятно, что на обеих сторонах мы не увидим совершенной картины, как на изделиях Монетного двора:

царапины, вмятины, следы производственного брака — всё это придётся подчищать на ходу, в том числе и с помощью BIS Journal — тоже весьма эффективного полигона, только не кибер-, а дискуссионного. Но главное, эта новая монета, запущенная в оборот, призвана активизировать процессы профессионального обмена и роста, поднять ИБ как профессию на новый уровень, как в своё время массовое развитие спорта создало новую культуру тела и физического здоровья.

**Артём СЫЧЁВ**

первый заместитель директора
Департамента информационной
безопасности Банка России

В ПЕРЕКРЕСТЬЕ ПРИЦЕЛА «КИБЕРБРИГАДЫ»

ЗНАЧЕНИЕ ДЛЯ ФИНАНСОВОЙ ОТРАСЛИ
ОБЗОРА «ОСНОВНЫЕ ТИПЫ КОМПЬЮТЕРНЫХ АТАК
В КРЕДИТНО-ФИНАНСОВОЙ СФЕРЕ В 2019–2020 ГОДАХ»

ПРЕДУПРЕДИТЬ, ЧТОБЫ ВООРУЖИТЬ

— Артём Михайлович, периодическая публикация Банком России объёмного, обстоятельного и популярного отраслевого обзора информационной безопасности — явление очень позитивное, но исключительное среди отраслевых государственных регуляторов. Причина в отличии финансовой сферы от других отраслей (промышленности, энергетики, культуры, образования и т.п.) или в позиции сотрудников и руководства ведомства?

— Позиция Банка России проста: финансовая отрасль должна быть предупреждена о возможностях посягательств, компьютерных атак на различные активы. Только тогда её участники могут должным образом подготовиться и вооружиться. Для государственного регулятора

публикация таких подробных обзоров и анализа рисков информационной безопасности — необходимый инструмент заблаговременного оповещения организаций об актуальных угрозах.

ТРАНСФОРМАЦИИ ЛАНДШАФТА

— Получает ли Банк России отклики на обзоры не только от профессионалов отрасли, но и из других отраслей, обучающих организаций, граждан?

— В информационном взаимодействии с ФинЦЕРТом Банка России принимают участие организации и специалисты не только финансовой сферы. Такая совместная работа полезна и другим отраслям, в первую очередь операторам телекоммуникаций и энергетике.



— Что побудило к созданию нынешнего формата обзора, какие объективные и субъективные причины?

— Формат был выбран в результате анализа данных за последний отчётный годовой период. Мониторинг и анализ ведутся постоянно, итоги подводятся регулярно. Особенности этого отчёта определены особенностями минувшего года — эпидемией коронавируса, значительным ростом объёмов дистанционных услуг, усилением и изменением характера активности злоумышленников.

В отчёт пришлось включить данные за весь нештатный период, что расширило его временные границы. Благодаря этому удалось получить полную и целостную картину изменения характера ландшафта кибербезопасности и киберустойчивости за последние два года. В этом контексте лучше и подробнее проявились особенности, присущие финансовой отрасли.

ОСОБЕННОСТИ ПАНДЕМИИ

— В какой степени модель рисков Банка России предполагала информационные угрозы 2020 года, возникшие в связи с ростом дистанционных финансовых услуг из-за «коронавирусных» ограничительных мер?

— В обзоре подробно изложены особенности, проявившиеся в результате ограничительных мер. Вынужденный перевод финансовых услуг преимущественно в дистанционный режим подтолкнул злоумышленников значительно изменить

В отчёт пришлось включить данные за весь нештатный период, что расширило его временные границы. Благодаря этому удалось получить полную и целостную картину изменения характера ландшафта кибербезопасности и киберустойчивости за последние два года

параметры своей активности. В частности, выстраивать мошеннические схемы по образу компенсационных мер, предлагавшихся государством гражданам.

Важно, что финансовые организации довольно легко перешли в расширенный режим оказания дистанционных услуг. Большинство из них были хорошо подготовлены к такому переходу: пришлось только увеличить мощности. Довольно быстро эта задача была решена вместе с обеспечением безопасности расширенных дистанционных сервисов.

— Какие «заготовки» в области обеспечения информационной безопасности сработали и что и как пришлось дорабатывать?

— В успешном увеличении объёмов дистанционной работы, внутрикорпоративной и с пользователями, положительную роль сыграла высокая степень подготовленности большинства финансовых организаций. Остальным пришлось срочно предпринимать ряд усилий, вносить изменения в

информационную инфраструктуру, включая обеспечение безопасности. Интеграция новых элементов не проводилась на пустом месте, а опиралась на существующие решения, допускавшие подобные модификации.

МАЯТНИК ВОЗВРАЩАЕТСЯ

— Каковы главные выводы по итогам 2020 года, какие меры в результате намечены, что должно измениться в сфере регулирования информационной безопасности финансовой сферы?

— Основной вывод по итогам отчётного периода таков: маятник возвращается. Злоумышленники вновь ведут поиск уязвимостей в системах информационной безопасности финансовых организаций. Стремительный рост объёмов и разнообразия атак на клиентов начинает падать, поскольку на данном этапе удалось выстроить эффективную систему противодействия нынешнему инструментарию.

Граждане, клиенты финансовых организаций, стали более информированными и бдительными, научились быть начеку и распознавать многие уловки злоумышленников. Результативность, выгодность социальной инженерии стала заметно снижаться. Направление атак начинает возвращаться к поиску лазеек в программном обеспечении, других технических средствах дистанционных сервисов.

Учитывая эту тенденцию, организации финансовой отрасли и Банк России как государственный регулятор нацеливаются на опережающее противодействие таким атакам. Могут применяться новые методы, ранее в России не использовавшиеся. Для этого потребуются не только внесение изменений в нормативные документы, но и широкое обсуждение специалистами.

ДИНАМИКА УГРОЗ

— Какие ещё прогнозируются возможные информационные угрозы, пока не реализовавшиеся (отключение РФ от SWIFT, внешние ограничения на использование интернета, иностранные санкции против российского финансового сектора, отдельных организаций, персон и т.п.)?

— Некоторые из потенциальных проблем способны проявляться неожиданно, как показывает недавняя история с сервисом групповой видеосвязи Zoom, хозяева которого ввели ограничения для российских государственных организаций. Перечисленные трудности возможны, работа по снижению подобных рисков ведётся. Публичное обсуждение этих вопросов пока преждевременно.

— Как за отчётный период изменился «удельный вес» разных источников информационных угроз — с одной стороны, недружественных действий иностранных правительств, компаний и международных структур, с другой стороны — киберпреступности?

Международная политика не входит в сферу компетенций Банка России. Можно говорить о том, что наглядно и

Результативность, выгодность социальной инженерии стала заметно снижаться.

Направление атак начинает возвращаться к поиску лазеек в программном обеспечении, других технических средствах дистанционных сервисов

доказуемо: основные источники информационных атак на финансовую сферу России находятся за границей. Серверы, ресурсы для телефонных звонков, спама и фишинга за пределами нашей страны. Эта тенденция сохраняется.

ОТМЫЧКИ НА ПРОДАЖУ

— Насколько трансформация технологий информационных атак на финансовый сектор РФ показывает использование не кустарных, а «промышленных» технологий — «ноу-хау» крупнейших глобальных компаний и иностранных государственных разработок?

— За часть этих вопросов отвечает Совет Безопасности РФ. Мы на своём уровне видим точно только то, что есть группы злоумышленников, которые используют инструментарий атак, который можно отнести к промышленным решениям.

Это опять же не новость, ещё 3–4 года назад приводились примеры развития технологий информационных атак, используемых злоумышленниками. Можно выделить несколько стадий этой эволюции: от замысла до коммерческого распространения готового «решения» промышленного уровня.

Такие стадии эволюции различного криминального инструментария отслеживаются и сейчас. Быстрее всего до «промышленного» решения на продажу «дозревают» приёмы и уловки социальной инженерии. На основе таких «решений» можно создавать «кибербригады» злоумышленников.

Актуальным серьёзным вызовом являются вирусы программы-шифровальщики, которые пока не коснулись финансовой отрасли. Пока есть эффективный инструментарий выявления и противодействия, но этот вид атак быстро совершенствуется.

ОБУЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ

— В «Обзоре...» есть разделы по повышению культуры информационной безопасности финансов и для профессионалов отрасли, и для граждан. Как получилось, что выполнять образовательно-просветительные функции в этой сфере приходится Банку России?

— Повышение осведомлённости граждан в вопросах безопасности дистанционных финансовых сервисов — одна из задач, которую решает Банк России. Обучать граждан не только кибербезопасности и кибергигиене, но и основам финансовой грамотности, умению владеть финансовыми инструментами. Эта работа ведётся не в одиночку, а вместе с финансовыми организациями, наши совместные усилия дополняют друг друга. Общая задача решается на разных уровнях совместно многими участниками финансовой отрасли.



**Екатерина
РАЧКОВА**

эксперт BIS Journal,
заместитель
начальника
Управления
по обеспечению ИБ
Банка ВТБ (ПАО)

ПРОВЕРКА ПО 716-П. РАЗБЕРИТЕСЬ В СЕБЕ

ИЛИ КАК ОКАЗАТЬСЯ «НА КОНЕ», ЕСЛИ
КАЖЕТСЯ, ЧТО «КОНЬ НЕ ВАЛЯЛСЯ»?

Любая проверка, кем бы и с какой целью она ни проводилась — подразделением внутреннего контроля, внешним контрагентом-аудитором или регулятором, — это всегда возможность посмотреть на инфраструктуру организации под другим углом, обнаружить что-то, что не было заметно «изнутри», причём не всегда это будут только недоработки и несоответствия.

Объективная проверка, какой бы результат она ни показала, — это предупреждение. А предупреждён — значит вооружён. Гораздо лучше, если уязвимость (а по сути, невыполнение регуляторного требования — это слабость защиты, открывающая существующую или создающая новую уязвимость) обнаружит проверяющий, а не злоумышленник. Ну как регулятор накажет? Предписание со сроком устранения даст, штраф по статьям 13.12 и 19.5 КоАП Российской Федерации, возможно, выплатить придётся, но это ни в какое сравнение с ущербом от успешной атаки или мошенничества не идёт. Если вовремя выявили и успели устранить, или даже не успели, но повысили бдительность и стали зорче следить за «слабым местом» — можно считать, повезло.

Так, главным критерием успешности прохождения проверки становится её объективность. А объективность не любит ошибок ни первого, ни второго рода. Иными словами, если что-то делается согласно требованиям, то выявить и корректно оценить это не менее важно, чем то же самое в отношении проблем и несоответствий.

ЧТО ПРОВЕРЯЕМ

Соответствие Положению Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе» в части риска информационной безопасности (далее — ИБ).

ИДЁМ ОТ ОБЩЕГО К ЧАСТНОМУ

Деятельность по управлению рисками ИБ, как правило, строится в рамках установленной методологии управления операционным риском

с отражением необходимой специфики ИБ в отдельных нормативных актах. А с операционными рисками работа наверняка ведётся. Это значит, по умолчанию всё, что в организации регламентировано для операционных рисков, верно и для рисков ИБ. Если в каком-нибудь локальном нормативном акте организации в явном виде зафиксировано, что риск ИБ — вид операционного риска, ещё лучше.

ИЩЕМ СВИДЕТЕЛЬСТВА ПРИМЕНЕНИЯ РИСК- ОРИЕНТИРОВАННОГО ПОДХОДА В ПОВСЕДНЕВНОЙ ДЕЯТЕЛЬНОСТИ

Деятельность по управлению рисками ИБ подразумевает защиту информационных ресурсов и активов и связанных с их использованием бизнес-процессов, обеспечение способности организации производить продукт или предоставлять услугу, а также защиту активов, участвующих в обеспечении функционирования информационных технологий (вычислительных и телекоммуникационных активов, работников и пр.). Если проводится работа по выявлению новых угроз и уязвимостей ИБ (хотя бы регулярно проглядывается база угроз безопасности ФСТЭК России и рассылки Центрального Банка), анализ адекватности и эффективности применяемого комплекса мер защиты клиентов (хотя бы в рамках мозгового штурма в рамках agile-команды), оценивается соотношение возможных потерь в результате реализации какой-то угрозы и затрат на защиту (хотя бы качественная, не количественная экспертная оценка), это оно и есть. Идентификация рисков происходит, как правило, в результате SWOT-анализа, HAZOP-анализа, сценарного анализа, планирования непрерывности бизнеса, анализа бизнес-процессов, анализа результатов проверки и аудита ИБ, расследования событий и инцидентов защиты информации (далее — ЗИ).

А попытка подумать над вопросом руководства «а что у нас будет, если случится как у конкурента такого-то» — это хоть и примитивный, но сценарный анализ рисков. Если свидетельства проработки этих вопросов письменные — отлично, переписка в электронной

почте — хорошо. На худой конец и интервью — источник свидетельств проверки. Но в любом случае это означает, что в организации есть практика управления рисками ИБ, которая, возможно, нуждается в большей формализации и систематизации.

КОРОТКИЙ ЧЕК-ЛИСТ ДЕЯТЕЛЬНОСТИ В РАМКАХ УПРАВЛЕНИЯ РИСКОМ ИБ

♦ Установление политики в отношении управления рисками ИБ: за счёт методологии управления операционным риском.

♦ Выявление и идентификация рисков ИБ, оценка остаточных рисков ИБ: даже если этими словами не называется, явно проводится, когда планируется внедрение той или иной защитной меры/средства. Мы же всегда хотим знать, полностью ли проблема решится, если мы что-то там внедрим. Это «полностью ли?» и есть оценка остаточных рисков.

♦ Планирование системы мер, направленных на снижение рисков ИБ: все применяемые меры — это защита от чего-то, в основном того, что ещё не случилось, но может, а не хотелось бы.

♦ Реагирование на риски и инциденты ИБ, в том числе формирование и поддержание в актуальном состоянии комплекса мер и средств защиты в соответствии с принятой политикой обеспечения ЗИ: собственно наличие мер и средств защиты — это и есть реакция на риски. В случае если просто выполняется базовый набор требований регулятора, например, ГОСТ Р 57580.1–2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер», подразумевается, что какие-то типовые риски за организацию уже оценил регулятор.

♦ Мониторинг и выявление событий риска ИБ: вспоминаем, например, отчётную форму 0403203 по Положению Банка России от 09.06.2012 № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».

♦ Обеспечение ситуационной осведомлённости подразделений и лиц, задействованных в процессах управления рисками ИБ: предупреждения и рассылки о вредоносных письмах, мошеннических действиях, атаках на другие организации — всё годится.

♦ Мониторинг рисков ИБ и анализ соответствия фактических значений контрольных

показателей уровня риска ИБ принятым значениям: даже если не установлен официально риск-аппетит организации, неформально градация допустимые/недопустимые потери, «N таких инцидентов в месяц — это уже много» наверняка применяется.

ИЩЕМ ПРИМЕРЫ ПРИМЕНЕНИЯ РАЗЛИЧНЫХ СПОСОБОВ ОБРАБОТКИ РИСКА ИБ

Короткий чек-лист вариантов обработки рисков ИБ (реагирования):

♦ принятие мер минимизации: меры ЗИ, направленные на уменьшение негативного влияния риска ИБ на качество процессов, величину потерь;

♦ сознательное и объективное принятие рисков ИБ с одновременной подготовкой ресурсов для покрытия ущерба, который может быть понесён в результате реализации принятых рисков: предполагает готовность принять возможные потери в рамках установленного лимита потерь с процедурой контроля соблюдения лимита;

♦ уклонение от риска ИБ (избежание): отказ от информационной технологии (средства обработки информации), от предоставления соответствующих продуктов и услуг в связи с высоким уровнем риска ИБ; используется, если реализация мер по минимизации риска ИБ не является экономически обоснованной;

♦ передача риска ИБ: страхование рисков ИБ, передача риска другой стороне — контрагенту и/или клиенту; используется в случае невозможности или нецелесообразности самостоятельного управления риском ИБ самой организацией.

ВЫДЕЛЯЕМ ДРУГИХ УЧАСТНИКОВ ПРОЦЕССА УПРАВЛЕНИЯ РИСКАМИ ИБ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Анализ и оценка рисков ИБ в отношении отдельных объектов защиты может выполняться только совместно всеми заинтересованными подразделениями. В число указанных подразделений входят:

- ♦ подразделение ИБ;
- ♦ подразделение, осуществлявшее (самостоятельно или с привлечением сторонних организаций) автоматизацию процесса и(или) внедрение соответствующего объекта защиты (далее — подразделение ИТ);
- ♦ подразделение, являющееся заказчиком и (или) владельцем соответствующих объектов защиты ресурсов (далее — подразделение заказчик/владелец);



♦ подразделение-пользователь, эксплуатирующее объект защиты (если отличается от перечисленных выше).

Подразделение ИТ формирует описание объекта защиты, процессов его автоматизации и реализуемых им технологических процессов. На основании этих данных подразделение ИБ с учётом результатов мониторинга и контроля ИБ идентифицирует уязвимости ИБ объекта защиты и возможные сценарии их использования (угрозы ИБ объекта защиты), после чего делает предположение о вероятности реализации идентифицированных угроз ИБ на основании статистических данных мониторинга событий и инцидентов ИБ Банка, а также имеющейся информации о подобных фактах в других организациях финансовой сферы. Далее подразделения — заказчик/владелец и пользователь объекта оценивают объём потенциального ущерба от реализации идентифицированных угроз ИБ в отношении объекта. Подразделениями ИТ

и (или) ИБ вырабатываются и согласуются с другими участниками процесса меры противодействия идентифицированным угрозам ИБ, и уполномоченный коллегиальный орган принимает решение о способе обработки риска ИБ, включая его принятие. Скорее всего, у каждого подразделения какие-то свидетельства выполнения соответствующих шагов найдутся.

...И ТАКИМ ОБРАЗОМ «НАТЯГИВАЕМ» СЕБЕ ОЦЕНКУ?

Нет. Ну, то есть, конечно, любое знание можно использовать как на благо, так и во вред, но приведённые выше советы рассчитаны не на получение оценки, а на обеспечение её объективности, на понимание сложившейся практики, зарождающегося процесса для наиболее эффективного его развития и надстройки, а не развёртывания некоего теоретического эталона в отрыве от ландшафта и специфики организации.

С ТОЧКИ ЗРЕНИЯ SWIFT

ЧТО ФИНАНСОВЫМ УЧРЕЖДЕНИЯМ
СТОИТ СДЕЛАТЬ ДЛЯ УСИЛЕНИЯ
КИБЕРЗАЩИТЫ В 2021 ГОДУ



**Екатерина
КАЛИНИНА**
директор по России
и СНГ, SWIFT

Помогая клиентам вернуть большую часть средств, подвергшихся атакам мошенников, наша программа безопасности пользователей CSP продолжает приносить важные результаты. Но это только начало. Помимо аттестации и проведения независимой оценки, клиентам предстоит сделать ещё многое для поддержания безопасности своих систем в 2021 году.

АТТЕСТАЦИЯ CSCF

К концу прошлого года 89% наших клиентов, которые представляют более 99% трафика SWIFT, прошли аттестацию на соблюдение обязательных элементов контроля, предусмотренных Концепцией обеспечения безопасности пользователей (CSCF). Данная концепция — ключевой элемент CSP.

Мы благодарим наше сообщество, а именно более 11 000 учреждений, за внедрение элементов контроля, предусмотренных концепцией CSCF в 2019 году. 89% аттестованных участников — прекрасное достижение, особенно в таком непростом контексте. В условиях пандемии COVID-19 многим учреждениям пришлось уделить основное внимание непрерывности бизнеса и в некоторых случаях даже заморозить другие процессы.

CSCF как основа киберзащиты сообщества SWIFT выделяет обязательные и рекомендательные элементы контроля, которые клиенты могут внедрить в локальной среде для предотвращения существующих и новых киберугроз. С момента своего запуска в 2017 году концепция стремится постоянно повышать планку безопасности для всего сообщества SWIFT.

И это работает.

Нас впечатлило, как в последние четыре года нашему сообществу удавалось поддерживать устойчивость перед лицом растущих и развивающихся киберугроз с помощью нашей программы безопасности пользователей CSP. Однако угроза кибератак никуда не уходит, и

мы продолжаем работать с клиентами над укреплением их киберзащиты с помощью версии концепции CSCF 2021 года и независимых оценок.

CSP В МЕЖДУНАРОДНОМ КОНТЕКСТЕ

Как SWIFT объединяет усилия с другими крупными инфраструктурами в Европе для борьбы с киберугрозой

SWIFT как участник рабочей группы Европейского совета по кибербезопасности для панъевропейских финансовых инфраструктур (ECRB), созданного Европейским центральным банком, был ключевым игроком в запуске инициативы, согласно которой крупные европейские инфраструктуры должны делиться значимой информацией о киберугрозе. Её цель — помочь защитить европейских граждан и финансовые учреждения от кибермошенников.

Сегодня угроза, которую кибератаки представляют для финансового сектора, велика как никогда. Злоумышленники обладают всеми необходимыми ресурсами, постоянно совершенствуют свои методы и соревнуются друг с другом в использовании новых технологий вроде искусственного интеллекта и машинного обучения.

В настоящее время организации финансового сектора находятся на разном уровне зрелости в плане использования аналитических данных. Они фрагментированы с точки зрения того, какими сервисами, технологиями и продуктами пользуются, и, как правило, между ними отсутствует какой-либо систематический обмен данными.

Чтобы решить эту проблему, Европейский совет по кибербезопасности для панъевропейских финансовых инфраструктур создал рабочую группу для обмена информацией. Основные цели программы, известной как Инициатива по обмену киберинформацией и аналитическими данными (CIISI-EU), следующие:

1. Предотвращать, обнаруживать, реагировать и повышать осведомлённость членов ECRB об угрозах в сфере кибербезопасности.

2. Организовывать обмен актуальной и действенной аналитической информацией между членами ECRB и правоохранительными органами с возможностью её распространения на более широкую экосистему.

3. Поощрять активное участие членов «доверенного круга» вместо пассивного потребления или малоэффективного использования информации.

4. Обрабатывать и систематизировать полученную информацию. Активно поощрять обмен стратегической аналитической информацией в дополнение к тактике, методам и процедурам оперативного характера, а также тактическим свидетельствам нарушения нормального функционирования систем безопасности.

5. Обеспечить постоянное обучение и развитие во всём, что касается процесса анализа, разработки и обмена информацией об угрозах кибербезопасности.

В ECRB входят крупнейшие и наиболее важные рыночные инфраструктуры ЕС. Это центральные банки, клиринговые палаты, фондовые биржи, поставщики платёжных услуг, правоохранительные органы и многие другие.

Киберпреступники всегда делятся друг с другом методами работы, тактикой и аналитикой, и, возможно, нам в нашей экосистеме стоило бы взять это для себя на заметку.

Исследования показывают, что обмен актуальной и своевременной информацией об угрозах является критически важным фактором, который помогает эффективно обнаруживать и предотвращать кибератаки. Вот почему мы решили создать структуру, которая позволяет упростить процесс обмена аналитическими данными с помощью повторного использования проверенных элементов, распространения стратегической информации и предоставления каждому участнику возможности провести эту работу в комфортные для него сроки. Мы надеемся, что это облегчит жизнь тем, кто обеспечивает защиту потребителей и участников финансового рынка от киберпреступников.

Впервые в истории крупные финансовые инфраструктуры, Европол и Агентство Европейского союза по кибербезопасности (ENISA) предпринимают совместные шаги по борьбе с киберугрозами. Мы надеемся, что это сотрудничество вдохновит другие юрисдикции на борьбу с одной из самых опасных угроз нашего времени. Обмен информацией — это

перспективный способ предотвращения мошенничества и в конечном счёте защиты средств граждан.

СОВМЕСТНОЕ РАССЛЕДОВАНИЕ

Как преступники обналичивают средства, полученные в результате масштабных кибератак

В рамках реализации CSP в прошлом году SWIFT совместно с BAE Systems провёл исследование процесса отмыwania денег. По его итогам был выпущен совместный отчёт «По следам денег» (Follow the Money), в котором описывается сложная схема преступников по использованию «денежных мулов», подставных компаний и криптовалют для обналичивания средств, полученных в результате кибератаки.

В отчёте подчёркивается изощрённость схем отмыwania денег для получения наличных и предотвращения любого последующего отслеживания средств. Например, киберпреступники часто размещают привлекательные объявления о приёме на работу и вербуют ничего не подозревающих соискателей в качестве «денежных мулов». А также используют инсайдеров в финансовых учреждениях, чтобы избежать комплаенс-контроля, процедур «Знай своего клиента» (KYC) и проверок при открытии новых счетов. Кроме того, они конвертируют украденные средства в имущественные активы и ювелирные изделия, которые не теряют своей ценности и не привлекают внимание правоохранительных органов.

Методы, используемые преступниками при осуществлении кибератак, достаточно хорошо изучены, в отличие от того, что происходит с деньгами после кражи. Цель отчёта — осветить способы «обналичивания» украденных средств, используемые киберпреступниками, чтобы глобальное сообщество SWIFT, состоящее из более чем 11 000 финансовых организаций, рыночных инфраструктур и корпораций, могло лучше себя защитить.

Другие выводы отчёта:

◆ Подставные компании — киберпреступники, как правило, для сокрытия средств используют предприятия текстильной, швейной и рыбной промышленности. Они предпочитают работать в определённых странах Восточной Азии с менее строгим законодательством.

◆ Криптовалюты — хотя количество выявленных случаев отмыwania денег с помощью криптовалют пока невелико, произошла пара серьёзных инцидентов, связанных с суммами в миллионы долларов. Цифровые транзакции привлекательны, потому что они позволяют избежать комплаенс-контроля и процедуры KYC,

проводимых банками, и часто требуют только адреса электронной почты.

♦ Опыт — метод, выбранный киберпреступниками для обналичивания и расходования украденных средств, свидетельствует об их уровне профессионализма и опыта. Неопытные преступники часто сразу же совершают экстравагантные покупки, привлекающие внимание правоохранительных органов и приводящие к арестам.

Сегодня угроза, которую кибератаки представляют для финансового сектора, велика как никогда. В отчёте подчёркивается, что рост количества кибератак увеличивает потребность в объединении усилий для борьбы с отмыванием денег и мошенничеством, а также для обеспечения кибербезопасности в финансовых учреждениях. Отчёт призывает участников финансового сектора расширить обмен информацией, ужесточить требования о проявлении должной осмотрительности и разумно инвестировать в создание систем для усиления собственной защиты.

ПО РЕКОМЕНДАЦИИ SWIFT

Что клиентам стоит сделать в 2021 году для поддержания своей безопасности

Использование таких инструментов, как обязательные элементы контроля, обмен аналитическими данными и экспертиза, позволяет CSP непрерывно помогать финансовому сообществу укреплять свою безопасность. CSCF 2021 года включает ряд дополнительных требований, 22 обязательных и 9 рекомендательных элементов контроля, по которым каждому клиенту нужно пройти аттестацию. О них было объявлено в 2020 году со сроком исполнения в конце 2021 года.

Два элемента контроля, 1.3 и 2.10, заявленные как рекомендательные в 2019 году, в CSCF 2020 года уже переведены в разряд обязательных. В CSCF 2021 года обязательным стал прежде дополнительный элемент контроля 1.4. Эти дополнения призваны обеспечить защиту и уменьшить потенциальную уязвимость критических компонентов интерфейса, а также критических систем, в которых более часто используется виртуализация.

Аттестация по версии CSCF 2021 года в KYC-SA, онлайн-хранилище данных об аттестации клиентов, станет доступной с июля 2021 года.

Все элементы контроля CSP соответствуют высшим отраслевым стандартам, включая Стандарт безопасности данных индустрии платёжных карт (PCI DSS), рамочные требования Национального института стандартов и технологий (NIST) и модель ISO/IEC 27001. Следуя общим принципам,

организации-участники CSP смогут повысить эффективность, снизить затраты и обеспечить надёжность своей инфраструктуры.

НОВОЕ В 2021 ГОДУ

Требуется независимая оценка

Для повышения целостности и надёжности информации об аттестациях пользователей все аттестации в соответствии с требованиями CSCF 2021 года должны быть подтверждены независимой оценкой.

Для проведения независимой оценки могут быть задействованы как внутренние, так и внешние ресурсы. Она также может проводиться группой специалистов, представляющих обе стороны. Внутренний независимый оценщик — это обычно вторая или третья линия защиты (например, отдел управления рисками или внутреннего аудита) или их функциональный эквивалент в компании.

Оценка должна включать обзор существующих средств контроля и их эффективности, а также подтверждение того, что они соответствуют целям CSP-контроля. Такая оценка требует меньше времени и затрат по сравнению с полноценным аудитом.

Чтобы поддержать наших клиентов, мы создали директорию компаний, оказывающих услуги по проведению CSP-оценки. Список составлялся с учётом таких критериев, как опыт и квалификация служб кибербезопасности; стратегическая ориентация на услуги кибербезопасности; хорошая репутация и желание работать с клиентами из финансовой сферы. Ознакомиться с ним можно на swift.com. Обратите внимание, что клиенты также могут заключить договор с компаниями, не указанными в списке.

КРАЙНИЙ СРОК

Когда необходимо пройти аттестацию?

Крайний срок, когда необходимо подтвердить соответствие требованиям CSCF 2021 года и предоставить независимую оценку аттестации, — 31 декабря 2021 года.

ВЫСОКИЙ УРОВЕНЬ

Как прошла аттестация в 2020 году?

В результате усилий нашего сообщества по оценке своего соответствия требованиям CSCF мы увидели значительный уровень аттестации в 2020 году. Средний уровень соответствия по каждому обязательному элементу контроля варьировался от 93 до 99 %.

Эта задача будет постоянной. Важно, чтобы все клиенты продолжали тесно работать со SWIFT над укреплением своей системы кибербезопасности в дальнейшем.

ОТ ХАОСА К ПОРЯДКУ

РЫНОК АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Как известно, вопрос проведения аудита состояния информационной безопасности в финансовых организациях приобрёл актуальность с появлением ГОСТ 57580 и связанных с ним Положений Банка России. Сегодня требования о проведении аудита ИБ распространяются на примерно 420 кредитных (банки и НКО) и 170 крупных некредитных финансовых организаций. Среди них страховые, пенсионные фонды, профессиональные участники рынка ценных бумаг. И в ближайшее время эти цифры только вырастут. Рынок вырисовывается достаточно широкий. И, увы, представители аудиторского сообщества констатируют, что сегодня он недостаточно проработан и нуждается в грамотных инициативах и уверенных практических шагах регулятора, поднадзорных организаций и профессиональных аудиторов.

ТЕКУЩЕЕ СОСТОЯНИЕ РЫНКА АУДИТА ИБ. МОРЕ ПОДРЯДЧИКОВ И... МОРЕ ПРОБЛЕМ

На текущий момент единственным требованием для компании, которая может выполнять внешний аудит, является наличие лицензии ФСТЭК на ТЗКИ с определённым видом деятельности. Таких организаций насчитывается более двух тысяч, но необходимо учитывать, что при получении лицензии на ТЗКИ к ним предъявляются требования, никак не предполагающие знания и опыт работы в специфической финансовой отрасли, а именно знание процессов ФО и регуляторики ИБ ФО. По факту на рынке сейчас существуют не более 20–30 аудиторских компаний, которые имеют релевантный опыт

и знания. Однако как финансовые организации могут найти «сильных» аудиторов с положительной репутацией? Реестра таких организаций нет, как нет и методики оценки релевантности опыта и знаний и разработанных официальных требований к профессиональным аудиторам по ИБ. Кроме того, всё ещё нет системы их обучения, профессиональной подготовки и подтверждения квалификации. Единственный ресурс на сегодня — это реестр аудиторов, прошедших обучение по ГОСТ в Академии информационных систем. Он размещён на сайте Ассоциации АБИСС и включает как информацию о внутренних специалистах финансовых организаций, так и данные о сотрудниках компаний-аудиторов. Таким образом, ситуация на рынке аудита ИБ финансовых организаций сейчас такова, что не имеющие релевантного опыта специалисты выполняют аудит низкого качества, результатам которого не может доверять ни финансовая организация, ни Банк России. Назрела необходимость в формировании доверенной системы аудита информационной безопасности финансовых организаций. И эту сложнейшую задачу возможно решить только при постоянном трёхстороннем взаимодействии регулятора, финансовых организаций и аудиторов.

КАК ЖЕ СЕГОДНЯ ФИНАНСОВЫЕ ОРГАНИЗАЦИИ ВЫБИРАЮТ АУДИТОРА?

Эксперты рынка аудита ИБ свидетельствуют, что часть поднадзорных Банку России организаций, которым показано проведение внешнего аудита, не проводят аудит в принципе. Распространены случаи, когда сотрудник банка самостоятельно

КОММЕНТАРИЙ АБИСС



Евгений ЦАРЁВ
RTM Group, эксперт АБИСС

Учитывая несформированность рынка и отсутствие критериев качества, в подавляющем числе конкурсов и запросов коммерческих предложений на проведение аудита контракт достаётся компании, которая предлагает самую низкую цену.



Антон СВИНЦИЦКИЙ,
ДиалогНаука, эксперт АБИСС

Аудиторы должны не только обладать знаниями нормативной базы, используемой при проведении оценки соответствия, но также должны подтвердить и поддерживать свою квалификацию и знания как процессов аудита, так и применяемых технологий защиты информации.

готовит отчёт и подписывает его у дружественного лицензиата «за три копейки». Иногда не подписываются даже фиктивный договор и акты на работы по аудиту (по таким проектам не проходят оплаты). Часть поднадзорных организаций проводят аудит формально, оплачивая компании-аудитору символические 50–100 тысяч рублей, но только на бумаге. Отчёт же готовится силами самих сотрудников банка и лишь подписывается у лицензиата. По оценкам экспертов, не менее 30% кредитных организаций «проводили» аудиты по описанной модели.

Отдельная проблема — демпинг на рынке аудита ИБ. Учитывая несформированность рынка и отсутствие критериев качества, в подавляющем числе конкурсов и запросов коммерческих предложений на проведение аудита контракт достаётся компании, которая предлагает самую низкую цену. Экспертам известны примеры конкурсов как открытых, так и закрытых (без проведения торгов на площадке), по которым цена аудита по ГОСТ 57580 составляла 100–300 тысяч рублей без НДС для небольших организаций, 400–800 тысяч рублей для средних и 800–1200 тысяч рублей для крупных. Проведение качественного аудита при такой цене невозможно. Не так давно Ассоциация АБИСС провела анонимный опрос десяти компаний-аудиторов ИБ ФО о средней стоимости работ по проведению аудита ИБ для двух смоделированных банков — маленького с высоким уровнем зрелости ИБ и среднего с низким уровнем зрелости ИБ. Стоимость аудита по итогам опроса составила 1,2 млн рублей (10 недель работы аудиторов) и 3,4 млн рублей (16 недель работы аудиторов) соответственно. Разумеется, речь шла о качественном аудите с реальной оценкой соответствия требованиям и сбором всех необходимых свидетельств.

КАЧЕСТВО АУДИТОВ. ОБРАЗОВАНИЕ, ОПЫТ И КВАЛИФИКАЦИОННЫЕ ТРЕБОВАНИЯ

К сожалению, некоторые требования новых положений Банка России по защите информации и требования ГОСТ Р 57580.1–2017 написаны слишком обобщённо, что часто не позволяет двум независимым друг от друга аудиторам одинаково трактовать эти требования и использовать единый подход к оценке соответствия. Увы, разовым повышением квалификации эта проблема не решается. Необходимо планомерно повышать степень информированности аудиторского сообщества о подходах к оценке и видении Банка России в части результатов таких проверок. И делать это необходимо на регулярной основе на базе анализа со стороны

Ситуация на рынке аудита ИБ финансовых организаций сейчас такова, что не имеющие релевантного опыта специалисты выполняют аудит низкого качества, результатам которого не может доверять ни финансовая организация, ни Банк России

Банка России результатов оценок соответствия, отчётных документов аудиторов и предложений кредитно-финансовых организаций.

Аудиторы должны не только обладать знаниями нормативной базы, используемой при проведении оценки соответствия, но также должны подтвердить и поддерживать свою квалификацию и знания как процессов аудита, так и применяемых технологий защиты информации (в том числе применяемых ИТ-технологий, используемых для реализации технологических процессов). Сейчас же требования к квалификации и знаниям аудиторов не предъявляются.

ЕДИНАЯ БАЗА ЗНАНИЙ ПРОФЕССИОНАЛОВ АУДИТА ИБ

Эксперты полагают, что создавать систему доверенного аудита ИБ без детализации обобщённых формулировок и ведения единой базы знаний невозможно. Причём наполнять и использовать эту базу должны как внутренние специалисты по ИБ финансовых организаций, так и представители аудиторского сообщества при участии представителей Банка России, ответственных за методологию и надзор, в том числе по результатам анализа отчётных документов аудиторов и предложений кредитно-финансовых организаций. Единая база знаний может стать ещё одним шагом к созданию доверенной инфраструктуры аудита. С подобной инициативой выступила недавно Ассоциация АБИСС, подчеркнув готовность запустить базу знаний на своей платформе.

ОТВЕТСТВЕННОСТЬ АУДИТОРОВ. ОТСУТСТВИЕ КРИТЕРИЕВ КАЧЕСТВА РАБОТЫ АУДИТОРОВ

Говоря об ответственности аудиторов ИБ за результаты проверок, можно смело утверждать: сейчас качество их работы невозможно оценить в принципе. Проблема заключается в отсутствии установленных объективных критериев качества работы аудиторов. И даже профессионалы, за плечами которых десятки проектов по ГОСТ 57580, могут по-разному оценивать

одни и те же свидетельства и давать различные оценки. Причём невозможно однозначно утверждать, что один из них абсолютно прав, а второй полностью неправ. Причина таких разночтений обусловлена большой вариативностью трактовок мер и отдельных положений ГОСТ.

Действительно, оценивать качество аудита ИБ необходимо, но сначала нужно сформулировать критерии качества — рекомендации и разъяснения регулирующего органа. Для этого необходимо разработать три механизма:

- 1) базу знаний с разъяснениями по спорным моментам аудитов;
- 2) систему периодического обучения всех практикующих аудиторов;
- 3) систему, при которой по факту аудиты будут проводить только прошедшие специальное обучение специалисты, которые периодически повышают свою квалификацию и реально работают на проектах по аудиту.

СОЗДАНИЕ ЕДИНОЙ ИНФРАСТРУКТУРЫ АУДИТА

По мнению экспертов, решением проблемы качества аудита ИБ финансовой отрасли может стать система добровольной сертификации аудиторов, где объектом сертификации будет методика работы аудиторов. При этом инфраструктура будет описывать взаимодействие Банка России, финансовых организаций, компаний-аудиторов и учебных центров (Анастасия Харыбина, АКТИВ.CONSULTING, председатель АБИСС).

Основные моменты концепции:

- ◆ Создание единой методики проведения аудита ИБ финансовых организаций с использованием упомянутой выше наработанной базы знаний, пользуясь которой будут работать как аудиторы, так и представители надзора и которая будет доступна внутренним специалистам финансовых организаций.

◆ Разработка требований к квалификации аудиторов, а также требования к компаниям-аудиторам.

◆ Создание методики оценки качества проведенных аудитов через выборочную проверку, а также определение последствий для компаний-аудиторов в случае ненадлежащего уровня качества.

◆ Разработка обучающих курсов для аудиторов и определение критериев аттестации и перееаттестации.

В Ассоциации АБИСС создана рабочая группа, которая при взаимодействии с ДИБ Банка России прорабатывает данные вопросы.

ИЩЕМ ВЫГОДЫ ДЛЯ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ И РЕГУЛЯТОРА ОТ КАЧЕСТВЕННОГО АУДИТА

На прошедшей в конце марта в рамках конференции РусКрипто'2021 секции Ассоциации АБИСС по аудиту ИБ для финансовых организаций с участием представителей ДИБ Банка России спикеры говорили о реальных выгодах, которые получают регулятор, аудиторы и поднадзорные организации от создания системы доверенного аудита и повышения его качества. Профит для Банка России — реальная оценка уровня выполнения требований по ИБ, которая, в частности, влияет на риск-профиль финансовой организации и уровень резервирования средств, а также переход от бумажной безопасности к реальной. Профит для финансовых организаций — понятные критерии квалификации аудиторов, доверие к результатам аудита, на основе которых можно выстраивать программу развития ИБ. Профит для компаний-аудиторов — конкурентный рынок, на котором можно оказывать качественные услуги, при этом оставаясь коммерчески заинтересованными в этой деятельности. Очевидно, что весомые выгоды от упорядочения рынка аудита ИБ для всех его участников значительно ускорят процесс создания доверенной инфраструктуры.

КОММЕНТАРИЙ АБИСС



Евгений БЕЗГОДОВ
Deiteriy, эксперт АБИСС

Оценивать качество аудита ИБ необходимо, но сначала нужно сформулировать критерии качества — рекомендации и разъяснения регулирующего органа.



Анастасия ХАРЫБИНА
АКТИВ.CONSULTING, председатель АБИСС

Решением проблемы качества аудита ИБ финансовой отрасли может стать система добровольной сертификации аудиторов, где объектом сертификации будет методика работы аудиторов. При этом инфраструктура будет описывать взаимодействие Банка России, финансовых организаций, компаний-аудиторов и учебных центров.

ЧТО ТАКОЕ SASE

ВАША НОВАЯ СТРАТЕГИЯ БЕЗОПАСНОСТИ

ТРИ ПОДХОДА К ЗАЩИТЕ ФИЛИАЛОВ

Если у вас в этом году открываются офисы в 100 новых регионах, у вас на вооружении три стратегии:

1. Направить трафик из всех точек в единый, хороший и очень дорогой корпоративный шлюз безопасности.
2. Купить 100 новых устройств для защиты в каждый офис.
3. Купить сервис по защите трафика и его оптимизации.

В первом случае вы серьёзно нагружаете центральное устройство, часто нужно купить более мощное, то есть вы повышаете CAPEX. Сразу же возникает вопрос: «А зачем мне, находясь в Азии, подключаться к корпоративной VPN в Европе, чтобы получить защищённый доступ для сервиса снова из Азии?»

С ростом компании подключения всех сотрудников надо как-то масштабировать, а это сложно. Например, до пандемии коронавируса так подключалось 5 % сотрудников, и это было терпимо. Но сейчас так подключается 100 % вашего персонала. И зачем вообще такое «гимнастическое упражнение» с отправкой и возвратом трафика через весь мир для всех? Качество работы, продуктивность и удобство сильно ухудшаются.

Возможно, есть какой-то безопасный способ защитить сотрудника в месте его подключения к интернету. Лучше всего, если мы не будем отправлять трафик на проверку и получать его обратно, а будем осуществлять эти проверки на безопасность сами, на месте.

Во втором случае можно поставить устройства защиты непосредственно в каждый офис и ещё более серьёзно увеличить CAPEX и OPEX, чем в первом случае. Вам нужно угадать с производительностью в каждом офисе, да ещё обслуживать устройства придётся, то есть нанять больше сотрудников.

В третьем случае вы гарантированно получите нужную вам производительность функций безопасности и качество каналов при всех включённых функциях, поскольку такой SLA включается в контракт. И для компании это уже OPEX. Вот этот случай мы и рассмотрим в данной статье.

ТЕРМИН SASE

Чтобы разобраться, нужен ли вам безопасный доступ в интернет в виде сервиса, нужно

рассмотреть несколько аспектов, которые составляют данную технологию. Термин Secure Access Service Edge (SASE) на русский можно перевести как сервис безопасного доступа. Термин придуман компанией Gartner и включает, по их мнению, несколько компонентов.

ЧТО УВИДЕЛ GARTNER?

- ◆ Всё больше сотрудников работают удалённо.
- ◆ Всё больше приложений уходит в IaaS из корпоративного ЦОД.
- ◆ Всё больше облачных приложений SaaS используют сотрудники.
- ◆ Всё больше конфиденциальной информации находится в облачных сервисах, а не внутри корпоративного ЦОД.
- ◆ Больше трафика из филиалов направляется в облачные сервисы, а не в ЦОД.

Итоговое резюме: нужно объединить сетевые сервисы (NaaS), такие как CDN, и контроль полосы пропускания с сервисами безопасности (общепринятое название SecaaS), такими как VPN, CASB, SWG, FWaaS, WAAPaaS, RBI, где WAAPaaS означает web application and API protection as a service, RBI — remote browser isolation, CDN — Content Delivery Network, FWaaS — Firewall as a service.

Таким образом, SASE представляет защищённый доступ на основе множества современных технологий в виде доступного в каждой стране облачного ресурса. И ещё одно его полезное свойство: теперь можно управлять политикой по каждому сотруднику или устройству, где бы они ни находились, что резко повышает контроль по сравнению с ситуацией, когда мы пишем политику на целую сеть.

Идентификация сотрудника, устройства или сервиса — тоже важный компонент SASE. Конечно, может быть и другой контекст подключения, который будет влиять на доступ: время и страна подключения, уровень доверия к данному рабочему месту на основе проверок его соответствия корпоративной политике установленных и запущенных приложений.

С точки зрения функций безопасности, SASE содержит блокировки вредоносного кода, DLP, UEBA и IPS, включая эти функции внутри SSL.

Важный аспект — гарантия скорости и качества доступа.

Сильные стороны SASE — практически бесконечная производительность и удобство



Денис БАТРАНКОВ
эксперт BIS Journal



подключения новых филиалов и мобильных пользователей. Для этого в каждом регионе поставщику SASE нужно сделать точку присутствия (PoP — Point of Presence). У лидеров рынка уже более 100 точек присутствия по всему миру.

Таким образом, возможности SASE поставляются как сервис, который базируется на идентификации объекта, текущего контекста, политик безопасности организации или требований compliance и постоянно анализирует риск в течение жизни каждой сессии любого приложения. Объектами защиты могут быть люди, группы людей (филиалы), устройства IoT, приложения, другие сервисы или вычислительные мощности из облака.

СКОЛЬКО СТОИТ?

CIO и CISO, которые рассматривают замену своих текущих средств защиты on-premise, стоит рассмотреть вариант переход на SASE, что также будет переходом с CAPEX на OPEX и поможет сэкономить финансы. Мне известны ситуации, когда компания из 100 тысяч сотрудников, расположенная в 100 странах, посчитала два варианта: установить везде on-premise устройства — вышло 15 млн долларов — или купить SASE — всего 4 млн.

Нужно считать и TCO. Я считаю, что логично сравнивать TCO на 5 лет, поскольку обычно смена оборудования происходит каждые 5 лет.

А КАК ПОДКЛЮЧИТЬСЯ?

Для того чтобы получить такой сервис, офис компании подключается обычным туннелем IPSEC до точки предоставления сервиса по всему миру. У мировых брендов точки присутствия есть в каждой стране. Например, в Palo Alto Networks говорят о 100 точках присутствия сервиса Prisma Access, причём две из них в России. Для того чтобы подключить мобильных сотрудников, на их компьютерах и смартфонах должен стоять клиент VPN, который также подключается к ближайшей точке контроля и оптимизации трафика. Существуют ещё варианты подключения через HTTP-прокси, но вы должны понимать, что это защита только веб-приложений, и то если они поддерживают эту функцию.

Всё больше корпоративных приложений размещается вне территории компании. Постепенно многие компании перестают использовать собственные ЦОД. Выясняется, что дешевле использовать облачные аналоги в виде IaaS: Microsoft Azure, Amazon AWS, Google Cloud, Яндекс.Облако. И бизнес поддерживает это. Часть приложений так удобны, что их лучше всего использовать в виде SaaS: Office 365, Gmail, Dropbox, Яндекс.Диск, Evernote, Trello. Если ваша компания перешла на использование виртуальных ЦОД в облаке, переход на SASE — это следующий шаг.

SASE оказался очень востребован, когда все страны одновременно посадили сотрудников

работать из дома. Один из CIO в интервью компании Gartner сказал: «До пандемии у меня было 100 офисов и 50 000 сотрудников, а в один прекрасный день у меня стало 50 000 офисов». Если раньше все сотрудники находились внутри офиса и, по сути, внутри доверенной сети, то сейчас мир в прямом смысле перевернулся — теперь все находятся снаружи, в недоверенных сетях.

ГДЕ КУПИТЬ?

80% SASE продается через MSS интернет-провайдеров, таких как British Telecom, Orange, Accenture. Они используют SASE, чтобы предоставить вам MSS-услуги. Плюс для вас — они сами управляют этим сервисом.

Вы можете приобрести SASE у различных производителей независимо от провайдера, но тогда уже вы сами будете управлять этим сервисом.

ПРЕИМУЩЕСТВА SASE

- ◆ Автомасштабирование: теперь облако само масштабирует производительность системы защиты.

- ◆ Гарантия производительности: теперь не надо мучиться с выбором модели с нужной производительностью, даже если ты включил все функции, в том числе SSL Decrypt, и все сигнатуры IPS и антивируса, — защита предоставляется на заданной скорости.

- ◆ Минимальные задержки: облачные сервисы теперь работают с минимальными задержками благодаря средствам оптимизации маршрутов трафика внутри SASE, использующих искусственный интеллект.

- ◆ Доступность во всех странах.

- ◆ Скорость развёртывания: теперь не нужно ждать покупки, доставки и настройки устройства, можно за несколько дней подключить ВСЕ офисы во ВСЕХ странах.

- ◆ IoT-устройства можно защитить через SASE.

ЧТО ОЗНАЧАЕТ ZTNA

Важное преимущество защищённого удалённого доступа SASE — наличие ZTNA (Zero Trust Network Access).

Сравните две стратегии:

1. Вы подключаете по IPSEC весь офис в Бразилии в свой московский офис. Любой хост из бразильского офиса видит все московские хосты? Удобно? А безопасно?

2. Вы подключаете по IPSEC весь офис из Бразилии в свой офис в Москве. Только избранные сотрудники и устройства в бразильском офисе могут подключаться к нужным для них приложениям в московской сети. И дополнительным критерием доступа становятся проверки, что на

устройствах находятся нужные и правильно настроенные компанией приложения.

И вторая стратегия — то, что, собственно, и называется ZTNA. Вы даёте конкретным сотрудникам доступ к конкретным приложениям, а для этого ваше средство защиты должно понимать, на каком IP-адресе сейчас работает каждый сотрудник и какое приложение он в данный момент использует. Конечно, эту функцию сейчас содержат NGFW, поэтому основа технологий ZTNA заложена в уже известные устройства NGFW.

Нужно регулярно проверять для гарантии безопасного доступа, что устройства сотрудников соответствуют политике компании и защищены: там включены и работают антивирус, бэкап, шифрование диска — и всё это последних версий. Такую функциональность проверки состояния устройств обычно встраивают в клиент VPN. Спросите вашего поставщика есть ли такая функция сбора информации о хосте и последующей проверки.

Установив ZTNA, что вы постоянно видите:

- ◆ пользователя;
- ◆ его роль (группу);
- ◆ приложение и его состояние;
- ◆ состояние компьютера или мобильного устройства;
- ◆ страну;
- ◆ время доступа;
- ◆ риск из системы NTA/UEBA/DLP.

А ЗАЧЕМ SD-WAN?

Сейчас удалённые офисы подключают через SD-WAN, чтобы снизить количество проблем у приложений при изменении качества каналов. И для ИТ-службы это выливается в снижение числа кейсов в helpdesk в 100 раз.

НОВАЯ ФУНКЦИЯ SASE — МОНИТОРИНГ КАЧЕСТВА КАНАЛА

Было ли у вас так: вы выбегаете с ноутбуком из комнаты ближе к роутеру или переключаетесь на интернет через телефон, чтобы ваше совещание по Zoom не прерывалось?

Теперь появилась новая функция Digital Experience Management (DEM), которая позволяет каждому сотруднику разобраться, почему не работает приложение: что «глючит» — его точка Wi-Fi, провайдер или сам сервис компании.

* * *

Резюмируя, SASE — это целый мир, который привлекает своими удобством и качеством. Который, похоже, вполне может стать новой стратегией безопасности и цифровой трансформации.



Алексей РАЕВСКИЙ
генеральный директор
Zecurion

ВЫБОР ИДЕАЛЬНОЙ DLP-СИСТЕМЫ

9 ВОПРОСОВ, КОТОРЫЕ НУЖНО ЗАДАТЬ ВЕНДОРУ

Сегодня DLP-системы стали настолько обыденным инструментом в арсенале корпоративных служб информационной безопасности, что к их выбору подходят примерно так же вдумчиво, как домохозяйки подходят к выбору стирального порошка. Чей бренд симпатичнее, чья реклама более настойчива, чья цена привлекательнее... Тем не менее «под капотом» DLP-систем можно обнаружить много такого, о чём не пишут в рекламных буклетах, а цена ошибки здесь намного выше, чем при покупке бытовой химии. В связи с этим ИБ-службам было бы полезно глубже погрузиться в технические подробности, не ограничиваясь формальным сравнением галочек по списку «фич». На рынке сейчас много решений разного уровня зрелости, и наличие плюса в строке таблицы сравнения не гарантирует, что в реальности эта функция работает так, как нужно пользователю. Некоторые вендоры стараются выпустить продукт как можно быстрее, и при этом его качество, удобство и надёжность оставляют желать лучшего.

Имея значительный опыт на рынке DLP, мы решили собрать несколько практических вопросов, ответы на которые помогут понять, насколько зрелое решение вы рассматриваете и не получится ли так, что, потратив значительные средства, вы вложите в

продукт, которому ещё далеко до общепринятых стандартов корпоративного ПО.

Кроме этого, преимущество технологически зрелого корпоративного решения заключается в том, что у вендора не будет проблем с его поддержкой и выпуском новой функциональности. Обычно DLP-системы выбираются исходя из трёх-, а то и пятилетнего горизонта планирования, поэтому соответствие текущим требованиям не единственный критерий выбора. Надо понимать, куда движется вендор, и прогнозировать, какие задачи могут возникнуть у вашей компании в среднесрочной перспективе. Если вендор сможет за это время только довести продукт до надлежащего enterprise-уровня, возможно, связываться с ним не стоит.

ДЛЯ КАКИХ КАНАЛОВ ВОЗМОЖНА БЛОКИРОВКА ПО КОНТЕНТУ?

Этот вопрос может показаться странным, ведь буква «Р» в аббревиатуре DLP означает «prevention». То есть DLP-система по определению должна предотвращать утечки, а это можно сделать, только заблокировав подзрительную операцию. Тем не менее многие организации предпочитают использовать DLP-системы в режиме наблюдения, без активного вмешательства в информационные потоки. При этом вся информация сохраняется в архив и служба безопасности реагирует

на утечки постфактум, выявляя нарушителей и применяя к ним меры дисциплинарного воздействия. В связи с этим потребность в функциях блокировки отходит на второй план, поскольку активное их использование и не планируется.

Часто такая постановка задачи объясняется рисками ложноположительных срабатываний или сбоев DLP-системы. Если из-за DLP-системы будет нарушено функционирование электронной почты или какого-то другого жизненно важного сервиса, ущерб репутации ИБ-и ИТ-отделов может быть очень высоким. Однако этот аргумент относится только к незрелым DLP-системам, которые практически невозможно внедрить и настроить так, чтобы они работали без сбоев. При этом потенциальная утечка из-за отсутствия режима блокировки может стоить бизнесу очень дорого. Кроме этого, многие руководящие документы (например, GDPR) прямо требуют иметь защиту от утечек в режиме блокировки и предусматривают серьёзные штрафы для нарушителей.

Некоторые каналы, которые контролируются DLP-системами, не позволяют реализовать блокировку по сугубо техническим причинам. Например, для мессенджеров WhatsApp и Telegram возможен только пассивный мониторинг, в противном случае они не будут работать. Однако вряд ли рассматриваемую DLP-систему можно



считать достаточно зрелой, если в ней нет блокировки по содержимому файлов следующих каналов: электронная почта, внешние USB-диски, принтеры, веб-сервисы (протоколы HTTP/HTTPS).

ГДЕ ВЫПОЛНЯЕТСЯ КОНТЕНТНЫЙ АНАЛИЗ И ПРИМЕНЕНИЕ ПОЛИТИК?

Смысл этого вопроса заключается в том, что очень мало DLP-систем, присутствующих сейчас на рынке, изначально создавались как единые полноценные системы с продуманной архитектурой. Большинство вендоров начинало с какого-то одного модуля. Далее вокруг этого модуля достраивалось окружение для контроля остальных каналов, хорошо, если разработанное тем же

вендором. При таком хаотичном развитии приходилось учитывать все ограничения и особенности, которые имелись у первого модуля. Естественно, что результат нельзя назвать образцом эффективной архитектуры, а это неизбежно сказывается на потребительских характеристиках продукта.

Таким образом, по тому, где выполняется контентный анализ, зачастую можно определить, с чего начиналась история той или иной DLP-системы. Например, если endpoint-агент передаёт информацию для анализа на DLP-сервер по протоколу SMTP, то можно предположить, что продукт начинался с модуля контроля электронной почты. При этом сервер может возвращать результат анализа на агент, а может и не возвращать. В последнем случае

возможность блокировки по содержимому при записи на USB-диск или при печати вообще отсутствует. Понятно, что при такой архитектуре требуется постоянное соединение с сервером, а загрузка сети может быть слабым местом. В тендерной документации даже иногда можно встретить вопрос, поддерживает ли DLP-система приоритизацию сетевого трафика (QoS, Quality of Service). Это, скорее всего, означает, что рассматривалась только одна такая система, поскольку при грамотном проектировании контентный анализ выполняется там же, где применяются политики. Необходимость в передаче больших объёмов информации по сети просто отсутствует, и вопрос приоритизации сетевого трафика неактуален.

Если для «пилота» на 50–100 клиентов нужно более одного сервера, это означает, что архитектура системы неоптимальна и, скорее всего, будет требовать повышенных ресурсов и на этапе промышленной эксплуатации

КАК РАБОТАЕТ АГЕНТ СИСТЕМЫ, КОГДА НЕТ СОЕДИНЕНИЯ С КОРПОРАТИВНОЙ СЕТЬЮ?

Этот вопрос — логическое продолжение предыдущего. Но проблема не только в том, чтобы оптимизировать использование сетевого трафика. Агент, кроме выполнения контентного анализа и применения политик, должен передавать информацию о событиях, теневые копии и другие данные на сервер для записи в архив. Если связь с архивом отсутствует, вся эта информация не должна теряться. Как правило, она сохраняется на локальном диске и передаётся на сервер в момент, когда соединение установлено.

В идеале политики должны применяться на агенте в зависимости от того, есть ли непосредственное подключение к локальной сети, или компьютер подключён через VPN, или подключение отсутствует. Таким образом, для каждой среды можно устанавливать соответствующие правила. Это бывает важно, когда сотрудник с рабочим компьютером находится вне офиса — например, в командировке или на «удалёнке».

УДОБНО ЛИ УПРАВЛЯТЬ СИСТЕМОЙ?

Удобство управления — это весьма субъективный критерий. Кому-то привычнее управлять системой с помощью командной строки, кому-то удобно создавать политики и правила, программируя на скриптовом языке. Тем не менее продуманный и удобный интерфейс может быть косвенным признаком того, что разработчик в состоянии обеспечить качественную разработку и функциональные компоненты системы также качественны и эффективны.

В плане удобства и проработанности интерфейса важно отметить два аспекта. Во-первых, единая консоль управления. Сейчас чаще всего предпочтение

отдаётся веб-консолям. Они платформонезависимы, не требуют установки дополнительного ПО, могут работать на мобильных устройствах. Если же консолей несколько — например, отдельные консоли для управления отдельными модулями, — это говорит о том, что продукт не проектировался и не разрабатывался как единая, логически законченная система. Возможно, модули дописывались разными командами и «прилеплялись» (каждый со своей консолью) друг к другу в ходе ускоренного эволюционного развития. Может, они вообще собраны «с миру по нитке» — лицензированы у разных производителей и интегрированы не так, как следовало бы, а так, как получилось.

Во-вторых, зрелая DLP-система должна иметь омниканальные политики. Это означает, что если требуется создать политику для контроля, например, тендерной документации, то достаточно сделать это один раз и просто указать, к каким каналам она будет применяться — электронная почта, веб, USB-устройства и т.д. Менее совершенная система потребует создавать однотипные политики для каждого канала отдельно. Это может показаться небольшой проблемой, но количество политик имеет тенденцию к росту. Когда оно переваливает за сотню, а в правилах используются сложные условия, где присутствуют не только контентные правила, а ещё и группы пользователей, дни недели и т.д., поддержание такого набора в синхронизированном состоянии может превратиться в серьёзную головную боль.

КАКОЕ МИНИМАЛЬНОЕ КОЛИЧЕСТВО СЕРВЕРОВ НУЖНО ДЛЯ ВНЕДРЕНИЯ?

Ещё одним явным признаком дефектной архитектуры, видимым уже на «пилоте», может стать количество серверов, необходимых для работы системы. Если для «пилота» на 50–100 клиентов нужно

более одного сервера, это означает, что архитектура системы неоптимальна и, скорее всего, будет требовать повышенных ресурсов и на этапе промышленной эксплуатации. Качественная система уровня enterprise одинаково хорошо масштабируется в обе стороны. Безусловно, при увеличении масштаба внедрения потребуется возможность разнесения отдельных компонентов системы на разные серверы и их кластеризация. Но на малых внедрениях DLP-система не должна требовать неоправданно больших ресурсов.

ЛЕГКО ЛИ РАЗВЕРНУТЬ СИСТЕМУ? НАБОР ВАРИАНТОВ ВНЕДРЕНИЯ

Для серьёзной DLP-системы характерна поддержка множества вариантов внедрения. Это, во-первых, упрощает задачу совмещения DLP-системы с существующей ИТ-инфраструктурой, а во-вторых, позволяет гибко балансировать функциональную и вычислительную нагрузку при контроле различных каналов. Сегодня на рынке есть ряд систем, предусматривающих контроль всех каналов на уровне только endpoint-агента. Это сильно упрощает задачу вендору, позволяет сэкономить на команде разработчиков и сократить сроки разработки и выпуска новых версий. Однако такая архитектура не может считаться уровнем enterprise. Большинство сетевых каналов более естественно контролировать на уровне шлюза, особенно для масштабных внедрений.

Зрелая DLP-система, кроме агента для конечных точек, предлагает следующие варианты шлюзового внедрения:

- ♦ интеграция с почтовыми серверами (например, Microsoft Exchange). В этом случае можно удобно контролировать и внутреннюю почту;
- ♦ приём почты из технического почтового ящика;
- ♦ интеграция с имеющимся интернет-шлюзом по протоколу ICAP;
- ♦ собственный почтовый транспортный сервер.

Наиболее зрелые вендоры предлагают ещё собственный прокси-сервер, который обеспечивает интеграцию с DLP-системой для контроля HTTP- и HTTPS-трафика.

ПОДДЕРЖИВАЕТ ЛИ ОБЛАЧНУЮ ИНФРАСТРУКТУРУ?

Несмотря на небыстрое принятие облачных технологий в отечественной корпоративной среде, проблема использования в ней DLP-системы возникает весьма часто. При этом она может возникать в разных аспектах.

Прежде всего, иногда требуется установить серверные компоненты DLP-системы в облаке. Такое случается, как правило, на «пилотах» или у небольших организаций. Всё-таки архив DLP-системы хранит в себе все корпоративные секреты, и размещать его в неконтролируемой среде рискнут немногие. Тем не менее, если DLP-система не поддерживает размещение собственных серверных модулей в облачной среде, это в какой-то момент может стать неприятным сюрпризом.

Второй аспект — это контроль облачных хранилищ и сервисов. Речь тут может идти как о банальной выгрузке файла с конфиденциальной информацией в облако, так и о более сложных схемах, например когда организация использует почтовые сервисы Office 365 или G Suite. Здесь есть много нюансов и возникающих из-за них проблем. Скажем, для выгрузки файлов в облачные хранилища могут использоваться веб- или «толстые» клиенты. Та же история с почтовыми службами — для доступа к ним можно использовать как браузерный клиент, так и классический, например Microsoft Outlook. И для каждого варианта приходится применять различные протоколы и разные варианты внедрения. Также при использовании облачных хранилищ в организации необходимо обеспечить их регулярное сканирование DLP-системой для выявления хранящейся там конфиденциальной информации. Для решения подобных задач появился целый класс решений — CASB (Cloud Access Security Broker, брокер безопасности облачного доступа), но по решаемым задачам эти системы концептуально очень близки к DLP. Так или иначе, эти задачи необходимо решать, поэтому соответствующая функциональность будет появляться и в DLP-системах.

ИНТЕГРАЦИЯ С ДРУГИМИ КОРПОРАТИВНЫМИ СИСТЕМАМИ

Здесь речь, конечно, не идёт об интеграции с Microsoft Active Directory, которая должна быть реализована в любой современной DLP-системе. Чаще всего при внедрении DLP-системы бывает полезно, если поддерживается интеграция с нижеперечисленными классами ПО.

Управление информацией и событиями по безопасности (SIEM). Это, пожалуй, наиболее частый вопрос о совместимости, что вполне объяснимо: сейчас постройка центров SOC — одна из самых горячих тем в ИБ, и всем хочется, чтобы события из DLP попадали в поле зрения SIEM. В принципе, большинство SIEM-систем умеют самостоятельно загружать информацию из базы данных DLP, но гораздо удобнее, если DLP-система поддерживает Syslog, CEF и другие подобные протоколы. В этом случае при настройке DLP-системы можно более гибко управлять тем, какая информация и в каком виде будет попадать в базу данных SIEM, и добиваться большей эффективности.

Управление правами документов (EDRM). Чаще всего в этом контексте упоминается Microsoft RMS. В принципе, системы DLP и управления правами удачно дополняют друг друга по функциональности и обеспечивают более надёжную защиту, если правильно развёрнуты и настроены. В этом случае DLP-система понимает политики документов RMS и их можно использовать в политиках DLP, при поиске в архиве, построении отчётов и т.д. Кроме этого, DLP-система может сама применять политики RMS по определённым правилам, например, при обнаружении определённого контента.

Системы классификации данных. Наиболее совершенные DLP-системы понимают метки в свойствах документов, которые проставляют системы классификации данных, такие как TITUS, Bolden James и т.п., и позволяют их использовать в политиках. В этом случае можно извлечь двойную выгоду из уже потраченных усилий на работы по классификации данных. Впрочем, в наших широтах такие

системы встречаются не так уж и часто, в основном у крупных корпоративных заказчиков.

МУЛЬТИПЛАТФОРМЕННОСТЬ

Поддержка нескольких endpoint-платформ также является признаком солидной DLP-системы. Самые простые решения предлагают агентский модуль только для Windows. Однако сегодня этого может быть уже недостаточно. Давно взятый политический курс на импортозамещение может привести к массовому переходу на один из клонов Linux в обозримом будущем. Понятно, что связанная с этим замена DLP-системы — самая маленькая боль при решении этой проблемы. Тем не менее уже сегодня есть более зрелые продукты, в которых агент работает и на Linux, и на Mac.

Отдельно стоит сказать о поддержке мобильных устройств на базе iOS и Android. О ней часто спрашивают, но, к сожалению, реализовать полноценный агент для смартфонов и планшетов, особенно от компании Apple, практически невозможно по объективным техническим причинам. С другой стороны, при реализации стратегии BYOD можно (и нужно) использовать решение класса Mobile Device Management. Оно позволит задействовать встроенные возможности мобильной ОС, настроить политики конфиденциальности и снизить риск утечки через гаджеты до приемлемого уровня.

ВЫВОДЫ

Как мы увидели, DLP-системы развивались неоднородно, что может сказываться и на степени целостности системы как слаженно работающего механизма, и на наличии поддержки отдельных каналов распространения информации, и на объёме данных, которые необходимо передавать по каналам связи для функционирования системы. Конечно, в современном мире также имеют значение и страна происхождения используемого программного продукта, и цена решения, и стоимость владения им. Но всё же DLP должны в первую очередь решать реальные производственные задачи и по возможности работать не только в режиме мониторинга.



Артём КИСЕЛЁВ
директор Департамента
Маркетинга StaffCorp
(ООО Атом Безопасность)

ВЕРСИЯ 4.9. ТЕПЕРЬ ДЕЙСТВИТЕЛЬНО БОЛЬШЕ!

АРХИТЕКТУРА STAFFCOP ENTERPRISE

StaffCop Enterprise — это клиент-серверное приложение для контроля потоков информации и событий системы, а также всех действий сотрудников за рабочим компьютером. Программный комплекс осуществляет сбор и анализ данных, блокировку запрещённых действий и данных, а также оповещает о нарушениях политик безопасности.

На Staffcop Enterprise получен сертификат ФСТЭК России № 4234 от 15 апреля 2020 года, а также Staffcop Enterprise успешно прошёл тематические исследования на соответствие требованиям ТИ-698 Центра ФСБ России по следующим пунктам:

- ♦ соответствие декларированных и реальных возможностей программного обеспечения;
- ♦ отсутствие недеklarированных возможностей программного обеспечения;
- ♦ совместимость с средствами защиты информации;
- ♦ возможность работы в безопасной среде.

И что, пожалуй, не менее важно в нынешнее время — является на 100%

отечественным решением, а значит подходит под политику импортозамещения. Давайте посмотрим на версию 4.9 более пристально.

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ DLP

Самое важное в современном мире — это информация, поэтому в Staffcop Enterprise имеется обширный набор функциональных возможностей для контроля файлов. Первый из них — цифровые метки. Каждому файлу присваивается уникальный идентификатор, который позволяет отследить весь жизненный путь файла — кто изменял файл, удалял, перемещал, переименовывал, загружал и т.д.

Второй важной функциональной возможностью является модуль удалённого сканирования файлов, который позволяет провести аудит всех документов офисного формата, находящихся на компьютере, выявить конкретные документы и файлы, которые содержат в себе определённый текст (рис. 1). А также удалить эти данные.

В новой версии мы добавили блокировку файлов по содержимому. Вы

задаёте правило, с примером нужного текста, и когда система обнаружит соответствующий файл — его передача будет заблокирована. Эта функция работает с файлами MS Office, Open Office, pdf и текстовыми документами.

Файлы могут «утекать» двумя путями — локальная утечка и сетевая утечка. В локальную утечку входят:

- а) ситуации копирования файлов на USB-накопители;
- б) печать документов;
- в) получение доступа к информации, в том числе, с помощью RuToken на чужом рабочем месте.

К копированию на внешний носитель можно отнести распечатку документов на принтере — это может быть что угодно: например, список клиентов вашей компании. Staffcop Enterprise полностью контролирует все перечисленные инциденты — полностью фиксируя происходящее и блокируя контент по необходимости (рис. 2).

Staffcop Enterprise использует технологии OLAP-кубов и drill-down, что позволяет обеспечить как хранение огромного массива собираемых

Поиск на ПК - pdf референс

Выгрузка и печать

Панель управления

Админ

События

Анализ

Учет времени

Отчеты

Агент: Компьютер

↑ x

Файл: Имя файла

↑ x

Файл: Путь

↑ x

+

Количес

DemoZoneNB3

Референс-лист.pdf

C:\SC-NB\Downloads\Microsoft.SkypeApp_kzf8qxf38zg5c!App\All\Референс-лист.pdf

1

Всего: 1, Кол

Рисунок 1. Результаты поиска файлов на компьютере сотрудника

Поиск - Тип события	Время	Компьютер	Пользователь	Приложение	Получатели	Контент	Размер	Связано с
Операции с файлами	2021-03-26 18:08:34	Gremma-PC	user	explorer.exe		Скачать пароли и компромат - копия.txt	12 B	FileOperation
Перехваченный файл								
Всего: 2, событий: 7								

Рисунок 2. Скриншот незаконного копирования на USB-накопитель

данных, так и сохранение всех взаимосвязей, позволяющих отслеживать произошедшее в хронологическом порядке, а также имеет продвинутый конструктор отчётов с широким набором виджетов — вы можете настроить выдачу данных именно так, как нужно: период, сотрудники, целые отделы, используемое ПО, затраченное время и т.д. и т.п.

Также, в Staffcop Enterprise используются и другие высокие технологии — модуль распознавания лиц и распознавания текста, основанные на нейронных сетях LSTM (Long Short Term Memory), позволяющий автоматизировать процесс распознавания фотографий сотрудников, работавших за АРМ и фотографий документов, паспортов и т.д. (рис. 3).

Ну и вишенкой на торте DLP-модуля является детектор аномалий поведения пользователей — для выявления действий пользователей, нетипичных для их обычного режима работы и получения уведомлений об этом.

Второй тип утечки — сетевой. Сотрудник может отправить файл по почте или через мессенджер, сообщить данные через мессенджер и электронную почту или своими действиями допустить заражение компьютера вредоносным программным обеспечением/предоставить доступ злоумышленникам. Конечно, это серьёзные угрозы, но и с ними Staffcop Enterprise позволяет успешно бороться, блокируя передачу конфиденциальной информации, полностью записывая весь спектр действий пользователя в сети Интернет и определяя опасные темы для разговора с помощью словарей.

К сетевой утечке можно отнести также выгрузку баз из различного программного обеспечения. Наиболее ярким примером, пожалуй, тут может стать выгрузка данных из бухгалтерской программы «1С: Бухгалтерия». Особенностью этой программы является то, что названия создаваемых ей



Рисунок 3. Скриншот результатов распознавания лиц

файлов написаны кириллицей, но для Staffcop Enterprise это не проблема.

Доработке подвергся и кейлоггер — теперь сотрудники отдела безопасности сразу видят спецсимволы, без дополнительной настройки. Кроме того, мы не можем не похвастаться, что наш кейлоггер работает и в AstraLinux.

Общеизвестным фактом является то, что сотрудник тратит на работу только 40% времени, которое находится на работе — а как показывает наша практика, и того меньше. Staffcop Enterprise отслеживает начало работы компьютера, позволяя сразу выявить всех «опозднунов», и учитывает время, когда сотрудник не работал. Также Staffcop Enterprise позволяет разделить используемые сотрудником ресурсы на разные категории — продуктивные и непродуктивные. К тому же, политики продуктивности можно персонализировать для сотрудников или должностей (рис. 4).

Как вы убедились из вышесказанного — Staffcop Enterprise обеспечит вашу компанию всем необходимым, а при этом ещё и обладает очень привлекательной ценой. Всё ещё не можете себе позволить? Staffcop Enterprise — это комплексное решение, позволяющее решать задачи различных отделов — вы можете использовать

консолидированный бюджет нескольких отделов и при этом иметь всё необходимое.

СЕКТОР «ENTERPRISE»

В версии 4.9 мы уделили этому особое внимание и добавили несколько серьёзных новшеств, после которых мы можем с уверенностью сказать, что наше решение подходит для абсолютно любых компаний.

Первым нововведением стал ETL-модуль — этот модуль снижает требования к ресурсам сервера, особенно при работе с большим количеством агентов — причём уменьшает на порядок, действительно серьёзно снижая количество используемых ядер.

Так как AD остаётся одной из самых популярных служб каталогов от компании Microsoft, то важен процесс автоматизации работы с AD — поддержка Organizational Unit и функция «умной» синхронизации, позволяющая выгружать только тех пользователей, которые есть в Staffcop, и избегать выгрузки «мусорных» учётных записей.

Конечно, практически в любой крупной компании есть СКУД — системы контроля и управления доступом, поэтому логичным шагом в развитии Staffcop Enterprise стала возможность интеграции со СКУД. Мы провели

Учёт рабочего времени за период с 3 ноября 2020 по 3 ноября 2020

3 ноября 2020 г. Вторник

Пользователь	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	Начало	Окончание	Общее время	Активное	Простой	Опоздание
																									10:56:14	19:54:49	8:58:35	7:21:01	1:37:34	0:00:00
																									11:52:15	18:20:11	6:27:56	4:47:12	1:40:44	0:52:15
																									10:17:02	19:57:25	9:40:23	7:51:49	1:48:34	0:00:00
																									8:15:17	21:36:52	13:21:35	9:48:39	3:32:56	0:00:00
																									9:56:57	19:55:24	9:58:27	7:29:56	2:28:31	0:00:00
																									11:06:41	21:59:22	10:52:41	8:37:15	2:15:26	0:06:41
																									10:52:39	20:56:58	10:04:19	6:58:17	3:06:02	0:00:00
																									8:45:18	18:01:12	9:15:54	8:17:36	0:58:18	0:00:00
																									10:56:20	23:25:22	12:29:02	7:46:14	4:42:48	0:00:00
																									10:23:46	23:25:26	13:01:40	6:35:15	6:26:25	0:00:00
																									10:57:33	20:03:46	9:06:13	7:19:01	1:47:12	0:00:00
																									10:52:32	19:34:09	8:41:37	6:49:35	1:52:02	0:00:00
																									10:55:53	20:05:50	9:09:57	7:11:09	1:58:48	0:00:00
																									9:25:25	20:19:57	10:54:32	6:41:12	4:13:20	0:00:00
																									11:02:31	19:00:18	7:57:47	4:33:15	3:24:32	0:02:31

Рисунок 4. Распределение времени сотрудников в течение дня

тесты на СКУД, используемой в нашей компании, и остались весьма довольны результатами — поэтому, при желании, наши специалисты смогут интегрировать Staffcop Enterprise с используемой клиентом СКУД.

Часто у крупных клиентов уже имеются установленные системы безопасности — помимо существующей возможности выгружать данные (в форматах pdf и html), мы улучшаем взаимодействие с известными на рынке SIEM-системами, такими как RuSIEM и MAX PATROL SIEM. Это помогает проще интегрировать Staffcop Enterprise с уже имеющейся системой.

Тех, кто используют Linux-системы, а также имеют необходимость контролировать сотрудников, работающих на MacOS, мы тоже игнорировать не вправе, поэтому постоянно улучшаем наш агент для Linux и Mac. В новой версии мы значительно прокачали оба агента.

В наш Linux-агент мы добавили инвентаризацию программного обеспечения и «железа» — для учёта установленных

программ и конфигурации рабочих станций. В дополнение к этому мы подключили логирование работы самых распространённых пакетных менеджеров — dpkg (Ubuntu, Debian etc.) и rpm (CentOS, Linux: Red Hat Enterprise etc.).

Нельзя обходить вниманием и третью популярную операционную систему — MacOS. Наш агент поддерживает все версии, вплоть до 11.2.

ЗАКЛЮЧЕНИЕ

Как вы можете видеть, Staffcop Enterprise старается расти и развиваться планомерными шагами, становясь с каждым релизом всё лучше и лучше. Да, до какого-то окончательного результата ещё идти и идти — ведь всегда можно что-то улучшить и доработать, особенно если об этом просят наши клиенты.

Мы сохраняем режим выпуска версий 2 раза в год — это дисциплинирует и заставляет двигаться вперёд. Основной нашей задачей остаётся создание и поддержание высококачественного отечественного продукта,

который позволяет решить большинство задач наших клиентов. Релиз 4.9 был посвящён усилению функций DLP-модуля и решению задачи масштабирования — Staffcop Enterprise отвечает требованиям по защите информации для компаний из любых отраслей: банков, промышленных предприятий и т.д.

* * *

Убедитесь лично в функциональных возможностях программного комплекса Staffcop Enterprise — вы получите доступ к их полному набору в течение месяца бесплатного тестирования¹ на необходимом количестве компьютеров. А также мы проведём бесплатный вебинар², на котором расскажем все-все-все подробности о новой версии — и вы сможете всё увидеть своими глазами!

¹ <https://www.staffcop.ru/sce49>

² <https://pruffme.com/landing/staffcop/webinar>



Дмитрий ГОРЛЯНСКИЙ
руководитель технического
сопровождения клиентов
«Гарда Технологии»

ТОТАЛЬНЫЙ ПЕРЕХВАТ

КАК ИЗБЕЖАТЬ ПОДВОДНЫХ КАМНЕЙ ПРИ ВНЕДРЕНИИ DLP

Переход в онлайн и на удалённый формат работы для большинства компаний не прошёл бесследно. Вопрос информационной безопасности и защиты информации от утечки со стороны сотрудников встал очень остро. Поэтому вопросами внедрения DLP-системы в 2020–2021 гг. стали интересоваться даже те организации, которые ранее не имели и не планировали внедрять подобные системы. Соответственно, в сторону вендора значительно увеличилось количество запросов на пилотные внедрения, что позволило выявить некоторые общие закономерности и трудности в работе пользователей с DLP-системами.

УСТАНОВИТЬ — НЕ РАВНО ВНЕДРИТЬ

Типичная ситуация для любого пилотного внедрения: система установлена, распространены агенты на выборочную группу рабочих мест, даже включены предустановленные политики и правила, но конечному пользователю непонятно, что теперь со всей этой информацией делать. И на этом этапе возникают одни и те же типовые сложности:

Какая информация подлежит защите, и как её описать с помощью тех средств анализа данных, которые предлагают DLP?

Частая задача — защита ПДн. Если мы ограничимся контролем передачи ПДн, задача будет решена лишь формально.

Простой пример: практически в любом пилотном внедрении ставится задача выявлять факты передачи персональных данных за пределы домена. На деле эта политика сразу начинает обрастать исключениями.

Поэтому при формировании политик по выявлению утечек ПДн нужно учитывать не только само наличие ПДн, но и форму, в которой они передаются.

Как работают предустановленные политики?

Предустановленные политики требуют донастройки. Важно учесть контекст — отправителя информации. Понимая процессы, можно с высокой точностью формализовать, какие отчёты и какие документы генерируют разные подразделения, работающие с персональными данными, и уже более точно настроить политики. Например, документ с персональными данными водителей отправлен сотрудником отдела технической поддержки. В большинстве случаев такой документ отправляют кадровые службы или проектные менеджеры. Поэтому политику нужно уточнить параметром «Отправитель» и указать другие подразделения.

Все ли потенциальные инциденты можно описать политиками безопасности?

Не все инциденты безопасности политика может распознавать по единичным срабатываниям. Для выявления косвенных признаков нужно настроить отдельные политики для последующего анализа.

Далее рассмотрим приёмы из нашей практики внедрений, которые могут оптимизировать этот процесс.

КАК ПРАВИЛЬНО ПОЛЬЗОВАТЬСЯ DLP-СИСТЕМОЙ

Работу с объектами в DLP-системе можно разделить на три больших направления:

1. Настройка политик для выявления инцидентов

Для правильного внедрения важно использовать все основные возможности, заложенные в функциональность системы защиты от утечек, и комбинировать их при настройке политик.

Основные способы детектирования информации:

1. Анализ по ключевым словам. Первое, что можно сделать при создании политик, — собрать ключевые слова, содержащиеся в критических документах.

2. Цифровые отпечатки документов. Сканирование документов по форме позволяет отслеживать их перемещение и предотвращать утечку данных.

3. Регулярные выражения.

4. Словари. Ключевые слова можно объединять в группы — основные понятия, термины, которые встречаются в определённом типе документов или переписки.

5. Свойства передаваемого объекта: канал передачи, отправитель/получатель, формат файла, дополнительные свойства.

Следует различать сами инциденты и их косвенные признаки. Автоматически выявить косвенные признаки инцидентов без участия человека, который сможет их проанализировать и сопоставить, очень сложно

Пример составления политики

Необходимо выявить утечки по определённым автоматизированным системам внутри компании, в частности, документ «Технический паспорт АС». При постановке на контроль образца документа или набора ключевых слов будет большое количество срабатываний, когда подобные документы передаются между службой ИБ и разработчиками АС.

Тут стоит использовать регулярные выражения. Необходимо подобрать regex, который:

- а) будет присутствовать только в паспортах на уже внедрённые АС;
- б) будет действителен для всех защищаемых АС, независимо от их назначения.

Изучив пример такого документа, можно найти раздел «Сведения об аттестации объекта», в котором указан инвентарный номер аттестата вида «Аттестат № 0101266-СТ».

Эта строка довольно удобна для построения регулярного выражения:

/№ \d{7}-[А-Я]{2}/gm

Таким образом, дополнив настройки политики условием — текстом, соответствующим данному регулярному выражению, можно гарантированно перехватывать технические паспорта только на внедрённые АС, поскольку у невнедрённых АС данный аттестат отсутствует.

Другой пример — печать платёжного поручения

Печать или передача пустого платёжного поручения не является инцидентом, но можно уточнить политику, добавив в неё условия:

- ♦ документ печатается не кассиром-операционистом / документ печатается не на принтере в кассе (DLP-система позволяет указывать имя принтера);

- ♦ в распечатанном документе присутствуют паспортные данные (по регулярному выражению).

Грамотным решением будет предварительная организация единого хранилища документов и внедрение в документы особых меток, содержащих буквенно-цифровые последовательности. Такой последовательностью можно закодировать определённые параметры документа (отдел, тип документа — договор, отчёт или другое, дата составления, уровень критичности и др.). При этом формируют в политиках соответствующие регулярные выражения для перехвата конкретных типов документов по закодированным в этой метке свойствам.

2. Поиск по перехваченной информации

Многие современные DLP-системы предлагают возможности по ретроспективному поиску по уже перехваченной информации. Это необходимо:

- ♦ для проведения расследований инцидентов и выявления контекста инцидента;
- ♦ для поиска инцидентов, не попавших под настроенные политики;
- ♦ для поиска косвенных признаков инцидентов.

Также, если это позволяет интерфейс DLP-системы, поиском удобно пользоваться для предварительной проверки работы политик. Например, задача перехвата технических паспортов АС. При наличии инструментов поиска можно смоделировать два факта передачи — один, который нарушает политику безопасности, второй — не нарушающий. Далее с помощью поиска и настраивают параметры таким образом, чтобы в выдаче на поисковый запрос присутствовало первое срабатывание, но отсутствовало второе. Уже после того, как поисковый запрос

отработает корректно, можно сохранить его как политику, чтобы она выявляла срабатывания в автоматическом режиме.

Формирование выборок объектов на основе поиска позволяет применять графическую визуализацию к результатам поиска. Это удобно для быстрого анализа объектов. Например, получив выборку всех документов, скопированных пользователями на внешние носители, мы можем выстроить отчёт по наличию в этих документах персональных данных и определить массовую утечку.

Подобными графиками также удобно пользоваться на этапе, когда ещё не настроено ни одной политики. Например, можно сделать выборку по определённому документу, проанализировать, на какие почтовые домены он отправляется, выделить для себя наиболее часто встречающиеся. Чаще всего это разрешённые получатели, и нужно добавить их в соответствующие периметры.

3. Идентификация косвенных признаков инцидентов

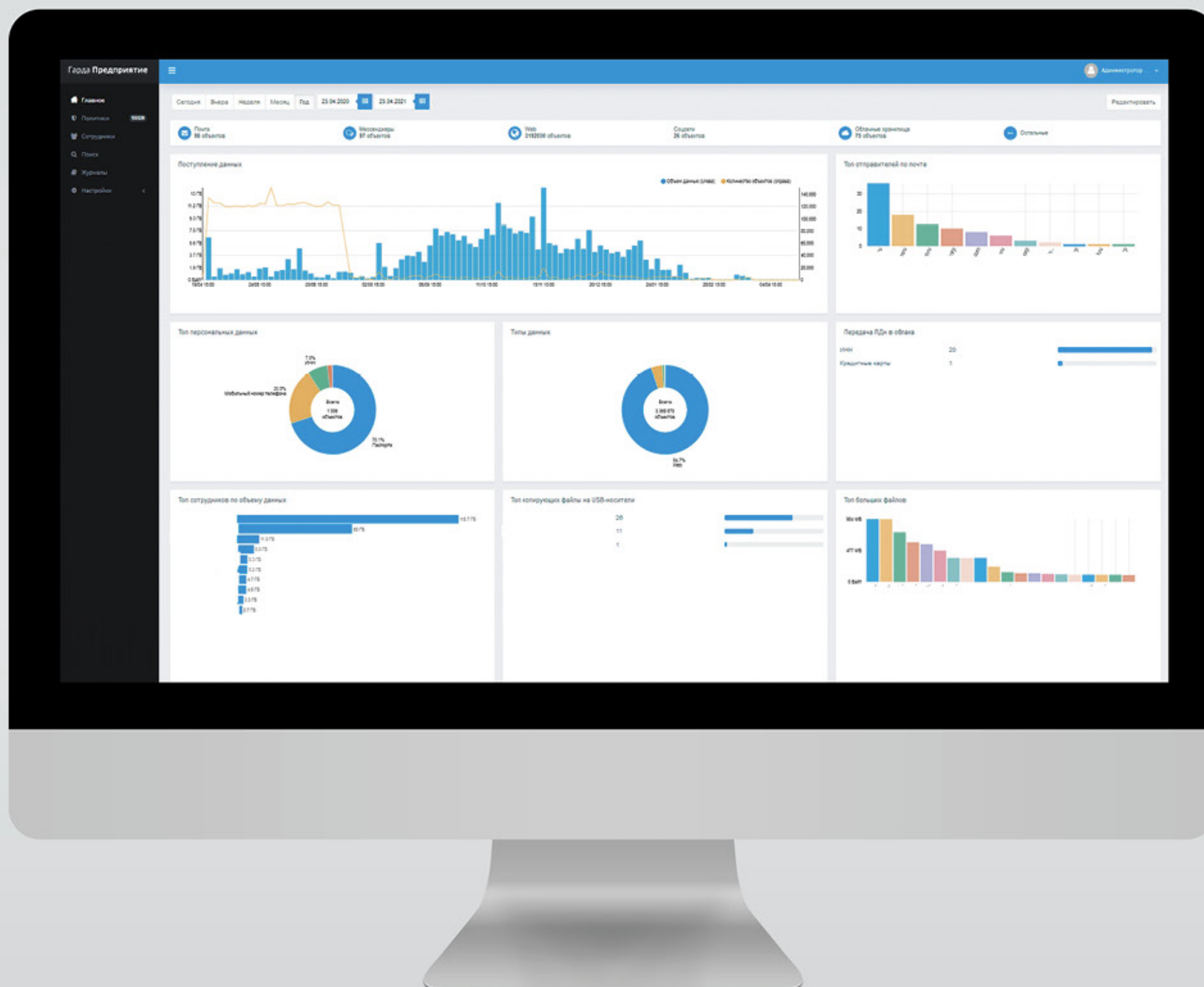
Следует различать сами инциденты и их косвенные признаки. Автоматически выявить косвенные признаки инцидентов без участия человека, который сможет их проанализировать и сопоставить, очень сложно.

Косвенные признаки инцидентов можно выявлять не только по типам данных, но и, например, распределив срабатывания по временной шкале и выявив факты обработки персональных данных в нерабочее время.

Аналогичный график можно построить по фактам открытия пользователями в MS Word критически важных документов.

В примерах использован поиск по ключевым словам в наименовании открытого приложения и заголовках активного окна, что позволяет отслеживать обращения пользователей к определённым документам.

Ещё одним косвенным признаком инцидента применительно к электронной почте является тема письма, а точнее — её отсутствие. Больше половины инцидентов в 2020 году на пилотных внедрениях выявлено по следующей комбинации признаков:



отправитель — внутренний пользователь, получатель — домены mail.ru, yandex.ru (и другие публичные сервисы), наличие в письме либо текста, либо регулярных выражений, либо документа по образцу и отсутствие темы письма. В большинстве случаев это будет либо передача пользователем письма самому себе на личную почту (многие пользуются этим способом «унести» данные при невозможности использовать USB-накопители), либо какая-либо нерабочая переписка.

Для описания признака «отсутствие темы» в данном случае мы используем выражение «!*?*», что означает отсутствие одного любого символа.

ВОЗМОЖНОСТИ DLP-СИСТЕМЫ «ГАРДА ПРЕДПРИЯТИЕ» ПРИ ВНЕДРЕНИИ В ОРГАНИЗАЦИИ

«Гарда Предприятие» — одна из первых DLP-систем, спроектированная с применением Big Data (технология больших данных). В системе работает политика тотального перехвата. Чтобы система собирала информацию, нет необходимости в предварительной настройке политик. Это даёт дополнительные инструменты в виде поиска по уже перехваченной информации.

Технически она представляет собой классическую DLP-систему с модулями агента, анализатора трафика, который

может работать с прокси-серверами по ICAP, а также с модулями интеграции с корпоративным почтовым сервером.

Агенты «Гарда Предприятия» успешно работают как с Windows, так и с Linux и iOS и выполняют большинство функций, необходимых для успешного функционирования DLP-систем: контроль печати, контроль мессенджеров, облачных хранилищ.

Внедрение DLP-системы всегда начинается с оценки задач и объёма защищаемой информации. Тонкая настройка позволяет не только выявлять и расследовать инциденты, но и предотвращать их уже по первым признакам.



**Алексей
ПАРФЕНТЬЕВ**
руководитель
отдела аналитики
«СёрчИнформ»

НЕ ВСЕ DLP «ОДИНАКОВО ПОЛЕЗНЫ»

КАК ВЫБРАТЬ СИСТЕМУ И НЕ РАЗОЧАРОВАТЬСЯ

DLP для многих компаний — решение из категории обязательных, когда речь идёт о защите от утечек информации и прочих инсайдерских рисков. Но опыт работы в программе для пользователей оказывается не всегда приятным. В статье мы рассмотрим заслуженные и несправедливые упреки в адрес DLP, разберёмся, какие касаются естественных ограничений класса систем, а какие — недостатков конкретных продуктов.

1. НЕ ХВАТАЕТ ФУНКЦИЙ ДЛЯ РЕШЕНИЯ ЗАДАЧ

DLP-системы давно переросли своё первоначальное назначение — контроль утечек данных. Сейчас они используются для решения гораздо более широкого круга задач информационной, экономической, кадровой безопасности. DLP сегодня — это настоящие супермашины.

Тем не менее заказчику может не хватать функций. Часто это выясняется после внедрения, потому что заказчик пренебрегает полноценным тестированием, ориентируясь на маркетинговые описания и чужие сравнительные таблицы. Тестирование отнимает время на старте, но сильно экономит его, когда дело доходит до эксплуатации. Поэтому к нему нужно подготовиться. Составьте свою сравнительную таблицу, ставьте на тест последовательно несколько систем и смотрите, как они отработают по наиболее критичным именно для вас задачам.

Например, одному нашему клиенту было важно блокировать пересылку файлов по метаданным, другие

случаи пересылки его не интересовали. Перед покупкой нашей DLP-системы («СёрчИнформ КИБ») компания тестировала несколько других, и выяснилось, что они с задачей не справляются. Хотя в брошюрах напротив этого типа блокировки стояла галочка.

Ограничение функциональности также может быть связано с тем, что в DLP применяются сторонние разработки. Иногда это целые движки, модули, платформы или даже whitelabeling чужого продукта под видом своего. В результате вендор ограничен функциональностью чужого программного продукта и его планами развития. Это частая проблема и иностранных, и ряда отечественных DLP-систем.

Мы в своё время приняли решение работать на собственном поисковом движке, его используем не только в DLP, но и в других продуктах. Все остальные элементы наших систем также самописные. Если клиенту потребуются доработки, исправление ошибок или техническая поддержка, он гарантированно их получит.

Часто ограничения DLP-системы связаны с тем, что заказчику требуется специфическая функциональность. Если это важные функции, которые к тому же окажутся полезны многим заказчикам, вендоры часто включают их в план разработки. У нас в системе из таких пожеланий появилась интеграция со СКУД-, BI-системами, таск-менеджер, элементы фразового поиска и многое-многое другое.

Но для решения многих задач клиента не всегда нужны специфические возможности, бывает достаточно комбинации существующих функций ПО.

Клиент, понятно, не всегда об этом знает, лучшими практиками должен делиться разработчик. Но в основном у вендоров это просто не предусмотрено, а всё сопровождение ограничивается техподдержкой. У нас, кроме техподдержки, есть отдел внедрения, которого нет у других. Специалисты подключаются к работе с первых дней тестов, учат работе с DLP, рассказывают о нюансах, помогают делать все настройки, чтобы «подогнать» систему под конкретные задачи. А потом — сопровождают клиента во время эксплуатации.

Ещё один фактор, который нужно учитывать, есть ли у вендора что предложить, кроме DLP. Эта система сегодня стала центральным элементом защиты от любых инсайдерских рисков, поэтому, выбирая её, заказчик, по сути, выбирает экосистему и других защитных продуктов. Если такой линейки у разработчика нет, компания может столкнуться с проблемой интеграции разных программ. Часто это сложная и даже нерешаемая задача, нужно помнить о ней заранее.

2. DLP СЛОЖНО ВНЕДРЯТЬ, ОНА «ПРОЖОРЛИВА» В ПЛАНЕ РЕСУРСОВ

Это одна из ключевых проблем. Разработчики по-разному подходят к оптимизации работы DLP-систем, в результате программы сильно отличаются по «прожорливости». Несмотря на то что вендоры подробно описывают минимальные технические требования, во время внедрения может произойти неприятный сюрприз. Чем больше объём внедрения, тем более он вероятен.

Варианта два. Идеальный — устраивать полноценный нагрузочный тест (развернуть все модули на максимальном количестве компьютеров). Но это не всегда возможно. Второй вариант — спрашивать мнение тех ИБ-специалистов, у которых стоит DLP-система на схожий с вами объём машин. Просите рассказать откровенно, с какими трудностями столкнулась компания.

Мы сами последовательно работаем над тем, чтобы снизить требовательность системы к «железу». Ещё в прошлом году изменили архитектуру, и это позволило увеличить быстродействие DLP на 30% и расширить спектр решаемых задач — искать данные в очень больших сетях, например. Раньше для этого заказчикам приходилось выделять большие мощности, размещать дополнительные сервера. В результате нашему КИБу нужно в 2–3 раза меньше серверных ресурсов, чем ближайшим конкурентам.

Имеет значение и скорость внедрения, ненормально, если оно занимает недели и уж тем более месяцы. Процесс может затянуться, если клиент ограничивает доступ или у него нет технического специалиста. Но в любом случае нормальная скорость внедрения типового пилота — несколько часов. Мы обеспечиваем её за счёт того, что на нашей стороне с клиентом работает технический специалист (инженер) и специалист внедрения (который обучит работе с программой, поможет настроить политики и решить конкретные задачи).

3. МНОГО ЛОЖНЫХ СРАБОТОК

Опытные ИБ-специалисты понимают, что это неизбежное «зло»: лучше считать ложные сработки, чем упустить важное. Но это не значит, что вся работа должна превратиться в разбор потенциальных инцидентов. У хороших программ число ложных сработок можно свести к минимуму за счёт гибкой настройки политик безопасности. Важно вовремя остановиться и найти баланс.

Например, можно исключить из мошеннической политики сработки на слово «кинуть», чтобы не получать ложные алерты «кинь мне деньги на карточку/телефон». Но мы советуем

DLP-система не работает как антивирус (поставил — и он работает). «Заводских» настроек программы для защиты от утечек хватит, чтобы вести мониторинг, блокировать пересылку по готовым политикам безопасности. Конечно, это уже обеспечит защищённость, но для её повышения нужно пересматривать политики безопасности, бизнес-процессы, проводить расследования.

этого не делать, потому что можно пропустить разговор о том, как сотрудники собираются кого-то обмануть.

Возможность настроить политики гибко — одна из сильных сторон нашей DLP-системы. У нас реализованы множество разных видов анализа: по словам, словарям, морфологии, атрибутам, по регулярным выражениям, цифровым отпечаткам, по алгоритму «поиск похожих», статистическим и комплексным поисковым запросам, а также любым комбинациям вышеперечисленных. При правильном подходе и с привлечением отдела внедрения можно настроить политики безопасности максимально тонко, но эффективно.

4. ПРОГРАММА КАЖЕТСЯ СЛОЖНОЙ, НЕКОМУ РАБОТАТЬ

DLP-система не работает как антивирус (поставил — и он работает). «Заводских» настроек программы для защиты от утечек хватит, чтобы вести мониторинг, блокировать пересылку по готовым политикам безопасности. Конечно, это уже обеспечит защищённость, но для её повышения нужно пересматривать политики безопасности,

бизнес-процессы, проводить расследования. И если у заказчика нет понимания, что делать с этими данными дальше, он будет использовать от силы 10–20% возможностей DLP.

Другая проблема в том, что с программой бывает некому работать или текучка ИБ-специалистов такая, что новый человек просто не успевает обучаться. Если вендоры не учитывают этот аспект, их система в какой-то момент рискует стать мёртвым грузом на балансе клиента. С неизбежным разочарованием в DLP-системе как в классе ПО.

Мы давно работаем с этой проблемой. Так появился учебный центр и сильный отдел внедрения, который, по сути, делит с клиентом большой объём работ. В результате мы можем развернуть и обеспечить работу DLP-системы независимо от того, какова квалификация ИБ-специалистов и укомплектован ли их штат у клиента.

Но мы пошли ещё дальше и запустили аутсорсинг DLP, чтобы полностью снять с клиентов головную боль за аналитику и отчётность. В таком формате аутсорсинг может работать и в тех компаниях, где вовсе нет ИБ-отдела, а если такой есть — как подмога ему.

Мы регулярно слушаем обратную связь от пользователей DLP-систем. Те, кто сумел правильно выбрать программу и использует её на 100%, знают, какие огромные возможности она даёт для управления безопасностью, кадрами и бизнеса в целом. Но чтобы система не разочаровала, а превосходила ожидания, её нужно тестировать. Запросите дополнительную информацию о возможностях DLP-системы «СёрчИнформ КИБ» по ссылке.





ЗАЩИТА КОРПОРАТИВНЫХ ДАННЫХ ОТ УТЕЧКИ



INFOWATCH
TRAFFIC MONITOR

DLP-система Traffic Monitor
с продвинутыми
технологиями анализа

МЕНЬШЕ РУЧНОЙ РАБОТЫ

Методы машинного обучения

МЕНЬШЕ ЛОЖНЫХ СРАБАТЫВАНИЙ

Полноценный контентный анализ —
28 патентов

КОНТРОЛЬ ВСЕХ КАНАЛОВ

Мобильные телефоны, соцсети,
облачные сервисы и проприетарные
системы — в дополнение
к привычному списку

Готовые интеграции для защиты информации
в постковидную эру: ERP, CRM и СЭД, MS Exchange
и MS Exchange Online, др.

ЗАКАЖИТЕ ДЕМОНСТРАЦИЮ

[TM.INFOWATCH.RU](https://tm.infowatch.ru)

РАСШИРЕННЫЕ ВОЗМОЖНОСТИ АНАЛИТИКИ ДАННЫХ DLP-СИСТЕМЫ



INFOWATCH
VISION

InfoWatch Vision — инструмент визуальной аналитики для построения наглядной карты коммуникаций в компании

ГРАФ СВЯЗЕЙ 50 ТЫСЯЧ УЗЛОВ

- Сокращает время на генерацию и проверку гипотез в 3–4 раза*
- Показывает маршруты перемещения информации, даже на личные адреса и usb-накопители
- Помогает работать с данными в организациях с распределенной структурой

Сводная статистика по всем филиалам и подразделениям, моментальный drill down до отдельных событий, области видимости данных для разделения полномочий



INFOWATCH
PREDICTION

InfoWatch Prediction — инструмент предиктивной аналитики данных для прогнозирования рисков и профилактики утечек

50+ АНАЛИЗИРУЕМЫХ ПАРАМЕТРА

- Позволяет выявлять отклонения в поведении сотрудников с помощью алгоритмов машинного обучения
- Подсвечивает аномалии, цепочки связанных событий и превышения заданных порогов
- Уведомляет специалиста ИБ о надвигающемся или скрыто реализующемся инциденте

*результаты опроса удовлетворенности клиентов InfoWatch Vision

[VISION.INFOWATCH.RU](https://vision.infowatch.ru)

[PREDICTION.INFOWATCH.RU](https://prediction.infowatch.ru)

 /InfoWatchOut

 /InfoWatch

 /InfoWatchNews



Дмитрий КУРАШЁВ
сооснователь UserGate

ПРЕВОСХОДСТВО РОССИЙСКОГО РЕШЕНИЯ

ШИРОКИЕ ВОЗМОЖНОСТИ ПОДДЕРЖКИ ДИСТАНЦИОННОЙ РАБОТЫ НА БАЗЕ ПЛАТФОРМЫ USERGATE

О новой грани преимуществ работы с отечественным производителем ИТ-оборудования и о том, как успешно выдержать экзамен в условиях ковидного аврала, рассказывает сооснователь компании «Юзергейт» Дмитрий Курашёв.

Напомним, что сфера деятельности «Юзергейт» — разработка и поставки комплексных систем защиты корпоративных сетей на основе межсетевых экранов нового поколения (NGFW) UserGate (модели C, D, D+, E, E+, F, X1), анализаторов событий и инцидентов в ИТ-среде UserGate Log Analyzer

(модели E6; E14; F25). Из этой краткой справки с упоминанием широкого спектра моделей уже можно сделать вывод, что одно из преимуществ работы с «Юзергейт» — гибкие возможности для штатного выстраивания системы обеспечения информационной и кибербезопасности предприятий. Но есть и иные аспекты гибкости платформы UserGate и гибкости сотрудничества с «Юзергейт», которые проявились в период аврального внедрения дистанционного режима работы и масштабирования ИТ-технологий для поддержки «удалёнки».

БУДЬ ГОТОВ!

— Дмитрий Сергеевич, не секрет, что в апреле 2020 года ряд компаний был вынужден в авральном порядке решать проблемы сохранения работоспособности своих коллективов на основе дистанционной работы. Можно предположить, что возникли проблемы разной природы. С одной стороны, это вопросы дооснащения инфраструктуры. С другой — необходимость повышения компетенций ИТ-персонала компаний в вопросах развёртывания систем безопасной «удалённой» работы с разными

BIS-КОММЕНТАРИЙ

Было бы наивно рассматривать ситуацию лишь взором, слегка затуманенным слезой умиления. В целом мы видим естественный процесс: заказчики сделали ставку на отечественного производителя, отечественный производитель помнит о своей ответственности (подробнее см. Антуан де Сент-Экзюпери «Маленький принц»). И, конечно же, среди предпосылок для благополучного разрешения «кризиса» — ещё и надёжный фундамент функциональных возможностей оборудования с брендом UserGate. И его качество, которое сотрудник отдела продаж назвал бы «бескомпромиссным», но мы лишь отметим, что оно — это качество — находится под контролем соответствующей системы управления качеством (КС У КП и ISO 9001).

Удалённый доступ на базе оборудования UserGate. Как уже упоминалось, шлюзы UserGate с масштабируемыми характеристиками (модели UserGate C, D, D+, E, E+, F, X1) реализуют концепцию межсетевого экрана нового поколения (NGFW). В «постулаты» этой концепции входит возможность поддержки безопасной дистанционной работы с корпоративными ресурсами и, при необходимости, дистанционной работы в корпоративной сети.

Платформой UserGate поддерживаются режимы «публикации» ресурсов и «удалённого» (дистанционного) доступа по VPN-каналу.

Для «публикации» ресурсов можно использовать технологии DNAT-публикации, Reverse proxy («обратный прокси») или веб-портала.

При использовании DNAT-публикации поддерживается ограничение доступа по IP-адресам, а режим Reverse proxy поддерживает, помимо ограничений по IP-адресу, ещё и авторизацию на основе сертификатов. «Обратный прокси» может быть использован для работы с внутренними системами CRM и ERP, с почтовыми службами, включая Sharepoint и OWA (Outlook Web Access), а также для обеспечения работы с определёнными файлами, находящимися на внутренних серверах организации.

Веб-портал позволяет сотрудникам получить безопасный доступ к корпоративным приложениям через браузер, предоставляя удобство использования технологии единого входа (SSO) для опубликованных сервисов, поддерживающих авторизацию

категориями пользователей. Как удалось найти выход из сложившейся ситуации заказчикам вашей компании?

— Безусловно, значительная часть наших заказчиков столкнулась с обеими проблемами. И сразу стало понятно, насколько грамотно организована работа корпоративной ИТ-инфраструктуры. В отдельных компаниях, в том числе и с помощью нашего UserGate, уже был организован безопасный доступ удалённых сотрудников к корпоративным ресурсам. Таким компаниям пришлось намного легче. Хотя и в подобных случаях возникали проблемы, связанные с тем, что аппаратные возможности используемых платформ не были готовы к ТАКОМУ числу удалённых пользователей. Нам в ряде случаев приходилось буквально «спасать» наших клиентов, предоставляя им дополнительные платформы без каких-либо процедур и даже бумаг. В любом случае, анализируя

тот острый период, важно заключить, что ИТ-инфраструктура должна всегда быть готова к подобным вызовам, в том числе к внезапному переводу сотрудников на удалённую работу.

ЛУЧШАЯ БИТВА ТА, КОТОРОЙ НЕ БЫЛО

— Дмитрий Сергеевич, ковидный аврал — это нештатная «вдруг»-ситуация. Но цифровизация отечественной экономики может заставить наши предприятия и организации испытать ещё одно потрясение, связанное с «внезапным» осознанием владельцами КИИ наступления сроков проверки показателей так называемого импортозамещения. Какие шаги вашей компании позволят реально решать задачи импортозамещения, не вступая в этот бой «с колёс»?

— Думаю, тут каждый должен делать всё возможное, находясь на своём месте.

Задача UserGate — это прежде всего разработка качественного и производительного решения как в программной, так и в аппаратной части. Задача заказчиков — это грамотное планирование, своевременное проведение пилотных работ, сравнений и, наконец, закупок. К сожалению, не все в полной мере выполняют свои обязанности. Мы очень стараемся идти против стереотипов и доказать обществу то, что в нашей стране могут быть потрясающие ИТ-решения, с помощью которых можно эффективно и сравнительно легко производить полноценное импортозамещение. Мы практически не сталкиваемся с теми, кто готов переходить на какие угодно решения, лишь бы российские. Типичный заказчик не готов терять абсолютно ни в чём. Поэтому мы в компании UserGate свою задачу видим в предоставлении заказчику не просто российского решения, а превосходящего российского решения.

по Kerberos, NTLM, SAML, в том числе с поддержкой MFA.

Технологию VPN платформа UserGate позволяет использовать как для удалённого подключения клиентских пользовательских устройств, так и для создания защищённых туннелей между NGFW-серверами UserGate. Для создания туннелей используется протокол Layer 2 Tunneling Protocol (L2TP), а для защиты передаваемых данных — протокол IPsec.

В режиме VPN-сервер для «удалённого» доступа клиентов (Remote access VPN) шлюз UserGate выступает как VPN-сервер, а пользователи других устройств — как клиенты.

При необходимости же использования канала VPN для защищённого соединения офисов (Site-to-Site VPN) один из шлюзов UserGate выступает как сервер, а другой как клиент. С помощью такого подключения разобщённые офисы компании объединяются в логическую сеть. Такое объединение сокращает затраты ресурсов и упрощает применение единых настроек для обеспечения безопасности в сетях филиалов.

Система анализа событий и инцидентов ИБ на основе UserGate Log Analyzer. Взрывное апрельское расширение числа удалённых сотрудников и предоставление возможностей работы с корпоративными ресурсами большему числу сторонних пользователей (партнёров, исполнителей и т.п.) привело к повышению требований в части анализа событий и инцидентов информационной и кибербезопасности.

В составе платформы UserGate возможности такого анализа упрощаются при использовании устройств UserGate Log Analyzer, специализированных анализаторов событий и инцидентов в ИТ-инфраструктуре. Компания предлагает в этой нише модели E6; E14; F25, число в шифре модели указывает на объём хранилища данных в ТБ. Очевидно, что этим обеспечиваются возможности масштабирования агрегации данных, связанных с анализом инцидентов безопасности, а также расширение возможностей мониторинга событий «вглубь» по временной шкале.

Специализированный сервер-анализатор UserGate Log Analyzer развёртывается отдельно от шлюзов безопасности NGFW UserGate, позволяя снизить нагрузку на межсетевые экраны и обрабатывать большой объём данных (Log Analyzer может агрегировать данные с нескольких NGFW-серверов и со сторонних устройств по SNMP-протоколу). При этом разделение функций обработки трафика и анализа данных повышает надёжность системы.

Говоря о надёжности, уместно отметить также, что оборудование UserGate поддерживает технологию кластеризации для обеспечения режима «высокой готовности» (High Availability), а в ряде моделей поддерживается технология «горячей» замены дисковых массивов.

На основании переданных в UserGate Log Analyzer данных осуществляется «глубокий анализ» произошедших событий безопасности, определяются и отслеживаются

подозрительные активности отдельных пользователей или хостов.

Программное обеспечение UserGate Log Analyzer содержит готовые шаблоны отчётов по ряду категорий: captive-портал, системные события, система обнаружения вторжений (COB), сетевая активность, веб-портал, трафик, веб-активность.

Отчёты категории COB предоставляют детальную информацию об атаках (определяются «топы» IP-адресов источников атак и протоколов, используемых в атаках, а также «цели» атакующих / IP-адреса хостов). Можно также получить информацию по используемым устройствам и «топ» сигнатур устройств.

Секция отчётов по событиям включает информацию об авторизации через консоль, сводный отчёт действий администраторов, изменений конфигураций по компонентам и отчёт о системных событиях по степени критичности.

Использование отчётов из различных категорий позволяет выявить потенциальные угрозы на основе анализа произошедших событий. Модуль UserGate Log Analyzer позволяет сопоставить результаты отчётов с установленными параметрами и обеспечить соответствие инфраструктуры требованиям корпоративной политики безопасности.

Сформированные отчёты могут автоматически отправляться по электронной почте администратору и другим уполномоченным лицам по расписанию, в требуемое время и указанный день недели.



Илья ОСАДЧИЙ
директор по развитию
бизнеса, «Тайгер Оптикс»



Виктор СЕРДЮК
генеральный директор
АО «ДиалогНаука»

SILVERFORT ЗАЩИЩАЕТ... НЕЗАЩИЩАЕМОЕ

БЕЗОПАСНАЯ
МНОГОФАКТОРНАЯ
АУТЕНТИФИКАЦИЯ
В ИЗОЛИРОВАННЫХ
КОРПОРАТИВНЫХ СЕТЯХ

ЧТО ТАКОЕ ИЗОЛИРОВАННАЯ СЕТЬ?

Сети, изолированные по принципу «воздушного зазора» (air-gapped), — это компьютерные сети, у которых физически нет интерфейсов для подключения к внешнему миру. Очевидно, что это достаточно радикальная мера обеспечения безопасности, поэтому такой подход обычно применяется в организациях с крайне чувствительными ресурсами, которым необходим максимальный уровень защиты.

Например, изолированные сети могут использоваться компаниями, являющимися субъектами КИИ (например, сети АСУ ТП в компаниях ТЭК или промышленности), а также организациями,

в которых работают со сведениями, составляющими государственную тайну (подрядчики Министерства обороны, государственные структуры, вооружённые силы и др.). Обычно эти организации полностью изолируют свои наиболее критичные сегменты сети, благодаря чему они, по крайней мере в теории, отрезаны от любых интернет-подключений.

В РЕАЛЬНОСТИ ИЗОЛИРОВАННЫЕ СЕТИ НЕ ТАК БЕЗОПАСНЫ, КАК КАЖЕТСЯ

Описанная выше концепция хорошо выглядит в теории, но на практике эти сети гораздо менее изолированы, чем предполагают их владельцы. В большинстве

случаев всё же есть необходимость периодического подключения к внешнему миру. Например, может потребоваться передать в защищённый сегмент сети файлы извне для работы или обновить ПО с помощью USB-накопителя. Кроме того, для некоторого оборудования или ПО в изолированной сети может потребоваться диагностика или тех. поддержка со стороны вендора, который может подключаться только удалённо через сеть Интернет. Все эти примеры показывают, что, по сути, сеть уже не полностью изолирована от внешней среды. Хорошо известна история с вредоносным кодом Stuxnet, который проник в изолированные сети через заражённые съёмные USB-носители.



ЗНАЧИТ, В ИЗОЛИРОВАННЫЕ СЕТИ ВСЁ-ТАКИ МОЖНО ПРОНИКНУТЬ

Оказавшись внутри изолированной сети, злоумышленники могут начать латеральное (внутреннее) движение, чтобы продвинуться ближе к информационным ресурсам, представляющим интерес для нарушителей. Это, например, осуществляется с помощью украденных паролей и учётных записей. Так, в 2017 году при атаках NotPetya злоумышленники использовали известный инструмент Mimikatz, причём этот метод распространения работал не только в ИТ-сетях с выходом в Интернет, но и в изолированных сегментах АСУ ТП.

Таким образом, изолированные сети вовсе не столь безопасные, как может показаться. Такой подход к обеспечению защиты мог казаться надёжным в прошлом, но современные угрозы и способы реализации атак показали, что изоляция сетей не обеспечивает их непроницаемости и защищённости, и этот риск необходимо учитывать.

ТРУДНОСТИ ЗАЩИТЫ ИЗОЛИРОВАННЫХ СЕТЕЙ

Как правило, изолированные сети содержат особо ценные ресурсы, поэтому организации с такими сетевыми сегментами остро нуждаются в гарантии того, что изолированные сети действительно защищены не только от угроз

внешнего мира, но и от злоумышленника, которому удалось закрепиться внутри сети. Проблема заключается в том, что достичь этого нелегко.

Многие изолированные сети содержат критичные системы, которые должны стабильно работать и быть доступны круглосуточно 365 дней в году, поэтому их нельзя перезапускать для установки обновлений ПО или патчей. На другие проприетарные системы распространяются жёсткие гарантийные условия вендора, по которым на серверах нельзя устанавливать какое-либо стороннее ПО. Кроме того, в этих сетях можно часто обнаружить устаревшие, но до сих пор активные системы, хотя они уже не поддерживаются своими производителями. Обычно это означает, что эти системы больше не поддерживаются и производителями средств защиты информации. Таким образом, развёртывание программных агентов для защиты систем в изолированных сетях часто невыполнимая задача.

Критичные системы должны быть стабильны и доступны, поэтому организациям также необходимо учитывать, как использование средств защиты будет влиять на скорость и стабильность работы приложений и устройств в изолированной сети. Если средство защиты генерирует слишком много ложных срабатываний или, что ещё хуже, блокирует легитимные процессы, то оно крайне негативно влияет на работу защищаемой системы. В этой ситуации решения для многофакторной аутентификации (МФА) обладают преимуществом, так как они не только предоставляют два варианта — разрешить или запретить доступ, но и позволяют пользователям самим подтвердить легитимные запросы доступа без привлечения службы поддержки или администраторов безопасности. Следовательно, это снижает количество ложных срабатываний, оптимизирует процессы и минимизирует количество прерываний в работе пользователей.

Однако сегодня многие средства защиты информации, особенно решения для аутентификации, требуют подключения к сети Интернет. Очевидно, что из-за этого они не подходят для изолированных сетей. В итоге остаётся не так уж много вариантов для

Уникальная инновационная архитектура решения позволяет организациям использовать многофакторную аутентификацию на любых системах

должной защиты таких сетей, и зачастую безопасность большинства изолированных сред не обеспечивается должным образом.

ТРЕБОВАНИЯ К БЕЗОПАСНОЙ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ В ИЗОЛИРОВАННЫХ СЕТЯХ

Как уже упоминалось выше, многофакторная аутентификация (МФА) — крайне важное средство защиты информации, позволяющее предотвратить несанкционированный доступ. Однако оно должно соответствовать жёстким требованиям изолированных сетей.

Для защиты изолированных сетей нужны решения, обладающие следующими свойствами:

- ♦ возможность работы без подключения к Интернету;
- ♦ отсутствие необходимости использования агентов и изменения кода приложений, так как зачастую развернуть агенты или изменить код невозможно для высокодоступных, устаревших или сторонних систем;
- ♦ минимальное количество прерываний в работе и отсутствие негативного влияния на стабильность и доступность критических систем и процессов;
- ♦ решения для безопасной аутентификации в изолированных сетях должны предоставлять аппаратные токены, которые считаются наиболее безопасными и могут использоваться там, где использование личных телефонов запрещено.

Из соображений безопасности и из-за отсутствия подключения к Интернету в изолированных сетях вместо мобильных устройств для аутентификации часто используются аппаратные токены. Токены с поддержкой стандарта аутентификации FIDO2 считаются более безопасными, чем устаревшие OTP-токены, которые можно украсть или потерять, к тому же они уязвимы к атакам типа «человек посередине». Из-за этого FIDO2 является предпочтительным

стандартом, применяемым в аппаратных токенах. Также считается, что токен FIDO2 исключает реализацию как новейших, так и традиционных фишинговых атак.

Однако возможности токенов FIDO2 изначально ограничены. Дело в том, что для их использования нужны защищённые приложения, которые бы применяли поддерживающие их протоколы webauthN или U2F. Очень сложно, если вообще возможно, вносить изменения в защищаемые системы, чтобы они могли поддерживать эти протоколы, поэтому с такими токенами может работать небольшое число приложений.

РАСШИРЕННЫЕ ВОЗМОЖНОСТИ БЕЗОПАСНОЙ АУТЕНТИФИКАЦИИ В ИЗОЛИРОВАННЫХ СЕТЯХ С ПОМОЩЬЮ РЕШЕНИЙ SILVERFORT

С момента своего появления Silverfort помогает организациям любых типов защищать активы, которые долго считались незащищаемыми, например ИТ-инфраструктура, файловые серверы, базы данных, устройства IoT и даже системы АСУ ТП, такие как человеко-машинные интерфейсы (HMI) и производственные серверы. Недавно Silverfort расширил свои возможности по обеспечению безопасной аутентификации на изолированные сети, предоставляя полностью локальное развёртывание, при котором не нужны интернет-соединения, программные агенты на серверах или изменения кода в системах, находящихся под защитой. В качестве второго фактора используются аппаратные токены FIDO2.

1. Новый режим развёртывания без подключения к Интернету: начиная с версии 3.0, Silverfort предоставляет режим полностью локального развёртывания. В этом режиме Silverfort работает как виртуальная машина и предоставляет полную функциональность, не вызывая сторонних функций.

Silverfort также поддерживает вариант SaaS-развёртывания и гибридного развёртывания в облаке и на площадке заказчика.

2. Безагентная архитектура, не требующая менять код: уникальная инновационная архитектура решения позволяет организациям использовать многофакторную аутентификацию на любых системах или ресурсах, без программных агентов на защищаемых серверах, а также без изменения кода или внедрения новых протоколов аутентификации.

3. Аппаратные токены, совместимые с FIDO2: Silverfort предоставляет организациям выбор поставщика аутентификатора для изолированных сред, обеспечивая гибкую интеграцию с поддержкой всех аппаратных токенов FIDO2.

Благодаря такой интеграции можно «бесшовно» закрывать технологический разрыв между современными токенами FIDO2 и существующей инфраструктурой предприятий, позволяя заказчикам использовать безопасные аппаратные токены без внесения изменений в инфраструктуру или приложения.

Благодаря инновации Silverfort многофакторную аутентификацию можно применять для защиты систем в изолированных сетях, не внося изменения в саму сеть, не используя пакеты разработчиков (SDK), агенты или прокси-серверы. Многофакторная аутентификация позволяет не только проверять подлинность пользовательских учётных записей, но и предотвращать дальнейшее движение злоумышленника внутри сети, если он смог туда проникнуть.

ЗАКЛЮЧЕНИЕ

В организациях с крайне чувствительными ресурсами изоляция сети может стать правильным выбором для её защиты — но только в том случае, если компании осознают и компенсируют слабые места, которые присущи таким средам. Благодаря безагентной платформе Silverfort заказчики могут усилить безопасную аутентификацию, проверяя подлинность пользовательских учётных записей в изолированных сетях, что добавляет необходимые компенсирующие защитные меры и обеспечивает непрерывную защиту доступа к наиболее критичным активам.

POSITIVE HACK DAYS: 20-21 МАЯ

THE STANDOFF: 18-21 МАЯ



THE STANDOFF

Партнер форума

POSITIVE HACK DAYS 10: НАЧАЛО

Реклама

Это случится снова: крупнейший форум по практической кибербезопасности Positive Hack Days в десятый раз соберет на одной площадке энтузиастов и звезд из мира ИТ и ИБ. Партнером форума в этом году станет The Standoff.

Два дня докладов, горячих дискуссий, мастер-классов от ведущих экспертов в сфере исследования безопасности и конкурсов по анализу защищенности систем и технологий, а также по поиску уязвимостей, уже ждут своих посетителей.

Грандиозная битва red & blue teams развернется на киберполигоне The Standoff — в цифровом двойнике современного мегаполиса. Ее участники в безопасной среде изучат возможности реализации кибератак на город и оценят масштабы их последствий.

Только здесь собираются белые хакеры и ИБ-специалисты крупнейших компаний со всей планеты, представители интернет-сообщества и госструктур, регулирующих организаций, политики, деятели науки и искусства — чтобы вместе формировать безопасное цифровое будущее. Присоединяйтесь и вы!

Открыта регистрация СМИ.

E-mail для заявок: ysorokina@ptsecurity.com

Билеты уже в продаже



**HYATT
REGENCY**
MOSCOW PETROVSKY PARK

phdays.com

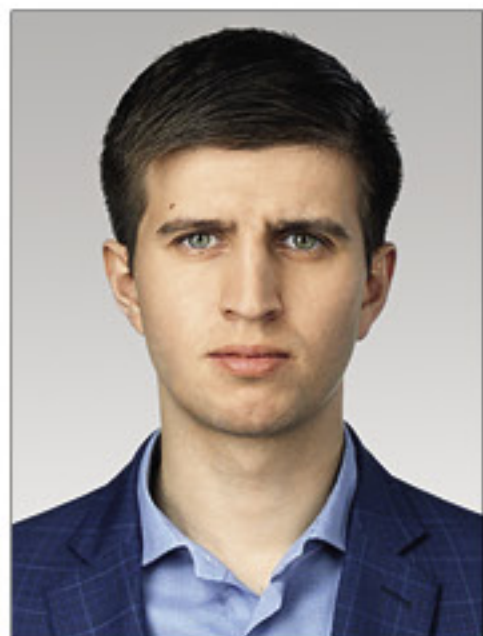
[#PHDays](https://twitter.com/PHDays)



twitter.com/phdays_ru



facebook.com/PHDays



Алексей КУЗНЕЦОВ
руководитель направления
анализа защищённости
BI.ZONE

УПРАВЛЕНИЕ ПОВЕРХНОСТЬЮ АТАКИ

ЦИФРОВЫЕ АКТИВЫ БАНКОВ ВСЁ ЧАЩЕ
РАСПОЛАГАЮТСЯ НА ВНЕШНЕМ ПЕРИМЕТРЕ —
ЗА ПРЕДЕЛАМИ КОНТРОЛЯ СЛУЖБ БЕЗОПАСНОСТИ

Периметр компании из контролируемого монолита трансформировался в живой организм, который меняется практически в режиме реального времени. В связи с этим уже недостаточно подхода в виде глухой обороны периметра, его чёткого определения и разграничения доступа. Особенно это стало заметно в период карантина, когда большинство организаций перешли на работу из дома и раскрутили гайки на внешнем периметре, чтобы предоставить удалённый доступ сотрудникам.

В этих условиях нужно менять подход к контролю периметра, основываясь на определении «поверхности атаки» (attack surface). Под этим словосочетанием мы понимаем совокупность цифровых активов, которые злоумышленники могут рассматривать в качестве целей своих атак: это любые внешние серверы, ПО, облачные сервисы и другие активы, которые обрабатывают конфиденциальные данные.

ОПРЕДЕЛЕНИЕ ПОВЕРХНОСТИ АТАКИ

Определение поверхности атаки — сложная задача, с которой иногда не справляются даже специалисты в таких зрелых организациях, как Microsoft. Так,

в марте 2020 года из-за простых ошибок конфигурации DNS-серверов 670 доменов третьего уровня подверглись риску взлома¹.

В финансовых компаниях подобных потенциальных точек входа, которые необходимо контролировать, — десятки.

При этом многие компании не имеют полного представления о том, какие ресурсы находятся на их периметре, поэтому не могут оценить поверхность атаки. Даже если на первый взгляд все критически значимые системы защищены, на внешний периметр может попасть административная панель управления контейнеризацией без аутентификации. Это может привести к проникновению злоумышленника в корпоративную сеть и другим негативным последствиям.

Избежать таких проблем поможет инвентаризация цифровых активов, которая является первым шагом в процессе определения поверхности атаки.

К таким активам на внешнем периметре относятся:

- ♦ веб-приложения и серверная часть мобильных приложений;
- ♦ облачные и сетевые хранилища данных;
- ♦ доступные извне сервисы (например, используемые контрагентами

FTP-серверы, на которых хранятся документы компании).

Также существует класс рисков, связанных с использованием сотрудниками личных устройств для работы, но меры защиты в этом случае будут совсем другими, поэтому в данной статье мы их не рассматриваем.

Источниками рисков могут стать не поддерживаемые системы и приложения, отказаться от которых в данный момент нельзя. К подобным активам следует ограничить доступ так, чтобы обращаться к ним мог минимальный круг лиц.

Такой подход позволит избежать пробелов при определении поверхности атаки.

АНАЛИЗ ЗАЩИЩЁННОСТИ ЦИФРОВЫХ АКТИВОВ

Традиционный подход: регулярный анализ защищённости периметра. После инвентаризации хорошей практикой будет составить риск-профиль: классифицировать все активы, выделить наиболее важные, оценить связанные с ними угрозы и уязвимости. Необходимо назначить сотрудников, ответственных за контроль состояния каждой группы или каждого типа активов.

В финансовой отрасли наиболее простые для злоумышленника точки

¹ <https://www.securitylab.ru/news/505618.php>

входа — серверные части приложений, веб-приложения и другие доступные извне сервисы финансовых организаций, поэтому при анализе защищённости следует сосредоточиться именно на них.

По нашим данным, веб-приложения составляют более 40 % внешнего периметра, при этом 72 % приложений в финансовом секторе имеют низкий уровень защищённости. Кроме того, оставляет желать лучшего уровень защищённости внешней инфраструктуры, который остаётся низким в 46 % финансовых учреждений.

Низкий уровень защищённости характерен для ситуаций, когда за разные компоненты приложения отвечают разные команды. В результате в процессе эксплуатации возникают серые зоны, где ответственность за кибербезопасность размыта, а некоторые аспекты вообще остаются без внимания специалистов. Часто это приводит к возникновению уязвимостей, связанных с небезопасной конфигурацией веб-приложений или используемых сторонних компонентов.

PCI DSS и положение Банка России № 382-П требуют от компаний, обрабатывающих данные платёжных карт, проводить тестирование на проникновение ежегодно. Однако, по нашим данным², в компаниях, которые уже три года проводят ежегодное тестирование на проникновение, количество уязвимостей не уменьшается, а остаётся на прежнем уровне. За то время, пока службы безопасности нейтрализуют старые бреши в безопасности, успевают появиться новые.

Процессный подход: непрерывный контроль изменений на периметре. Разовые пентесты лишь временно повышают уровень защищённости, но не помогают выстроить процесс и обеспечить непрерывное управление поверхностью атаки. В связи с этим в нашей отрасли по всему миру наблюдается тренд на процессный подход и непрерывный поиск уязвимых активов. Ведущее аналитическое агентство Gartner с 2018 года рекомендует специалистам по защите

Внешние специалисты, которые постоянно занимаются анализом защищённости и тестированием на проникновение, имеют более широкий взгляд на безопасность за счёт богатого опыта и разнообразия кейсов

информации постоянно проводить мониторинг внешнего периметра и оценивать изменения в нём. Это действительно важно, но очень трудозатратно: необходимо сочетать автоматизацию поиска уязвимых активов и экспертную обработку полученных результатов. На втором этапе работ иногда требуется привлекать целую команду специалистов.

Для безопасного развития бизнеса в таких условиях мы создали сервис непрерывного мониторинга внешнего IT-периметра (СРТ — Continuous Penetration Testing). Данный сервис позволяет отслеживать любые изменения на периметре, такие как появление новых активов или обновления в старых, а также проводить точечное тестирование на проникновение.

ПРЕИМУЩЕСТВА НЕПРЕРЫВНОГО КОНТРОЛЯ ИЗМЕНЕНИЙ НА ПЕРИМЕТРЕ ПРИ УПРАВЛЕНИИ ПОВЕРХНОСТЬЮ АТАКИ

Непрерывный контроль периметра финансовых организаций с использованием сервисов автоматизированного пентеста повышает эффективность управления поверхностью атаки. Важно отслеживать любые изменения на периметре: появление новых точек входа, изменение конфигураций отдельных активов. Такой подход позволяет не только постоянно мониторить защищённость активов, но и сокращать время жизни уязвимостей.

Благодаря СРТ можно получить более полную картину состояния периметра. Внешние специалисты, которые постоянно занимаются анализом защищённости и тестированием на проникновение, имеют более широкий взгляд на безопасность за счёт богатого опыта и разнообразия кейсов. Со стороны проще заметить неочевидные

уязвимые активы, имитируя действия злоумышленника.

СРТ подразумевает непрерывную проверку периметра на наличие забытых активов: серверов с устаревшим и уязвимым ПО, доменов, ведущих на IP-адреса, которые уже не принадлежат организации. За счёт этого минимизируются цифровые риски: снижается вероятность атаки и нанесения ущерба. Для компаний в финансовом секторе это особенно важно, ведь их IT-инфраструктура открывает путь к денежным средствам клиентов.

Также СРТ помогает снизить издержки, связанные с содержанием собственной команды.

Наконец, эксперты вручную обрабатывают отчёты и отслеживают изменения на периметре. Таким образом отсеиваются ложные срабатывания и уязвимости, которые не могут использоваться злоумышленниками, и удаётся более точно определить реальную поверхность атаки и найти бреши в безопасности без высоких расходов.

* * *

Итак, управление поверхностью атаки — задача, которая особенно актуальна для финансовой отрасли, расположенной в самом начале списка целей киберпреступников. Чтобы решить её, нужно обеспечить непрерывный контроль изменений на периметре. Такой подход позволит бизнесу ставить более чёткие задачи и направлять силы специалистов по анализу защищённости на обнаружение наиболее важных уязвимостей. В то же время компании смогут действовать на опережение и избегать неожиданных инцидентов безопасности, ведь бреши в инфраструктуре будут устраняться быстрее, чем ими успеют воспользоваться злоумышленники.

² https://bi.zone/upload/for_download/Threat-Zone_Report_2020_RU.pdf



Елена ВЕРЕЩАГИНА
генеральный директор
ООО «СМАРТС-Кванттелеком»

ДРУГОЕ ШИФРОВАНИЕ

БЕСЕДЫ О КВАНТОВЫХ КОММУНИКАЦИЯХ¹

Большинство найденных редакцией по «квантовой» теме статей числят ООО «СМАРТС-Кванттелеком» среди компаний, развивающих рынок «квантовых коммуникаций», причём помещают её когда в тройку лидеров, а когда и на первое место. Например: «В России прототипы квантовых сетей с доверенными узлами построили только две организации: Университет ИТМО — совместно с КНИТУ-КАИ — в Казани, и с „Открытым кодом“ — в Самаре, а также РКЦ — совместно с „Газпромбанком“».

Тут стоит пояснить. Компания «СМАРТС-Кванттелеком» была учреждена в 2014 году выходцами из Университета ИТМО (Санкт-Петербург) и никогда не прекращала тесного сотрудничества с ИТМО в научной, внедренческой и образовательной сферах в области технологий квантовых коммуникаций вообще и квантового распределения ключей шифрования (КРК) в частности. Поэтому-то в ряде публикаций авторы и не вдаются в формальные детали кооперативных связей при осуществлении конкретных проектов.

По просьбе BIS Journal роль проводника по лабиринтам понятий, недомолвок и недоговорённостей сферы «квантовых коммуникаций» на этот раз любезно согласилась исполнить генеральный директор ООО «СМАРТС-Кванттелеком» Елена Верещагина. Скромность интервьюируемой компании нам удалось преодолеть вопросом: что же позволило компании стать одной из двух организаций, упомянутых в приведённой выше цитате? На который был получен следующий ответ:

«Работа «СМАРТС-Кванттелеком» корнями уходит в разработанный Университетом ИТМО подход кодирования квантовой информации в боковые частоты модулируемого излучения. Эффективность подхода показана в ряде

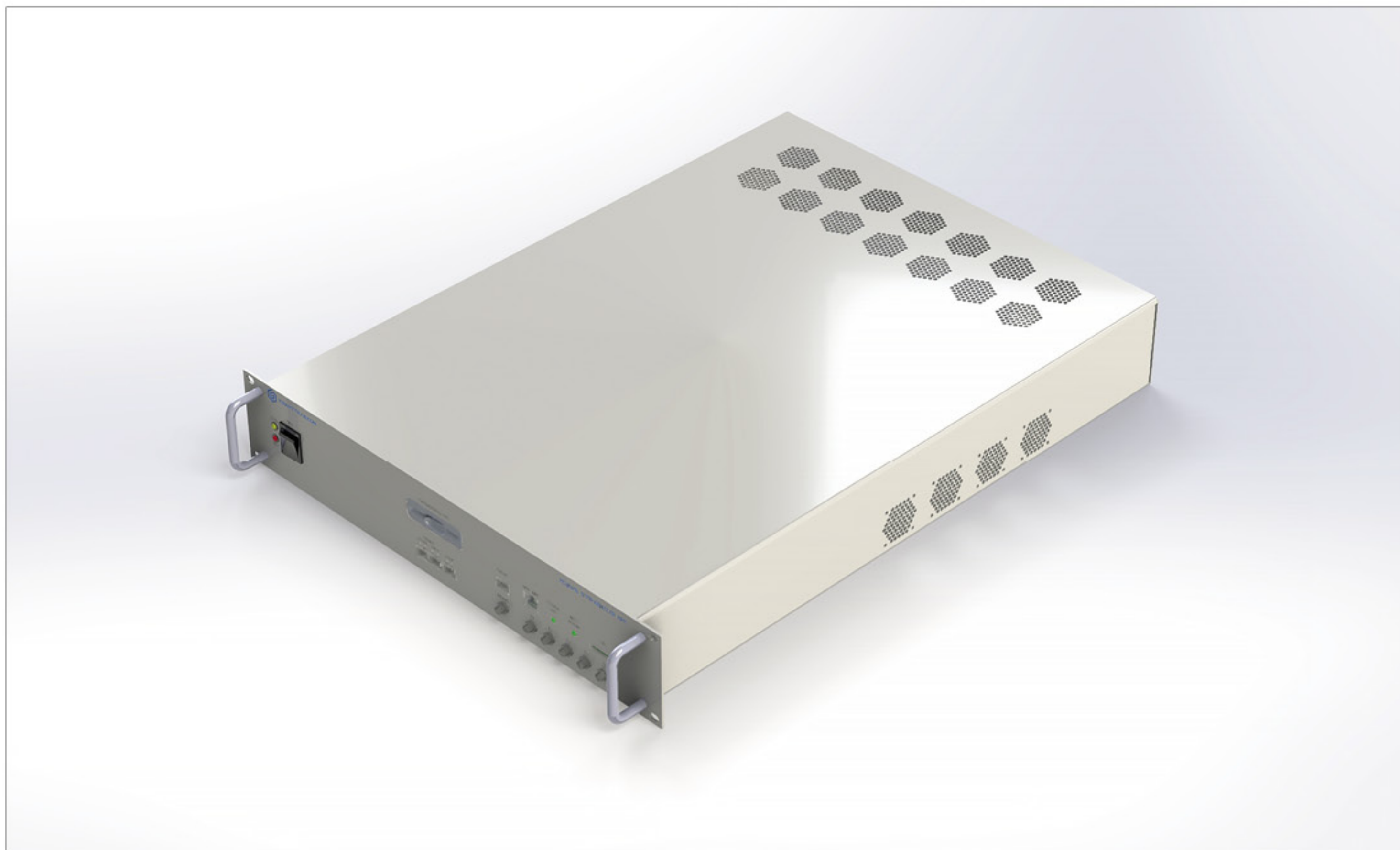
работ, описывающих реализацию нескольких различных протоколов КРК. Здесь же следует отметить, что большая работа была проделана в части теоретического анализа секретности, суть которого была во введении только адекватных и чётких технических ограничений, в то время как описания многих современных протоколов КРК и систем, на них базирующихся, могут быть сформулированы достаточно нечётко (например, вышеупомянутый подход decoy state). Таким образом, конечная система КРК компании Кванттелеком может быть успешно использована в контексте квантовых сетей».

На наш взгляд, мы получили исчерпывающий ответ, который ещё больше повысил наше доверие к компании «СМАРТС-Кванттелеком» как партнёру, готовому открыто, не растекаясь мыслью по древу, раскрывать тайны своей профессии.

Уместно при этом отметить, что единственными «недостатками» приведённого ответа можно назвать употребление аббревиатуры КРК без её расшифровки и англицизм «подход decoy state». Но аббревиатура КРК (квантовое распределение ключей [шифрования]) уже расшифровывалась в предыдущей публикации в первом номере BIS Journal, а понятие, кроющееся за нерусскими словами decoy state, как следует из стилистики ответа, уже обсуждалось на ранней стадии беседы.

После этой преамбулы нам остаётся только добавить, что одним из «крайних» дел «СМАРТС-Кванттелеком» на ниве квантовых коммуникаций стало участие в строительстве опытной магистральной квантовой сети вдоль железной дороги между Москвой и Санкт-Петербургом общей протяжённостью более 800 км. Проект разработан специалистами ОАО «РЖД» совместно с научными и производственными организациями страны, в нём заняты ведущие эксперты Университета ИТМО и компании «СМАРТС-Кванттелеком».

¹ Начало в BIS Journal № 1(40) / 2021, «Бизнес-ветвь потомков Ландавшица»



Модуль отправителя КРК

ВОПРОС-ОТВЕТ

BIS Journal. В открытой печати встретилось следующее утверждение: «Фактически под термином «квантовая криптография» понимают метод конфиденциального квантового распределения криптографических ключей (КРК) (QKD — Quantum Key Distribution) между участниками сети, когда линия или сеть КРК решает задачу доверенного «курьера» по доставке секретных ключей абонентам...» В связи с этим вопрос: технологии квантовых коммуникаций (ТКК) и квантовые технологии шифрования (КТШ) — это синонимы или КТШ — это часть ТКК? Квантовые технологии шифрования — это что? Только квантовое распределение ключей [шифрования], передача этих ключей по каналам связи? Или КТШ — это ещё и сами процедуры шифрования / дешифрования и передачи/приёма зашифрованных сообщений?

«СМАРТС-Кванттелеком». ТКК — представляют собой набор методов передачи квантовых состояний от отправителя к получателю. КРК — методы формирования ключей между

сторонами, гарантия безопасности которых обеспечивается свойствами квантовых состояний. После процесса распределения ключей легитимные пользователи могут использовать классические технологии шифрования для закрытия конфиденциальной информации.

BIS Journal. В открытой печати встретилось утверждение о том, что «...для поддерживаемых технологий и в мире и в России отмечается максимальный, девятый, уровень TRL. Речь идёт об интеграции КРК с классическим шифратором, образовательных решениях, квантовом генераторе случайных чисел, классической постобработке квантовых ключей и детекторе одиночных фотонов». Что стоит за понятием уровня готовности технологий квантовых коммуникаций (TRL), измеряемых, вроде бы, отметками от 1 до 9? Девятка — это наличие коммерческого оборудования «на полках» или готовность документации для производства оборудования?

«СМАРТС-Кванттелеком». Есть документация, опытный образец, технология готова к производству.

BIS Journal. В открытой печати встретилось следующее утверждение: «В большинстве магистральных оптоволоконных сетей применяется мультиплексирование по длине волны. Наличие классического сигнала в одной жиле оптоволокна создаёт засветки для квантового сигнала. Решением может быть как выделение тёмного волокна, так и мультиплексирование по времени, а также развитие методов оптической фильтрации для квантово-классического xWDM мультиплексирования. С этой точки зрения очень перспективным является КРК на непрерывных переменных». «Классический сигнал» — это синоним слов «оптический сигнал» и это не «квантовый сигнал»? Какие простые аналогии можно было бы подобрать для подчёркивания различий между «классическим» и квантовым сигналами? Что такое КРК на «непрерывных переменных»?

«СМАРТС-Кванттелеком». Оба сигнала — и «классический» и «квантовый» — являются оптическими. Вся разница заключается в их интенсивности. У классического сигнала обычно

	ИТМО	Альфа	Браво
Скорость генерации просеянного ключа, бит/с	7 200	2 000	
Скорость генерации секретного ключа, бит/с	600	400	10
QBER, %	4,6 %	5 %	7–8 %
Поддержка буфера для хранения ключей	Да	Да	Нет
Квантовый генератор случайных чисел	Нет	Нет	Да
Используемый протокол КРК	Фазовый на боковых частотах	BB84 decoy state	Собственная разработка
Детектор фотонов	Импортный	Собственная разработка	Собственная разработка
Поддержка стороннего СКЗИ	Да	Да	Нет

Таблица 1. Сравнение достижений, сделанных в стенах ИТМО, с достижениями конкурентов

высокая интенсивность (среднее число фотонов в импульсе/временном отрезке высокое), под квантовым излучением в данном контексте принято считать излучение по интенсивности близкое к однофотонному уровню энергии.

КРК на непрерывных переменных — отдельный класс протоколов, использующих на приемной стороне когерентное детектирование (гомодинное и гетеродинное детектирование) вместо детекторов одиночных фотонов. При таких методах приёма получатель имеет непрерывный сигнал на выходе приёмного модуля, который должен быть соответствующим образом обработан.

BIS Journal. Как вы можете прокомментировать следующую таблицу сравнения достижений, сделанных в стенах ИТМО, с достижениями конкурентов (таблица 1)?

Встретив такую таблицу, как вы прокомментируете разницу между «Фазовый на боковых частотах» и «Собственная разработка» в строке об используемом протоколе КРК? Как вы прокомментируете плюсы и

минусы протоколов «Фазовый на боковых частотах» и BB84 decoy state? «СМАРТС-Кванттелеком» использует импортный детектор фотонов? Наличие собственных разработок детекторов фотонов — это хорошо или это может привести к удорожанию разработок по сравнению с использованием унифицированного детектора фотонов? Может ли вообще детектор фотонов быть унифицирован для разных ветвей развития оборудования КРК? Что такое QBER? QBER должно быть как можно меньше? Что мешает достичь идеала величины QBER?

«СМАРТС-Кванттелеком». QBER (Quantum Bit Error Rate) — характеризует величину ошибок в квантовом канале, соответственно, чем меньше это значение, тем выше дальность распределения ключа. Величина QBER не может быть полностью нулевой, в том числе из-за неидеальности оптических и электронных компонентов системы КРК.

Комментировать что-либо под названием «собственная разработка» сложно,

под этими словами может скрываться абсолютно всё что угодно, так что сравнение в данном случае выглядит не очень уместным. По поводу протоколов «Фазовый на боковых частотах» и BB84 decoy state можно сказать, что главное их различие заключается в разнице подходов к оценке наиболее опасных атак, из чего следуют все особенности их реализации.

На данный момент в ИТМО и «СМАРТС-Кванттелеком» разработан квантовый генератор случайных чисел. Разработка внедряется в существующую систему КРК.

В настоящее время «СМАРТС-Кванттелеком» использует детектор одиночных фотонов (ДОФ) собственной разработки. Разработка и производство собственных детекторов позволяет снизить стоимость комплекта КРК. Интерфейс ДОФ аналогичен интерфейсам импортных аналогов, имеющих в продаже и использующихся в системах КРК.

Продолжение следует

ВМЕСТО ПРОМЕЖУТОЧНОГО ЭПИЛОГА

Одной из проблем «классической» сферы ИБ является неумение многих профессионалов ИБ разговаривать на понятном языке с пользователями и потребителями услуг защиты информации. Вместо такого, понятного, языка — англицизмы вкупе с «птичьим языком», где пара терминов может содержать смыслы, объяснение которых обычным языком требует

целой страницы или очень точной яркой аналогии. В лице компании «СМАРТС-Кванттелеком» редакция нашла доброжелательного собеседника, готового последовательно разъяснять и помогать понимать нам скрытые смыслы публикаций в откровенно революционной сфере. Что позволит нам всем выйти в эту новую область с ясным пониманием и чётким видением.



Батр АЛЬЧИНОВ
инженер
Департамента
информационной
безопасности
АМТ-ГРУП

УПРАВЛЯЕМ СЕТЕВЫМ ДОСТУПОМ БЫСТРЕЕ И ЭФФЕКТИВНЕЕ

РАСШИРЕНИЕ ВОЗМОЖНОСТЕЙ
ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ
ДОСТУПОМ ЗА СЧЕТ ИНТЕГРАЦИИ
С КОРПОРАТИВНОЙ ИНФРАСТРУКТУРОЙ

В современных организациях ИТ-инфраструктура является одним из столпов, поддерживающих реализацию бизнес-процессов. И скорость выполнения операций по управлению и адаптации конфигурации сетевых устройств к потребностям ИТ-систем оказывает существенное влияние на эффективность работы пользователей.

Например, новому сотруднику из-за ручного процесса выполнения изменений сетевой доступ к необходимым ИТ-ресурсам предоставляется две недели. В итоге, человек всё это время получает зарплату, не делая ничего. Или сотруднику, являющемуся ключевым по проекту, доступ к необходимым ИТ-системам предоставили на неделю позже из-за того, что изменение политик доступа на промежуточных устройствах происходило вручную. Вследствие чего сотрудник не смог выполнить работы вовремя, что повлекло за собой сдвиг сроков проекта, выход за рамки бюджета и т.д.

НЕЗАМЕНИМЫЕ ЕСТЬ

В условиях роста ИТ-инфраструктуры и её изменений предоставление сетевого доступа, особенно в сетях с низким уровнем документирования или при отсутствии такового, становится всё более трудоёмкой задачей, зачастую завязанной на малое количество людей, а иногда и на одного человека. Такие люди становятся неким «центром компетенции», и при их уходе из организации без передачи знаний об устройстве ИТ-инфраструктуры может возникнуть проблема с управлением ИТ-инфраструктурой, что приведёт к

замедлению или прекращению процессов функционирования бизнеса.

Пример. На моей памяти был случай, когда у одного заказчика весь ИТ-отдел уволился в один день. Карт сети, сервисов не было. Очень быстро эта организация сдала позиции в своём сегменте рынка из-за невозможности выполнять прежний объём заказов. И это далеко не единственный случай.

Избежать таких ситуаций, а также помочь абстрагироваться от уровня ручной конфигурации, позволяют системы для централизованного управления сетевым доступом от таких производителей, как Algosec, Tufin, Skybox, Firemon. Стоит отметить, что при интеграции с другими корпоративными ИТ-системами, эффект от их внедрения многократно возрастает.

Конечно, существуют открытые так называемые «opensource» решения, предлагающие именно автоматизацию управления конфигурациями, в частности управление сетевыми устройствами, например, Nornir, Ansible, Puppet, Chef, Salt. Но они предлагают лишь часть того, что есть в системах для централизованного управления сетевым доступом и не являются их полноценными аналогами. Но несмотря на то, что открытые решения бесплатны, стоимость их владения далеко не нулевая.

А ЧТО ПРО ПРОЦЕССЫ?

На определённом уровне зрелости организации возникает необходимость в формализации процесса управления сетевым доступом. Системы для централизованного управления сетевым доступом можно встраивать в эти

процессы, оптимизируя их, делая процессы более гибкими и адаптивными для последующих изменений.

Если процессы, затрагивающие управление сетевым доступом, отсутствуют или находятся на стадии разработки, системы для централизованного управления сетевым доступом могут стать одной из базовых составляющих таких процессов за счёт возможностей по:

- ♦ интеграции с корпоративной инфраструктурой;
- ♦ настройке ролевых моделей согласно процессу управления сетевым доступом;
- ♦ настройке этапности обработки запросов на сетевой доступ согласно процессу;
- ♦ оценке рисков по запрашиваемым доступам (с возможностью использования своих профилей риска);
- ♦ и других возможностей.

Более подробно об основных возможностях систем для централизованного управления сетевым доступом ранее говорилось в статьях моих коллег¹. В данной статье мы сфокусируемся на возможностях интеграции систем для централизованного управления сетевым доступом с корпоративной ИТ-инфраструктурой.

ЗАЧЕМ ЭТО НУЖНО?

Обмен информацией между ИТ-системами и системами для централизованного управления сетевым доступом

¹ «Что? Где? Куда?» (BIS Journal №2 (33) / 2019); «Куда? Кому? Как?» (BIS Journal №3 (34)/2019); «ГОСТ оправдывает средства?! Управление сетевыми устройствами и подсистемами сетевой защиты» (BIS Journal №2 (37)/2020)

даёт максимально полную картину происходящего в ИТ-инфраструктуре, что позволяет более оперативно реагировать на изменения в ней.

Настраиваемое поведение систем для централизованного управления сетевым доступом на основе данных, получаемых от интегрируемых ИТ-систем, дает возможность автоматизировать часть работы сотрудников, позволяя сосредоточиться на более важных для бизнеса задачах.

Пример. До интеграции системы для централизованного управления сетевым доступом и тикет-системы запросы на сетевой доступ обрабатывались вручную в обеих системах. После интеграции через API-вызовы в системе для централизованного управления сетевым доступом запросы создаются, закрываются, изменяют статус автоматически, после получения соответствующих API-вызовов со стороны тикет-системы, что разгружает сотрудников, позволяя не дублировать действия, тем самым снижая трудозатраты.

Подход к управлению ИТ-инфраструктурой с ориентацией на бизнес-приложения в системах для централизованного управления сетевым доступом реализован, например, в модуле AppViz системы ASMS производителя AlgoSec или SecureApp системы TuffinOS производителя Tuffin. Интеграция с этими модулями позволяет абстрагироваться и перейти от уровня ручной конфигурации сетевых устройств к управлению доступом на уровне бизнес-приложений, что снимет с сотрудников часть работы, связанной с поиском устройств, где необходимо корректировать правила и вручную изменять правила сетевого доступа.

Пример. После интеграции с IDM-системой при запросе пользователем доступа к бизнес-приложению, в системе для централизованного управления сетевым доступом создаётся запрос для открытия доступа после получения API-вызова от IDM-системы.

ДОБАВИМ КОНКРЕТИКИ

Интеграция с SIEM/SOAR/IRP. Системы централизованного управления сетевым доступом содержат в себе информацию, которая после определённой фильтрации в SIEM/SOAR/

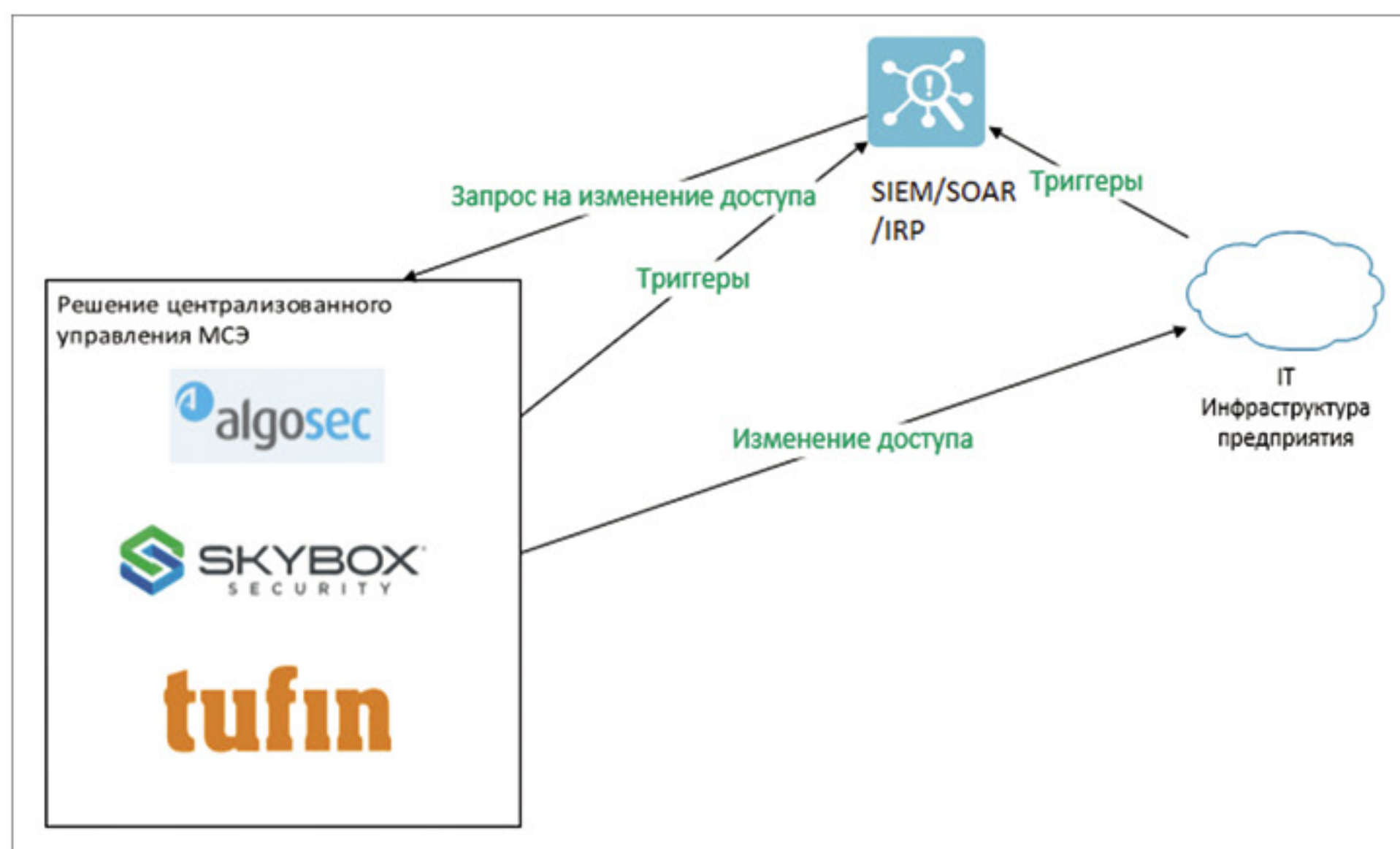


Рисунок 1. Интеграция с SIEM/SOAR/IRP

IRP может дать не только дополнительные триггеры для увеличения вариативности действий при инцидентах ИБ, увеличить прозрачность того, что происходит в инфраструктуре, но и может повысить уровень автоматизации реагирования на инциденты ИБ (рис. 1).

Описание:

- ♦ Информирование SOC о запросах на открытие/изменение/закрытие доступов к business-critical ресурсам до исполнения таких запросов;
- ♦ Отслеживание изменения конфигурации сетевых устройств на предмет соответствия заявленным доступам: например, если изначальный доступ был расширен/сужен/закрыт после выполнения запроса на сетевой доступ;
- ♦ Проверка доступа к/от скомпрометированному хосту или сегменту.

Результат:

- ♦ Проактивная реакция на попытку получения «опасных» сетевых доступов;
- ♦ Возможность автоматической блокировки доступа к/из скомпрометированных сегментов инфраструктуры.

Интеграция со сканерами уязвимостей. Сопоставление информации об уязвимостях на хостах с базой политик МСЭ позволяет определять потенциальные вектора атак (рис. 2).

Описание:

- ♦ Импорт данных об уязвимостях хостов;
- ♦ Визуализация уязвимостей и правил, разрешающих их эксплуатацию.

Результат:

- ♦ Повышение уровня защищённости ИТ-инфраструктуры за счёт оценки рисков открытия сетевого доступа с учётом информации об уязвимостях хостов;
- ♦ Повышение уровня защищённости ИТ-инфраструктуры за счёт учёта уязвимостей хостов при аудите безопасности правил сетевой безопасности.

Интеграция с тикет-системами. Интеграции такого типа не только уменьшают время на операционные задачи в рамках управления сетевым доступом, что позволяет выделять освободившееся время на более приоритетные задачи, но и дают импульс для оптимизации процессов по управлению сетевым доступом (рис. 3).

Описание:

- ♦ Облегчение приведения фактического процесса управления сетевым доступом к регламентному за счёт возможности определения шагов и действий на стадиях обработки запроса на сетевой доступ и назначения ролей для выполнения действий согласно процессу управления запросами на сетевой доступ;
- ♦ Настраиваемые уведомления как в сторону заинтересованных лиц, так и в сторону смежных ИТ-систем, с использованием как почты, так и web API;
- ♦ Возможность отправлять API-вызовы в зависимости от состояния запроса на сетевой доступ, например: автоматическое изменение статуса в одной

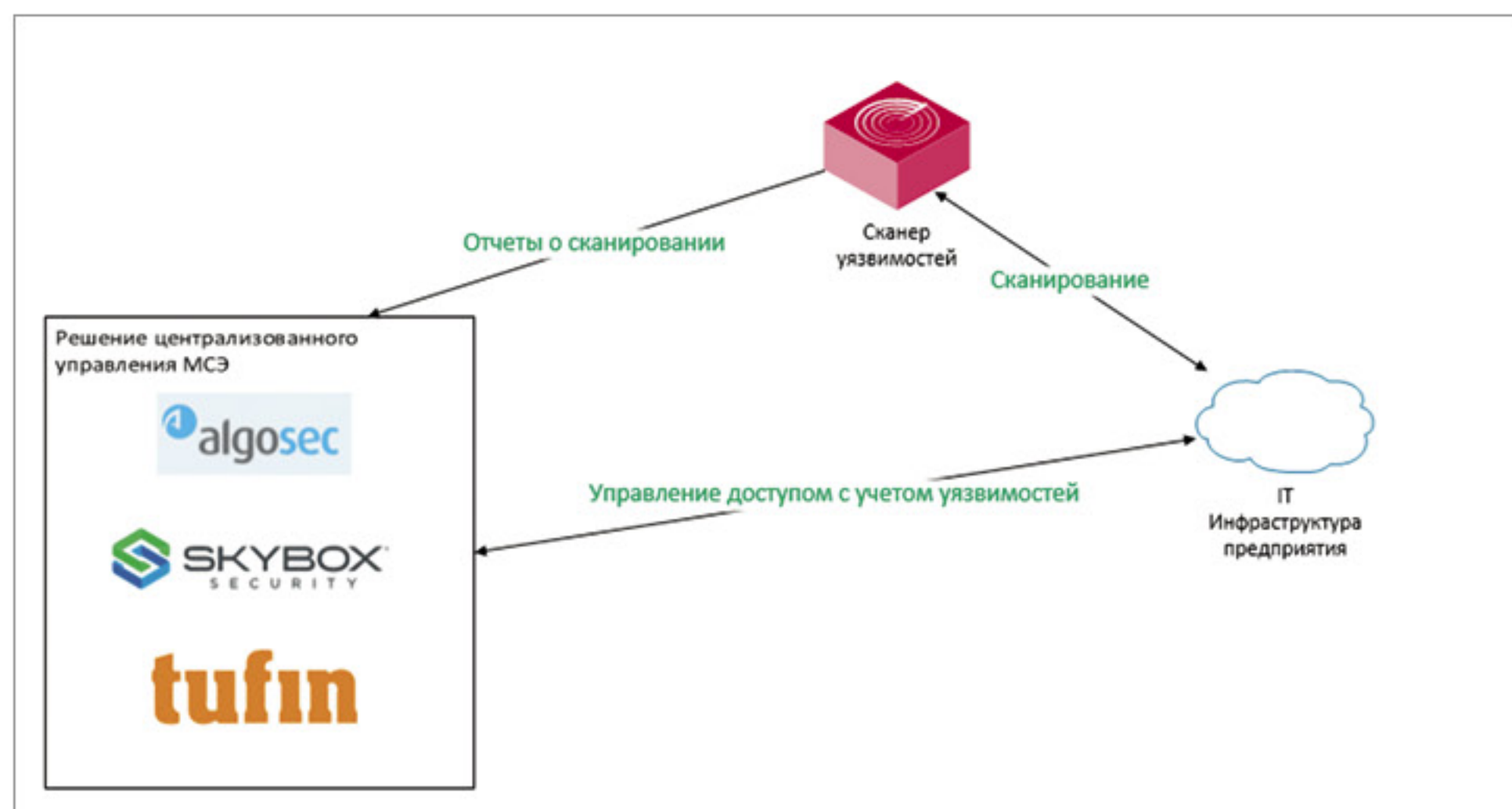


Рисунок 2. Интеграция со сканерами уязвимостей

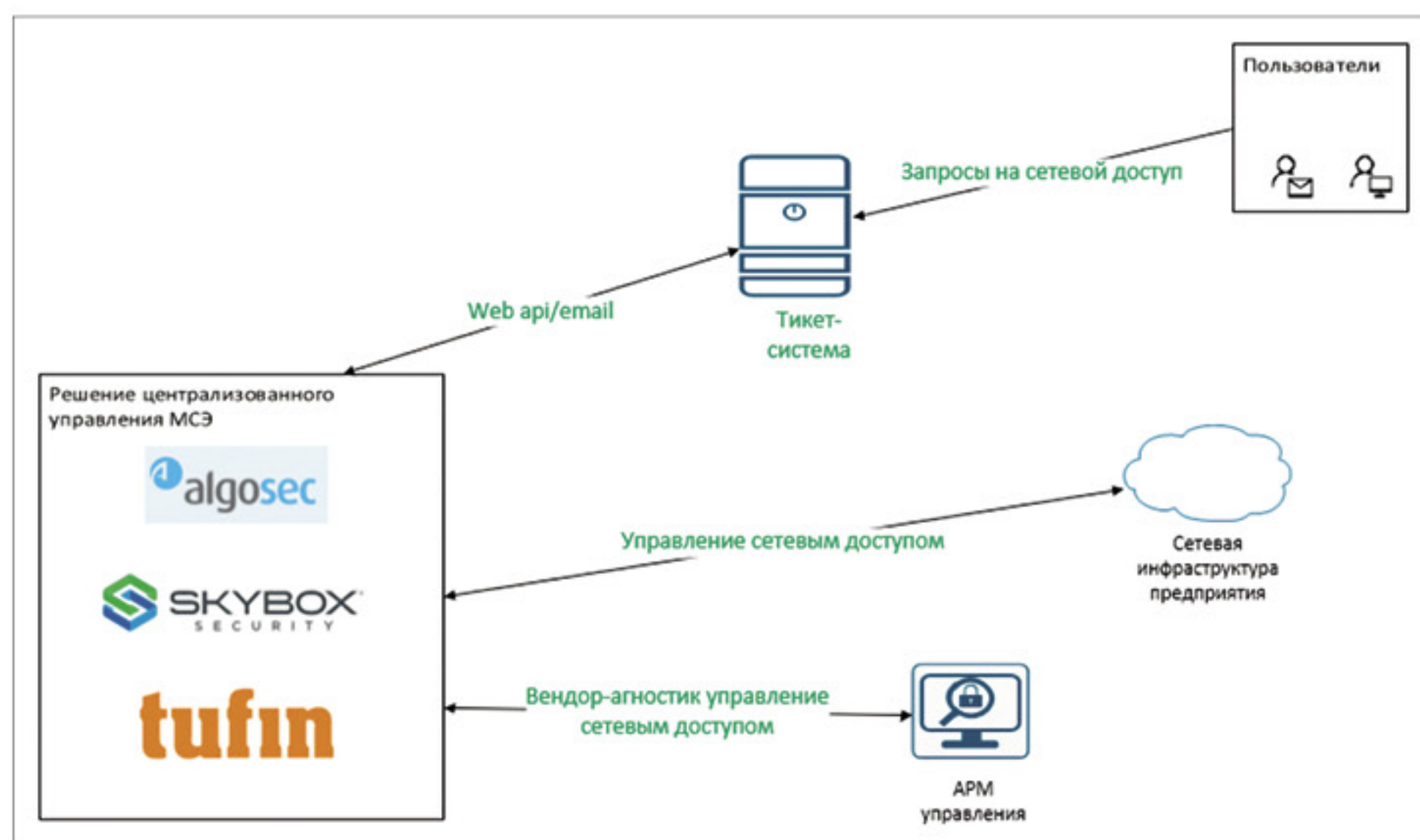


Рисунок 3. Интеграция с тикет-системами

ИТ-системе в зависимости от статуса в другой;

- ♦ Облегчение создания запроса за счёт автоматического считывания файлов, содержащих описание сетевых доступов (под необходимый шаблон заполнения) и обнаружения ошибок в них.

Результат:

- ♦ Оптимизация времени выполнения запроса на сетевой доступ за счёт централизации управления сетевыми устройствами в части политик сетевой безопасности. Например, если вручную определение маршрута запрашиваемого доступа, устройств на нём и определения того, где именно и какие изменения необходимо внести для предоставления доступа затрачивалось 4 часа, то с использованием систем централизованного управления сетевым

доступом этот процесс может занять несколько минут (в зависимости от количества устройств, правил и некоторых других факторов), так как эти данные уже хранятся в системе;

- ♦ Снижение времени создания запроса на сетевой доступ за счёт автоматического парсинга форм заявок с необходимыми доступами (к примеру, в Algossec парсер можно доработать под существующие в организации формы — обычно это шаблоны Excel или Word);
- ♦ Приведение фактического процесса управления сетевым доступом к регламентному за счёт гибкости настройки шаблонов и рабочего процесса запросов в системах класса Algossec/Tufin/Skybox/Firemon.

Интеграция с платформами бизнес-аналитики. Интеграция с платфор-

мами бизнес-аналитики может дать более детальную статистику по работам, связанным с предоставлением сетевого доступа, что позволяет выделять, например, наиболее трудозатратные запросы для последующей оптимизации по работам такого типа.

Описание:

- ♦ передача информации о времени выполнения работ по заданному расписанию/фильтру.

Результат:

- ♦ получение статистики по заданным параметрам, например, среднее время выполнения запроса с категоризацией по исполнителям, среднее время нахождения в конкретном статусе и т.д., что может помочь с оценкой трудозатрат, например, для расчёта KPI.

Интеграция с IDM. Интеграция систем для централизованного управления сетевым доступом с IDM-системами предоставляет более мощный инструментарий, чем при использовании этих систем по отдельности. Интеграции такого рода позволяют контролировать жизненный цикл предоставляемого доступа и обогатить обработку запросов в IDM информацией о сетевом доступе:

- ♦ Проверка наличия;
- ♦ Создание запросов на предоставление;
- ♦ Продление;
- ♦ Закрытие.

Данный список далеко не исчерпывающий, возможны более сложные сценарии, эффект от которых будет более ощутимым для бизнеса организации.

Системы для централизованного управления сетевым доступом как отдельные элементы ИТ-инфраструктуры предоставляют эффективный инструментарий для управления сетевым доступом, но при интеграции с корпоративными сервисами польза от использования каждой системы увеличивается за счёт расширения возможностей и обмена информацией между интегрируемыми системами, что даёт ощутимый эффект от таких взаимодействий.



Максим ТЕМНОВ
заместитель генерального
директора по сервису, СТИ

ПРОСТАЯ ЛОГИКА

ПРЯМОЙ СЕРВИСНЫЙ КОНТРАКТ ИЛИ ДОГОВОР С СИСТЕМНЫМ ИНТЕГРАТОРОМ?

Максим Темнов, директор по сервису системного интегратора СТИ, рассказывает, как изменится рынок системной интеграции и что ожидает обладателей объектов КИИ.

ПРЕДПОСЫЛКИ

В конце 2020 года Министерство цифрового развития, связи и массовых коммуникаций РФ разработало проект постановления правительства об утверждении требований к программному обеспечению, телекоммуникационному оборудованию и радиоэлектронной продукции, используемым на объектах критической информационной инфраструктуры (КИИ), а также предложило на год ускорить переход на отечественное ПО и/или оборудование при наличии соответствующих российских аналогов.

Одним из ключевых пунктов документа стала необходимость обслуживания объектов КИИ российскими организациями в целях обеспечения технологической независимости и безопасности КИИ в экономической сфере. Согласно первому параграфу требований, при использовании ПО, телекоммуникационного оборудования и/или радиоэлектронной продукции должна быть обеспечена возможность его модернизации, гарантийного обслуживания и технической поддержки российскими организациями, зарегистрированными как юридические лица в соответствии с

законодательством РФ и являющимися резидентами РФ.

В рамках общественного обсуждения проекта нормативного правового акта прозвучало предложение исключить необходимость оказания поддержки исключительно резидентами РФ, однако оно было отклонено, поскольку не были представлены достаточные обоснования. Из этого следует, что проект постановления будет отправлен в неизменном виде на утверждение Правительства, а после — вступит в силу. В ходе процесса утверждения в проект могут быть внесены изменения. Так, в соответствии с предложением Министерства экономического развития РФ, возможно, будет ограничена область действия документа, и требования коснутся организаций, эксплуатирующих только значимые объекты КИИ. Тем не менее вектор дальнейшего развития вопроса задан на высшем уровне, и это значит, что поручения президента будут выполнены.

Вместе с тем законодатели и регуляторы отмечают, что процент организаций, исполняющих Постановление Правительства РФ № 127 от 8 февраля 2018 года об утверждении правил категорирования объектов КИИ РФ, а также перечня показателей их значимости, неуклонно снижается. Чтобы урегулировать этот вопрос, на сегодняшний день в Государственной думе РФ уже прошёл первое чтение законопроект о внесении изменений

в КоАП РФ, напрямую затрагивающий субъекты рынка, относящиеся к ключевой информационной инфраструктуре РФ.

ПРО СЕРВИСНЫЕ КОНТРАКТЫ

Все эти обстоятельства указывают на то, что текущие прямые сервисные контракты, заключённые российскими субъектами КИИ с зарубежными производителями, вскоре могут утратить всякую ценность, либо потребуются дополнительные затраты. Оценивая сложившуюся ситуацию, некоторые вендоры уже сейчас озаботились созданием российских представительств, однако с позиции законодательства они вряд ли будут признаны резидентами РФ. В ещё более рискованном положении находятся компании, эксплуатирующие объекты КИИ AS-IS, намеренно отказываясь от какой-либо сертифицированной поддержки. В случае поломки или выхода оборудования из строя они могут столкнуться с рядом серьёзных проблем — от ИБ-угроз до нарушения бесперебойной работы предприятия — и понести значительные финансовые потери.

Если срок действия контракта с вендором подходит к концу, а на повестке дня стоит вопрос о заключении нового, самое время задуматься об обращении к сертифицированному системному интегратору, и вот почему.

Казалось бы, взаимодействие с зарубежным производителем ПО и/или оборудования — это максимально

логично. Отсутствуют посредники, обеспечивается оперативный доступ к технической документации, создатели хорошо знают потенциал и уязвимости своих продуктов. Производители оказывают все три линии поддержки, а проблемы зачастую решаются удалённо. Но, несмотря на то что системный интегратор выступает в роли первой и второй линий поддержки, оставляя третью в ведении производителя, преимущества работы именно с сервисным центром интегратора перевешивают чашу весов в его пользу.

ПОЧЕМУ ТОЛЬКО СИСТЕМНЫЙ ИНТЕГРАТОР?

В нынешних условиях в связи с планируемыми изменениями в законодательстве только системный интегратор способен обеспечить легитимную эксплуатацию зарубежного оборудования. Чтобы получить право оказывать такую поддержку, сервисный центр интегратора проходит сложную и ресурсоёмкую процедуру авторизации. Полученный в результате статус даёт право оказывать техническую поддержку заказчикам от имени и на условиях производителя. Заключение договора с системным интегратором гарантирует безопасность с точки зрения исполнения существующего и перспективного законодательства и требований регуляторов. Особую важность такая перспектива имеет для заказчиков, имеющих многолетние вендорские контакты. Дело в том, что компании нередко заключают трёх- и пятилетние договоры с производителями, тем самым предоставляя долгосрочный доступ к информации или к функционирующим системам КИИ. Зарубежные производители обязаны исполнять законные требования исполнительных органов своих государств, в том числе специальных служб. Случается, что представительства зарубежных компаний, которые имеют юридический адрес в России и нанимают здесь сотрудников, на самом деле являются не производителями, а, к примеру, коммерческими департаментами. В этой ситуации заключённые с ними контракты на техническое сопровождение не имеют должной юридической силы.

Если срок действия контракта с вендором подходит к концу, а на повестке дня стоит вопрос о заключении нового, самое время задуматься об обращении к сертифицированному системному интегратору

Кроме того, взаимодействие с системным интегратором — это выгодно. Стоимость услуг российских сервисных центров ниже вендорских, а если учитывать потенциальные затраты, которые грозят в случае неисполнения законодательства, разница в объёме вложенных средств может быть разительной. К тому же заказчик избегает возможных проблем с оборудованием: интегратор берёт риски на себя за счёт собственного склада запчастей, а также складов оборудования дистрибьюторов и производителей.

В случае необходимости удобнее обратиться в авторизованный сервисный центр, расположенный в России. Проблема будет решена быстрее, а излагать её суть на русском языке как минимум комфортнее для заказчика. Помимо языка, на котором осуществляется коммуникация, а также территориальной близости экспертных ресурсов сервисных центров интеграции, очевидным плюсом является возможность получить комплекс услуг по цифровой трансформации бизнеса по принципу «одного окна». Системные интеграторы разрабатывают детальные сценарии таких изменений, помогая не только проектировать и внедрять решения, но и далее — обслуживать их и модернизировать.

ПУТЕВОДНЫЙ СЕРВИС

Действуя согласно требованиям проекта постановления правительства, на первом этапе компании-субъекты КИИ должны провести аудит используемого ПО и радиоэлектронного оборудования. Второй этап — составление плана по импортозамещению существующих зарубежных решений или перехода на преимущественное использование российского ПО и оборудования в ходе развития инфраструктуры. Компании должны обеспечить возможность технической поддержки для тех зарубежных решений, импортозамещение в отношении которых будет отсрочено.

* * *

Системные интеграторы — «проводники» в обслуживании объектов КИИ — формируют новый пласт знаний для работы с российскими ИТ-продуктами. Опыт подобной работы позволит спрогнозировать затраты, сформулировать перечень критериев, которым должны соответствовать ПО, телекоммуникационное оборудование и радиоэлектронная продукция, оценить условия, соблюдение которых необходимо для перехода на отечественные аналоги.

СПРАВКА

Сервисный центр СТИ — это:

- ◆ более 350 действующих сервисных контрактов по поддержке ИТ-инфраструктуры крупных ретейлеров, телеком-операторов, банков;
- ◆ более 1 млн единиц оборудования на поддержке;
- ◆ 65 собственных сервисных инженеров;
- ◆ более 200 авторизованных сервисных подрядчиков;
- ◆ 550 тысяч пользователей обслуживается ежегодно;
- ◆ 4500 ежемесячных обращений фиксируются;
- ◆ 4,98 из 5 — средний балл удовлетворённости клиентов качеством услуг СТИ;
- ◆ 2 часа — среднее время устранения инцидента.



Роман КОСИЧКИН
ведущий эксперт Департамента
комплаенса кредитно-финансовой
сферы ГК «ЦИБИТ»

АУДИТ — НЕ ОТЧЁТ!

КОМПЛАЕНС ДЛЯ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ: ПРОБЛЕМЫ И РЕШЕНИЯ

В конце 2020 года Банк России провёл киберучения среди 22 банков страны. Первый замглавы Департамента информационной безопасности регулятора Артём Сычёв заявил, что банки справились с задачами лучше, чем ожидалось. Однако в ведомстве по-прежнему обращают внимание на расширение спектра угроз, которым подвержены финансовые организации.

Сегодня мошенники постоянно придумывают новые способы и меняют схемы — по статистике самих банков, число атак в прошлом году на фоне пандемии значительно увеличилось, в некоторые периоды наблюдался двукратный рост активности мошенников. Всё это актуализирует тему выполнения всеми подотчётными организациями требований в области информационной безопасности.

Сдерживание активности кибермошенников достигается в том числе выполнением требований положений, принятых Банком России и направленных на организацию защиты платёжных систем, а также стандартов по обеспечению информационной безопасности кредитных организаций.

В целях соответствия всем требованиям регулятора финансовым организациям необходимо проведение аудита на соответствие требованиям Банка России:

♦ Положение № 382-П от 09.06.2012 «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке

осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».

♦ ГОСТ Р 57580.1–2017 «Безопасность финансовых (банковских) операций. ЗАЩИТА ИНФОРМАЦИИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ. Базовый состав организационных и технических мер».

Эксперты Департамента комплаенса кредитно-финансовой сферы ГК «ЦИБИТ» отмечают: сегодня в стране действуют несколько тысяч компаний-лицензиатов, формально отвечающих требованиям Банка России, предъявляемым к внешним аудиторам в области информационной безопасности. При этом организаций, которые реально обладают компетенциями и достаточным опытом в проведении аудитов ИБ, всего около четырёх десятков по всей стране.

Поэтому мы рекомендуем при выборе аудитора, который проведёт проверку на соответствие требованиям регулятора, обратить внимание на ряд важных нюансов.

НИЗКАЯ ЦЕНА НА УСЛУГУ ≠ КАЧЕСТВО

Аудит финансово-кредитной организации — процесс многоэтапный и сложный. Качественная проверка на соответствие всем требованиям Банка России требует больших временных затрат.

Самое главное, что нужно понимать клиенту, — в его же интересах качественно выполненный аудит, а не сделанный на скорую руку отчёт.

Комментирует Роман Косичкин, ведущий эксперт Департамента комплаенса кредитно-финансовой сферы ГК «ЦИБИТ»:

«Со стороны регулятора (Банка России) на текущий момент предъявляется единственное требование к таким компаниям, озвученное во всех Положениях, связанных с информационной безопасностью:

«Оценка соответствия защиты информации должна осуществляться с привлечением сторонних организаций, имеющих лицензию на проведение работ и услуг, предусмотренных подпунктами «б», «д» или «е» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утверждённого постановлением Правительства Российской Федерации N 79».

Никаких других дополнительных требований ни к самой компании, ни к квалификационным данным сотрудников, проводящих аудит, не предъявляется».

Многие компании, работающие в этой области, занижают цены и предлагают «ускоренные» варианты проведения аудита и составления аудиторского отчёта, но для самого банка это может обернуться целым рядом проблем.

Роман Косичкин:

«При проведении аудита людьми, не являющимися профессионалами в данной области, возможно непонимание ими, с одной стороны, банковских технологических процессов, а с другой — сути и смысла тех мер защиты, которые прописаны в ГОСТе и других стандартах.



Данный минус усугубляется тем, что со стороны Банка России как регулятора не прописаны методологические указания по оценке применения мер защиты. Всё это приводит к необъективности получаемой оценки соответствия, в основном в сторону завышения. В результате в случае проверки результатов аудита со стороны Банка России будут выявлены многочисленные несоответствия, что приведёт к штрафным санкциям со стороны регулятора».

ПРИНЦИПЫ РАБОТЫ СПЕЦИАЛИСТОВ ГК «ЦИБИТ»

В Департаменте комплаенса кредитно-финансовой сферы ГК «ЦИБИТ» разработан ряд краеугольных принципов, которые применяются в процессе оказания услуг:

1. Объективность

Наши специалисты работают только с фактами и делают выводы исключительно на основе предоставленных свидетельств аудита (наблюдений, опросов, файлов данных).

2. Открытость

Мы постоянно находимся в контакте с аудируемой организацией и делимся с ней теми выводами (в том числе и

промежуточными), которые получаем в ходе проведения оценки соответствия.

3. Эффективность

В Департаменте разработана собственная методика проведения аудита, включающая алгоритмы работы, начиная от первой встречи с заинтересованными лицами аудируемой организации, хранения и обработки свидетельств и заканчивая заключительной встречей с презентацией официального отчёта и рекомендаций по устранению выявленных недостатков. Всё это позволяет нам рационально и максимально быстро осуществлять процесс оценки соответствия, не жертвуя при этом точностью получаемых результатов.

Роман Косичкин:

«Для нас как аудитора сложность заключается в соблюдении баланса меж-

ду требованиями регулятора (Банка России), выраженными в Положениях и Стандартах (отраслевых и ГОСТ), и желанием аудируемой организации получить максимально возможную оценку».

Для аудируемой организации сложность заключается в количестве ресурсов, выделяемых для проведения оценки соответствия. К этим ресурсам относятся как финансовые (стоимость аудита достаточно чувствительна, особенно для средних и малых финансовых организаций), так и людские (для помощи аудиторской группе в сборе свидетельств обычно выделяются сотрудники подразделений ИБ и ИТ, которые на время проведения оценки соответствия не могут полноценно выполнять свои служебные обязанности)».

Чтобы получить более подробную информацию по проведению аудита на соответствие требованиям Банка России, обратитесь к нам за консультацией, заполнив заявку на сайте: <https://www.cibit.ru/financial-compliance/>

Контакты:

+7 (495) 792-80-80,
info@cibit.ru



ГРУППА КОМПАНИЙ
ЦИБИТ



Андрей ЧАПЧАЕВ
генеральный директор
ИнфоТеКС

ИНФОТЕКСУ — 30 ЛЕТ!

ИСТОРИЯ КОМПАНИИ, СЫГРАВШЕЙ СУЩЕСТВЕННУЮ РОЛЬ В СТАНОВЛЕНИИ ИНФОРМБЕЗОПАСНОСТИ РОССИИ

Рассказывает один из основателей компании ИнфоТеКС, её бессменный генеральный директор Андрей Чапчаев.

КАК ВСЕ НАЧИНАЛОСЬ

— Андрей Анатольевич, поздравляем Вас с юбилеем! Желаем и Вам и компании крепкого здоровья, активного долголетия, верных друзей и надёжных партнеров! Расскажите, пожалуйста, как всё начиналось?

— Начало деятельности компании связано с введения в «гражданский» оборот технологий криптографической защиты информации. До этого криптография системно использовалась только в военной сфере и в областях, связанных с гостайной. В конце 1980-х в стране был опубликован ГОСТ 28147–89 на алгоритмы криптографической защиты информации. Коммерциализация экономики в начале 1990-х начала создавать спрос на криптографическую защиту информации, прежде всего в среде крупных структур, исторически заинтересованных в защите своих данных. Именно они первые заинтересовались «гражданской» криптографией.

Конечно, на тот момент говорить о каком-то сложившемся рынке информационной безопасности было преждевременно. Единицы были готовы вкладываться в развитие криптографических средств защиты информации. Мы были одними из первых, кто увидел и поверил в перспективы развития этого направления.

ВРЕМЯ ИНТЕРНЕТА

Толчком, который способствовал увеличению спроса на криптографию, послужило активное подключение организаций к сети Интернет в качестве универсальной коммуникационной среды. Экономически это стало более обоснованным, чем строительство собственных выделенных сетей связи. Это же, в свою очередь, привело к активизации как отдельно взятых мошенников, так и целых преступных сообществ, нацеленных на получение конфиденциальной информации и выведение из строя элементов информационных систем путем рассылки вредоносных писем с вирусами. Все мы, например, прекрасно помним истории с открытой продажей в те годы компакт-дисков с базами данных разных ведомств на Горбушке.

Таким образом к началу 2000-х гг. сформировался спрос на построение доверенной информационно-коммуникационной среды предприятий и доверенного электронного документооборота. А в продуктовом портфеле ИнфоТеКСа появилось решение «Виртуальная частная сеть ViPNet», которое и по сей день является основой многих наших продуктов.

Интересно отметить, что, когда на рубеже 2000-х наши зарубежные коллеги ставили на крыло протокол организации VPN сетей IPSec, специалисты ИнфоТеКС разрабатывали и совершенствовали свой защищенный протокол — IPlir (IP layer interconnection robust), который за эти годы не только подтвердил свои высокие качества надежного VPN-протокола, но и не так давно был утвержден Росстандартом в качестве рекомендаций по стандартизации Р1323565.1.034–2020 «Информационная технология. Криптографическая защита информации. Протокол безопасности сетевого уровня». И мы, как и 20 лет назад, продолжаем считать наш IPlir достойной альтернативой IPSec'у, обладающей целым рядом преимуществ.

PKI-ПРОДУКТЫ

В 2001–2002 гг. компания помимо развития сетевых средств безопасности: VPN-продуктов и межсетевых экранов; начинает активно работать в направлении создания собственной линейки PKI-продуктов. В это же время создается первая дочерняя компания — ИнфоТеКС

Единицы были готовы вкладываться в развитие криптографических средств защиты информации. Мы были одними из первых, кто увидел и поверил в перспективы развития этого направления

Интернет Траст, нацеленная на оказание услуг в области защищенного документооборота и РКИ.

ПОДГОТОВКА СПЕЦИАЛИСТОВ

Несмотря на то что в начале 2000-х у компании было еще не так много клиентов, было принято решение вкладываться в развитие учебного направления. Мы понимали: мало просто создать продукт и выпустить его на рынок, необходимо, чтобы были специалисты, способные работать с ним. Так, на рубеже 2000-х начинает формироваться еще одно направление, связанное с собственной системой дополнительного профессионального образования и повышения квалификации. Изначально его развитием занимался отдел технической поддержки, на базе которого позднее сформировалось специализированное подразделение — отдел учебных программ.

10 лет назад с учетом роста требований к системе подготовки квалифицированных кадров в сфере ИБ (как в части содержания программ, так и методологии обучения) было сформировано отдельное юридическое лицо — НОЧУ ДПО ЦПК «Учебный центр ИнфоТеКС», обладающее квалифицированными преподавательскими кадрами, набором программ подготовки и учебных материалов по разным направлениям, аккредитованное в качестве образовательного учреждения в соответствии с регуляторными требованиями в сфере образования.

ПРОГРАММНО-АППАРАТНЫЕ КОМПЛЕКСЫ

Исходно ИнфоТеКС ориентировался на разработку программных средств защиты информации, рассчитывая, что заказчик будет самостоятельно осуществлять выбор аппаратных платформ для размещения данного ПО. Такой

концепции мы придерживались до 2008 года. Когда стало ясно, что сложности информационных систем на стороне заказчиков и комплекс решаемых ими задач стал таким, что у заказчика просто не остается времени на выбор и интеграцию отдельного «железа» и программного обеспечения. Мы все чаще стали получать запросы на приобретение готовых программно-аппаратных комплексов, обеспечивающих защиту информации, поэтому в 2008 г. начали производство собственных ПАКов. Надежным поставщиком аппаратных платформ для нас стала компания «Аквариус»; кстати, это технологическое партнерство продолжается до сих пор.

«ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ»

Очередным логическим этапом нашего продуктового развития после 2010 г. стало создание нового

30+ ЛЕТ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основной бизнес ИнфоТеКС лежит в сфере разработки и производства высокотехнологичных программных и программно-аппаратных средств защиты информации. Но ИнфоТеКС сегодня — не только вендор, это еще Группа компаний, включающая, помимо компании с «родным» названием, и такие отдельные «юридические лица», как:

- ♦ Центр повышения квалификации «Учебный центр ИнфоТеКС» — негосударственное образовательное частное учреждение. Через него в год проходит свыше 1000 человек, программы обучения согласовываются и получают одобрение ФСБ и ФСТЭК, при этом по некоторым курсам длительность обучения составляет сотни часов. Выпускники учебного центра получают удостоверения государственного образца о получении дополнительного образования и повышении квалификации.

- ♦ Компания «СФБ Лаборатория», занимающаяся сертификацией средств защиты информации (СЗИ).

- ♦ Компания «Перспективный мониторинг» (ПМ), специализирующаяся на мониторинге и предотвращении компьютерных атак. Как бизнес-единица «Перспективный мониторинг» предоставляет услуги СОСа для ряда крупных государственных и коммерческих структур (Московская биржа, МТС Банк, Финам, Сбербанк Страхование, Кредит Урал банк, Эльдorado и др.). При этом опыт специалистов «Перспективного мониторинга» позволяет обогащать и совершенствовать продукты ИнфоТеКС, предназначенные для обнаружения и предотвращения компьютерных атак.



- ♦ «Инфотекс Интернет Траст» — аккредитованный удостоверяющий центр, входящий в пятерку крупнейших. Оператор юридически значимого электронного документооборота и сдачи электронной отчетности. Специалисты компании участвуют в создании инфраструктуры электронного ведения бизнеса, необходимой для развития отечественной экономики.

- ♦ Компания «Системы практической безопасности», специализирующаяся на разработке СКЗИ высокого класса защищенности. Ее флагманским решением является сертифицированный комплекс средств криптографической защиты информации «Квазар», предназначенный для поддержки криптографической защиты высокоскоростного обмена информацией между центрами обработки данных с использованием региональных и магистральных каналов транспортных сетей OTN.

- ♦ Совсем недавно к Группе компаний присоединилась еще одна компания — «Промышленные Криптосистемы» (ПроКСи). Она специализируется на разработке продуктов и прикладных решений на базе технологий распределенного реестра (блокчейна) и смарт-контрактов.

продукта — системы обнаружения компьютерных атак. И тут уместно вспомнить об еще одной нашей дочерней компании «Перспективный мониторинг», созданной в то же время. Практический опыт, который получают специалисты ПМ, обеспечивая мониторинг защищенности информационных систем клиентов, имеет применение и в прикладной сфере. Например, базы решающих правил, которые используются в продуктах ИнфоТеКС, создаются и регулярно обновляются сотрудниками «Перспективного мониторинга», а значит, снижается зависимость от коммерческих сигнатур зарубежных разработчиков.

Хочу отметить, что «Перспективный мониторинг» стал первым корпоративным центром мониторинга, подключившимся к ГосСОПКА, о чем свидетельствует соглашение, заключенное в октябре 2017 г. между компанией и ФСБ России о взаимодействии в области обнаружения, предупреждения и ликвидации последствий компьютерных атак.

ДЛЯ ЗАЩИТЫ АСУ ТП

В 2016 г. было принято решение о создании еще одного продуктового направления, объединившего средства защиты информации для промышленных информационных систем, включая распределенные системы IIoT. В настоящее время оно представлено двумя специализированными линейками для защиты АСУ ТП: наложенными сетевыми средствами, выполненными в виде шлюзов безопасности в промышленном исполнении, и встраиваемыми средствами криптографической защиты. Совместно с нашими продуктами и решениями корпоративного класса они закрывают большинство требований по защите объектов КИИ.

Существенным достижением в данном направлении стала разработка нами специализированного криптопротокола, предназначенного для защиты информационного обмена между элементами АСУ, М2М- и IIoT-устройствами. Протокол получил название CRISP. Приказом № 1504-ст Федерального агентства по техническому регулированию и метрологии от 30.12.2019 были утверждены рекомендации по стандартизации этого протокола.

Особенностью данного протокола является его небольшая избыточность, так как он ориентирован на обработку небольших объемов информации, специфичных для АСУ и универсальность — независимость от используемых в конкретной АСУ протоколов транспортного уровня. Это позволяет ему быть более эффективным, чем стандартные протоколы, пришедшие из классических ИТ. При этом в зависимости от поставленных задач протокол способен обеспечивать конфиденциальность (шифрование), целостность и аутентичность защищаемых данных как одновременно, так и каждое из этих свойств отдельно. Так, например, в сфере АСУ ТП целостность данных чаще оказывается гораздо важнее их конфиденциальности.

СФБ ЛАБ

Разрабатывая многие годы широкий спектр СКЗИ и занимаясь их сертификацией по требованиям ФСБ, мы накопили большой опыт, вылившийся на рубеже 2020 г. в создание новой компании в группе компаний «ИнфоТеКС» — специализированной исследовательской лаборатории СФБ Лаб. В настоящее время СФБ Лаб является аккредитованной ИЛ ФСБ России и может проводить весь комплекс тематических и специальных исследований СКЗИ любого класса защищенности.

НАДЕЖНЫЕ ПАРТНЕРЫ

Отдельно хочу отметить нашу тесную партнерскую работу с компанией «Системы Практической Безопасности» (СПБ) — коллеги являются высококласными специалистами в области создания сетевых шифраторов высоких классов защищенности. Но первой нашей совместной работой стала работа в другом направлении: создание специализированного решения для банков — отечественного платежного HSM — криптографического ядра любой современной платежной системы. Поэтому вхождение компании СПБ в 2018 г. в состав ГК «ИнфоТеКС» стало для нас всех вполне логичным шагом, доказывающим нашу совместную устремленность на создание уникальных и

востребованных рынком продуктом, особенно в свете активно идущих процессов импортозамещения.

В 2020 году ГК «ИнфоТеКС» пополнилась еще одной инновационной компанией «Промышленные криптосистемы» — специалистами по платформам распределенных реестров. Нет, это совсем не про криптовалюты. Это про системы корпоративного класса, позволяющие организациям эффективно оптимизировать свою деятельность, переводя свои бизнес-процессы, включающие взаимодействие со множеством контрагентов, в форму смарт-контрактов. Конечно, мы бы не были ИнфоТеКС, если бы не реализовали для всего этого правильной криптографии.

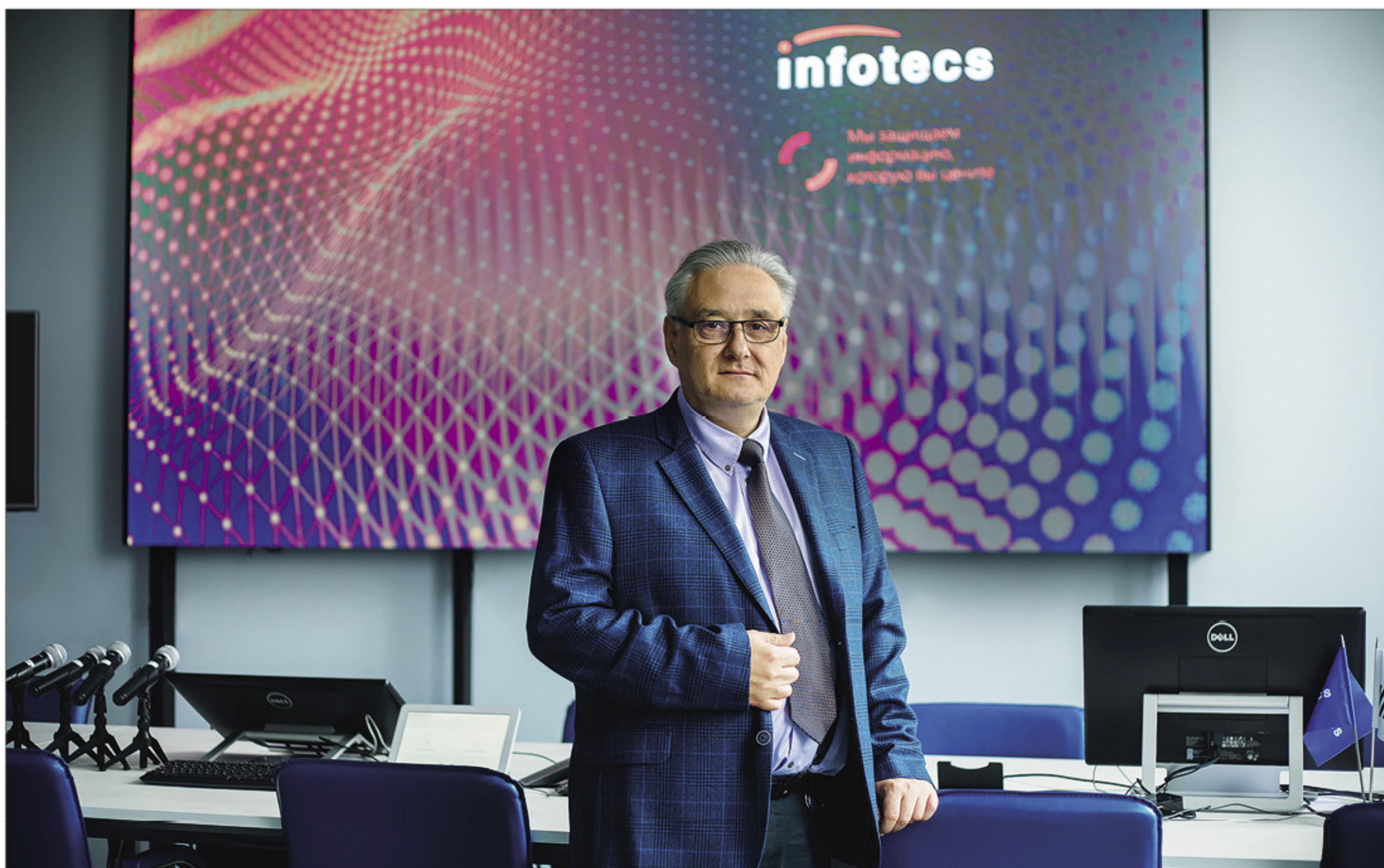
УСТРЕМЛЕННОСТЬ В БУДУЩЕЕ. НА НОВОМ ВИТКЕ

Подводя итог нашего небольшого исторического экскурса, хочу отметить, что ИнфоТеКС нацелен не только на решение текущих задач по защите информации. Мы смотрим в будущее и вкладываем немалые усилия и средства в научные разработки. Знаковым событием для нас стало заключение в 2017 году соглашения с физическим факультетом МГУ им. М. В. Ломоносова. Это партнерство привело к появлению опытных образцов аппаратуры квантовой криптографии, основанной на технологии квантового распределения ключей. Сейчас ИнфоТеКС находится на этапе сертификации первых квантовых разработок. В наших ближайших планах — вывести свои продукты на массовый рынок.

Можно сказать, что на очередном витке развития ИнфоТеКС вернулся к своим истокам — к криптографии, но уже на новом уровне, когда гарантии защиты информации обеспечиваются фундаментальными физическими принципами, а не ресурсоемкой математикой.

При этом опыт производства рыночных продуктов, накопленный ИнфоТеКС более чем за два десятилетия, позволил компании за короткий срок воплотить научные идеи в реальное «железо».

В этом направлении компания ставит перед собой глобальные и довольно амбициозные цели — создание



коммерческих продуктов, которые могли бы стать основой для будущих перспективных квантовых сетей связи России.

НОРМОТВОРЧЕСТВО И СТАНДАРТИЗАЦИЯ

— Выше мы упоминали о протоколах IPsec и CRISP — результате многолетней работы специалистов компании. Какую еще работу на поле нормотворчества и стандартизации ведет ИнфоТеКС?

— За 30 лет выстроено плодотворное взаимодействие с регуляторами, профильными комитетами Росстандарта и профессиональным сообществом в целом по вопросам стандартизации и нормотворчества в сфере ИБ.

Так, в техническом комитете по стандартизации ТК № 26 «Криптографическая защита информации» ИнфоТеКС выполняет роль секретарской компании, обеспечивая деятельность комитета и регулярно собирая экспертов на своей площадке для обсуждения актуальных вопросов развития криптографии и ее стандартизации.

Специалисты компании являются активными участниками ТК 362 «Защита информации», а также подкомитета № 1 «Безопасность финансовых (банковский) операций» Технического комитета по стандартизации № 122 «Стандарты финансовых операций» ЦБ России.

Кроме этого, эксперты ИнфоТеКС участвуют в работах Консультативного совета Роскомнадзора, входят в состав экспертного совета Минцифры по отечественному ПО, а также являются членами ряда общественных организаций: Ассоциации документальной электросвязи (АДЭ), АРПП «Отечественный софт», АПКИТ и пр. Учебный центр ИнфоТеКС помогает в разработке федеральных государственных образовательных стандартов и профессиональных образовательных стандартов в области информационной безопасности.

Отдельно хочется подчеркнуть наше активное участие в международной организации по стандартизации ИСО (ISO), в том числе в комитете ISO/TC 307 Blockchain and distributed ledger

technologies, который занимается стандартизацией в области блокчейн-технологий. Наши специалисты содействуют разработке международных стандартов и принятию российских национальных стандартов криптографической защиты в качестве международных.

ИСТОРИЯ С ГЕОГРАФИЕЙ

— Расскажите о географических аспектах жизни компании. Как ИнфоТеКС осваивает Россию?

— 30 лет назад ИнфоТеКС начинался как объединение нескольких единомышленников, верящих в то, что «гражданская» криптография будет востребована. Сегодня в компании трудится более 1500 человек, а ее представительства открыты от Санкт-Петербурга до Хабаровска.

Наша географическая экспансия тесно связана с расположением крупного бизнеса в России, научных школ в области прикладной математики (информатики) и центров регионального управления. В настоящее время группа компаний — это сеть территориально распределенных офисов, наши

представительства есть во многих крупных городах: в Томске, Хабаровске, Новосибирске, Екатеринбурге, Уфе, Ростове-на-Дону, Пензе.

В Москве находится центральное подразделение компании, второй по масштабам офис располагается в Санкт-Петербурге.

Такая территориальная распределенность позволяет нам быть более устойчивыми. Приведу свежий пример: недавно у московского офиса случился внеплановый переезд, тем не менее это никак не сказалось на планах разработки продуктов или на научной деятельности. Разработка, тестирование, коммерческий блок — все это давно уже не консолидировано только в столицах.

Хочу отдельно подчеркнуть тот вклад, который вносят в развитие ИнфоТеКС наши партнеры — системные интеграторы, поставляющие и поддерживающие решения компании по всей России и в странах СНГ.

На данный момент в партнерскую сеть входит более 200 компаний, а также несколько десятков компаний — технологических партнеров, с которыми ИнфоТеКС совместно разрабатывает и поставляет на рынок комплексные решения в области информационной безопасности.

«КАДРОВАЯ ПРОБЛЕМА НАМ НЕ ЗНАКОМА»

— Как мы знаем, на рынке ИБ и ИТ сейчас наблюдается жесткий кадровый голод. Как компания «ИнфоТеКС» решает для себя эту проблему?

— Предвидя данную проблему, мы довольно давно запустили проект «ИнфоТеКС Академия», который сейчас

является для компании своего рода кузницей кадров. Он включает две программы: грантовую и стажировочную.

Грантовая программа рассчитана на поддержку студенческих научных коллективов. Мы выделяем деньги молодым специалистам на развитие их идей и реализацию проектов, которые потом проходят апробацию на пригодность их интеграции в продукты и решения ИнфоТеКС.

Стажировочная площадка дает возможность студентам получить опыт реальной разработки без отрыва от учебы. Стажеры получают стипендию от компании, а самые успешные приглашение стать ее частью после прохождения программы. Хочу отметить, что больше половины студентов (около 90%), принявших участие в стажировке, остаются работать в компании. Мы считаем это отличным показателем.

Сегодня у нас четыре стажировочные площадки, которые находятся в Санкт-Петербурге, Томске, Уфе и Пензе, что, несомненно, дает возможность региональным представительствам расширяться, не испытывая кадрового голода.

«С УВЕРЕННОСТЬЮ СМОТРИМ В БУДУЩЕЕ!»

— Готовы ли вы поделиться информацией о своих коммерческих успехах? С какими результатами вы завершаете 30-летний цикл?

— Несмотря на то что пандемия коронавируса, под знаком которого прошел 2020 г., серьезно ударила по экономике всей страны, на бизнес компании это не оказало негативного влияния. Наоборот, наши продажи выросли и

составили более 7 млрд рублей для группы компаний.

Такое положение дел вполне объяснимо: экстренный переход наших заказчиков на удаленный режим работ позволил продемонстрировать все преимущества наших продуктов по обеспечению безопасного удаленного подключения к корпоративным информационным системам.

Для многих оказалось неожиданно, что в наших продуктах, предназначенных для удаленного доступа, уже заложены сценарии безопасного подключения, в этой части мы не делали ничего нового.

Кроме этого, видя трудности, которые испытывают наши заказчики и партнеры за время карантина мы безвозмездно передали более 1 млн временных лицензий на наши продукты, обеспечив их необходимым техническим сопровождением. Это позволило им оперативно перейти на «удаленку», не испытывая никаких проблем, связанных с выделением средств на закупку решений для обеспечения безопасного удаленного доступа.

В конечном итоге эти факторы оказали положительное влияние на продажи. Прогнозы на 2021 г. также обнадеживают, будем надеяться, что тенденция роста сохранится и в дальнейшем. Мы же планируем активно работать над улучшением существующих продуктов и выводом на рынок новых разработок. Подводя итог, хочу сказать, что мы с оптимизмом и надеждой смотрим вперед — на следующие 30 лет.

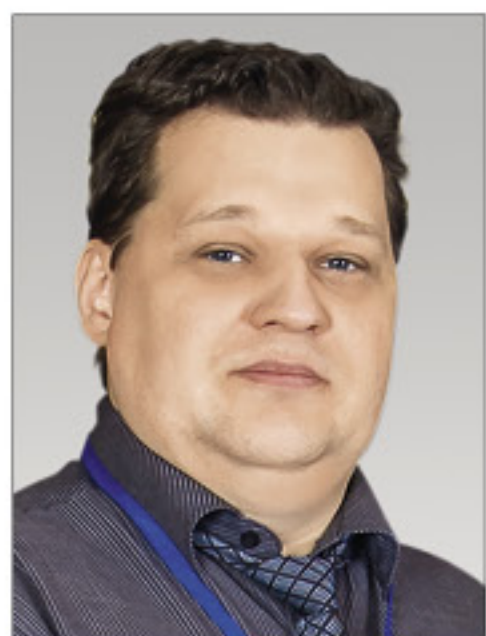
— Спасибо! Желаем успехов!

Вопросы задавал Валерий Куликов

ИНФОТЕКС СЕГОДНЯ — ЭТО:

- ♦ один из лидеров российского рынка в области «гражданской» криптографии, удовлетворяющий почти все потребности бизнеса и государственных органов в средствах защиты информации;
- ♦ поставщик средств сетевой безопасности, в частности криптошлюзов, межсетевых экранов нового поколения, программно-аппаратных комплексов (ПАК), способных конкурировать с зарубежными аналогами, удовлетворяя при этом требования регуляторов;

- ♦ надежный партнер крупных коммерческих и государственных компаний в сфере организации доверенного электронного документооборота;
- ♦ поставщик продуктов для построения SOC;
- ♦ центр развития перспективных направлений в сфере ИБ, в том числе систем квантовой криптографической связи;
- ♦ поставщик услуг в сфере дополнительного профессионального образования и повышения квалификации в области информационной и кибербезопасности.



Александр ВИНОГРАДОВ
специалист службы
информационной безопасности
КБ Максима (ООО)



Владимир ГОЛОВАНОВ
ответственный секретарь
Подкомитета 1 «Безопасность
финансовых (банковских)
операций» ТК122 «Стандарты
финансовых операций», сотрудник
АО «ИнфоТеКС»

ТК 122 / ПК 1 — 10 ЛЕТ!

БОЛЬШОЙ ПУТЬ СТАНОВЛЕНИЯ СТАНДАРТИЗАЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФИНАНСОВОЙ СФЕРЫ

Наверное, нет в России ибэшника, который не знает, что такое СТО БР и ГОСТ, но не всем известно, что это не просто документы ЦБ РФ, а прежде всего — большое коллективное творчество.

Сначала, сразу после 2008 года, «прозвучал» «Комплекс стандартов Банка России», а с приближением к введению в действие 152-ФЗ «О персональных данных» безопасники узнали, что вступил в действие и СТО БР, который может одновременно закрыть ряд норм

регулирования в банках. Время шло, и на горизонте появился ГОСТ Р 57580. У многих возник вопрос: а кто пишет эти документы, как их понимать в неоднозначных местах и как вносить изменения? Тогда коллеги по отрасли и узнали, что есть такой Технический комитет (ТК) № 122, а в нём подкомитет № 1, в рамках работ которого и оттачиваются эти актуальные документы.

Ранее эти работы стартовали на площадке ТК № 362 «Защита информации» ПК № 3 «Защита информации

в кредитно-финансовой сфере», который действовал с октября 2003 по апрель 2011 года. В этом подкомитете шла отработка версий документов «Комплекс стандартов Банка России». За всё время работы ПК № 3 были выпущены следующие стандарты: СТО БР ИББС-1.0, СТО БР ИББС-1.1, СТО БР ИББС-1.2, РС БР ИББС-2.0, РС БР ИББС-2.1, РС БР ИББС-2.2, РС БР ИББС-2.3, РС БР ИББС-2.4 (более подробно на сайте Банка России http://www.cbr.ru/information_security/).



Участники заседания ТК №362 в 2006 г. в Воронеже



Встреча 2 апреля 2013 г. была посвящена вопросам программы и плана работ на 2013–2014 гг.



Встреча 19 апреля 2013 г. с ключевыми поставщиками банковских приложений

С мая 2011 года работа ТК 362/ПК 3 была перенесена на профильную банковскую площадку ТК 122/ПК 1 «Безопасность финансовых (банковских) операций», заседания которого проходили преимущественно на базе помещений Банка России (ул. Неглинная, 12, Ленинский пр., 1/2 и др.). Работа проходила как очно (проведение заседаний), так и заочно (через созданный для этого ресурс <http://www.tk122.ru/pk1/>). Перед ТК 122/ПК 1 ставились следующие задачи: организация и координация процессов разработки национальных стандартов финансовых операций, адаптация действующих международных стандартов с целью повышения эффективности российского сектора финансовых услуг и интеграции с международными финансовыми рынками. Председателем ПК 1 в 2012 году был назначен Андрей Петрович Курило, заместитель начальника Главного управления безопасности и защиты информации Банка России.

Организационно структура ПК 1 включала в себя следующие роли: председатель подкомитета (Курило А. П.), организация-секретариат (НПФ «Кристалл», ответственный секретарь: Голованов В. Б.), а также члены ПК 1 (на базе коллектива, участвовавшего в разработке стандартов Банка России).

Число организаций, пожелавших принять участие в работе ПК 1, с каждым годом росло: 2012 г. — 34 члена, 2013 г. — 47 членов, 2014 г. — 49 членов, 2015 г. — 85 членов, 2016 г. — 93 члена, 2018 г. — 100 членов, 2020 г. — 112 членов.

Резкий рост числа кандидатов в 2015 г. связан преимущественно с

охватом деятельности некредитных финансовых организаций (НФО) и привлечением их представителей к работам подкомитета.

Помимо основной работы, по плану организовывались и рабочие встречи инициативной группы ПК 1 с участниками платёжного рынка на площадке некоммерческого партнёрства «Национальный платёжный совет».

В рамках работ подкомитета в 2013 году был принят национальный стандарт РФ, гармонизированный с международным, предложенный подкомитетом к включению в ПНС-2013 и отработанный с участием его представителей и экспертов от регулятора-учредителя ТК 26: ГОСТ Р 55811–2013 «Управление сертификатами для финансовых услуг. Сертификаты открытых ключей».

В 2014 году произошли организационные изменения. Председателем ПК № 1 был назначен заместитель начальника Главного управления безопасности и защиты информации Банка России Сычев А. М. Его появление придало новый импульс работам, оживило процесс общения Регулятора по линии работ подкомитета с участниками финансового рынка.

В 2014–2016 годы были приняты следующие стандарты Банка России: новые редакции СТО БР ИББС-1.0–2014 «Общие положения» и СТО БР ИББС-1.2–2014 «Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0–2014», новый стандарт СТО БР ИББС-1.3–2016 «Сбор и анализ технических данных при

реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств». На текущий момент редакции данных документов не изменились.

Были введены в действие новые рекомендации в области стандартизации: РС БР ИББС-2.5–2014 «Менеджмент инцидентов информационной безопасности», РС БР ИББС-2.6–2014 «Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем», РС БР ИББС-2.7–2015 «Ресурсное обеспечение информационной безопасности», РС БР ИББС-2.8–2015 «Рекомендации по обеспечению информационной безопасности при использовании технологии виртуализации», РС БР ИББС-2.9–2016 «Предотвращение утечек информации».

С 2018 года были приняты: национальные стандарты для нужд регулирования вопросов по защите информации мерами технического регулирования — ГОСТ Р 57580.1–2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций» и ГОСТ Р 57580.2–2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия», новые стандарты Банка России СТО БР ИББС-1.4–2018 «Управление риском нарушения информационной безопасности при аутсорсинге», СТО БР БФБО-1.5–2018 «О формах и сроках взаимодействия Банка России с участниками информационного обмена при выявлении инцидентов, связанных с нарушением требований к обеспечению

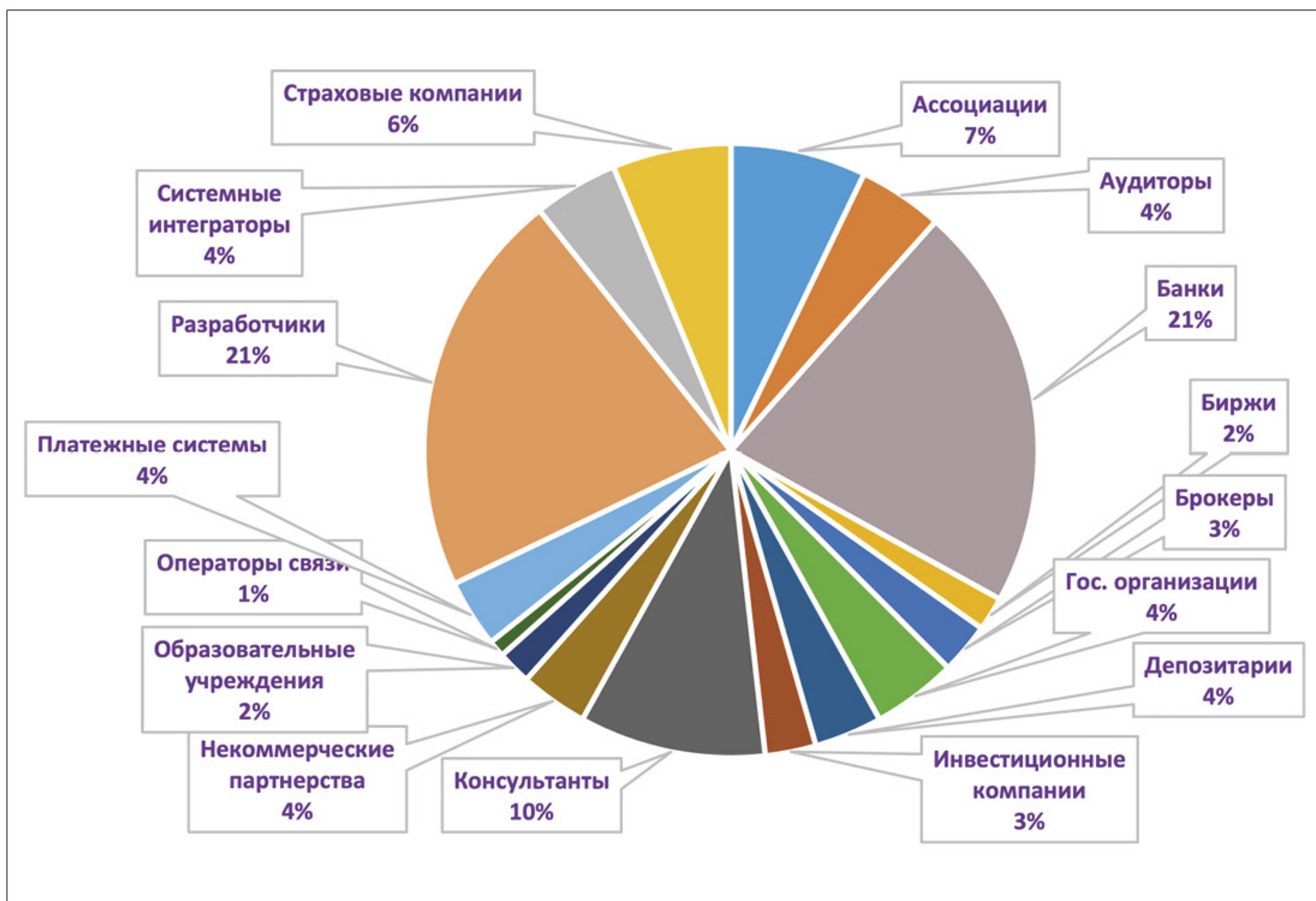


Рисунок 1. Состав членов ПК № 1 на конец 2020 года.

защиты информации», СТО БР ФАПИ. СЕК-1.6–2020 «Прикладные программные интерфейсы обеспечения безопасности финансовых сервисов на основе протокола OpenID. Требования».

В 2019 году в составе ПК № 1 были сформированы две экспертные рабочие группы (РГ) по направлениям: управление риском реализации информационных угроз; обеспечение операционной надёжности.

Начиная с 2020 года работы проводятся в дистанционном формате ввиду резкого ухудшения эпидемиологической обстановки.

На конец 2020 года состав членов ПК № 1 иллюстрирует приведенная диаграмма (рис. 1).

Работа ТК 122/ПК 1 не останавливается ни на один день. У его членов много предложений, которые в скором времени будут представлены сообществу, например, разработаны проекты новых национальных стандартов: «Безопасность финансовых

(банковских) операций. Управление риском реализации информационных угроз. Общие положения» и «Безопасность финансовых (банковских) операций. Обеспечение операционной надежности. Общие положения», включая стандарты методики оценки соответствия требованиям данных стандартов.

Ведётся плотная работа с экспертами ТК 26 «Криптографическая защита информации» в части организации и проведения экспертизы членами ТК 26 проектов стандартов Банка России, прямо или косвенно связанных с применением криптографических механизмов в финансовых операциях.

Проводятся консультации с руководством ТК 098 «Биометрия и биомониторинг» по согласованию планов работ по стандартизации в целях развития и совершенствования системы и протоколов удалённой идентификации на базе Единой биометрической системы (ЕБС).

Осуществляется регулярное взаимодействие с руководством и секретариатом ТК 362 «Защита информации» в рамках работ по программе национальной стандартизации, включая работы, предусмотренные программой «Цифровая экономика».

Развитие отечественной экономики и финансовой отрасли требует всё новых решений и технологий, широкое использование которых невозможно без развитой системы стандартов. Этот тезис в так называемых развитых странах есть аксиома, а в России — всё ещё как бы теорема, которую надо доказывать. Будем надеяться, что период взросления российской сферы технического регулирования встанет на путь устойчивого поступательного развития, а эпоха гонений на отрасль стандартизации начала 2000-х канет в Лету как страшный сон.



КИБЕРБЕЗОПАСНОСТЬ — НАШИ ДНИ. ПРОМЫШЛЕННЫЕ ТЕХНОЛОГИИ — 2021

ЕЩЁ ОДИН ФОРУМ НА УРАЛЕ!

В феврале в ДЦ «Юбилейный» под Магнитогорском состоялся первый форум «Кибербезопасность — наши дни. Промышленные технологии», посвящённый проблемам безопасности промышленной инфраструктуры.

Стремительная цифровизация и повсеместная автоматизация в промышленности вскрыли и слабые, киберуязвимые места этих процессов. О способах и современных методиках их защиты можно было узнать на новом мероприятии от Медиа Группы «Авангард», организованном при участии ФСБ России, ФСТЭК России и РГУ нефти и газа им. И. М. Губкина.

В мероприятии приняли участие более 130 человек. В одном месте собрались практики ИБ, представители регулятора, вендоры, работающие на рынке

промышленной кибербезопасности, а также потенциальные заказчики.

ТОЧКИ НАД I

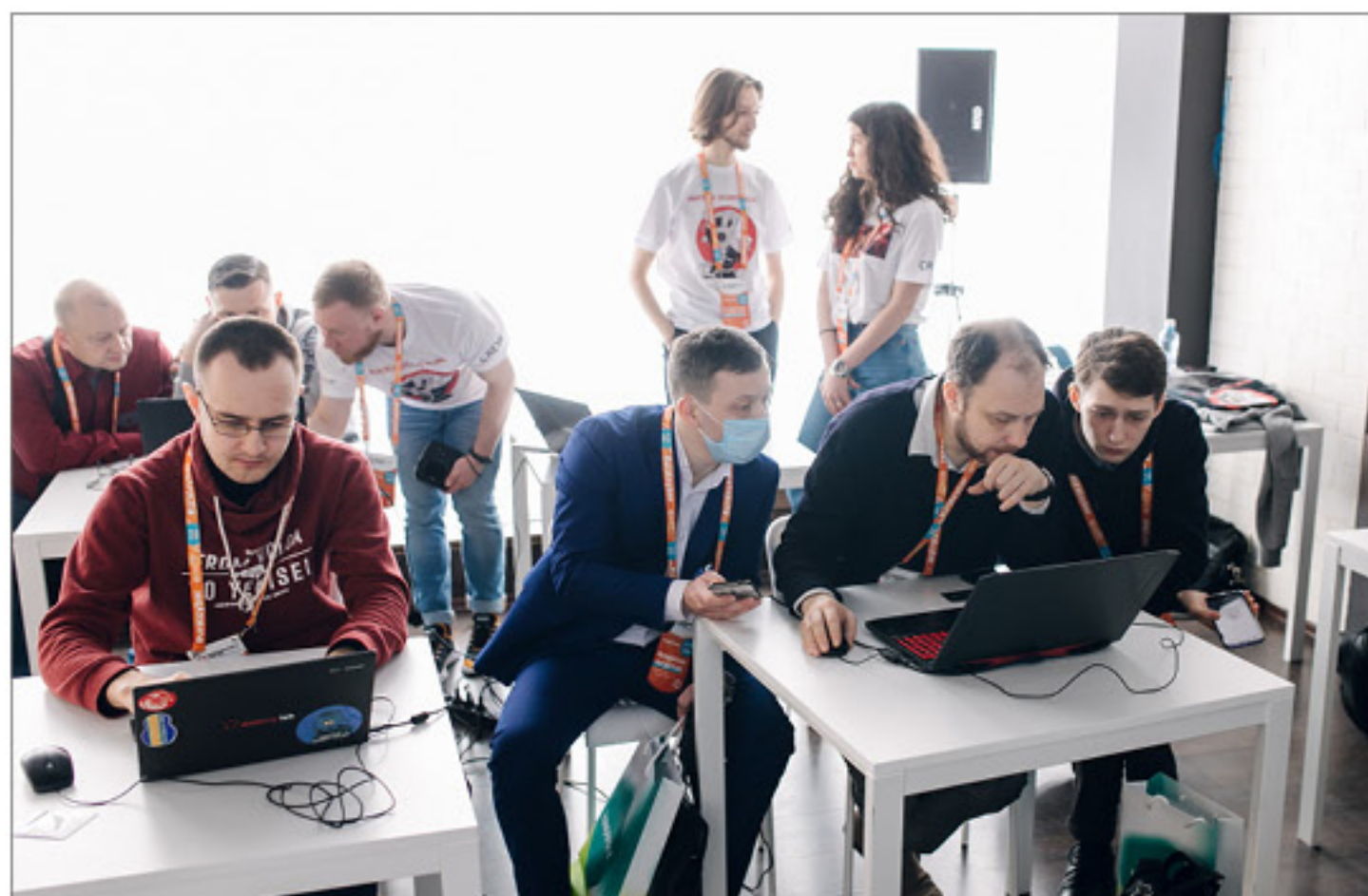
Уже первый день Форума показал, что заявленная проблематика не может быть разрешена преобразованием опыта, накопленного в сфере ИБ корпоративной цифровой инфраструктуры. Эксперты сразу расставили точки над i, заявив, что в промышленной информационной безопасности метрика конфиденциальности отходит на второй план, а во главу угла должны быть поставлены целостность и доступность информации, которые тесно увязаны с целостностью и доступностью оборудования. Такую точку зрения, в частности, высказал председатель программного комитета Форума, заведующий кафедрой комплексной безопасности

критически важных объектов РГУ нефти и газа (НИУ) имени И. М. Губкина Александр Баранов.

ФСТЭК ОТВЕЧАЕТ

Большим событием Форума стал телемост «Москва — Урал» — диалог ИБ-сообщества (в лице Алексея Лукацкого) с заместителем директора ФСТЭК России Виталием Лютиковым. Трансляцию телемоста в прямом эфире на онлайн-платформе посмотрели свыше 2 тыс. человек.

В ходе этого диалога, длившегося более полутора часов, Виталий Лютиков подробно ответил на поступившие от ИБ-сообщества вопросы. Хотя на освещение всех тем, волнующих специалистов отрасли, времени всё же не хватило, наиболее острые и актуальные получили полноценные разъяснения.



Воркшоп Practical Security Village



Игра Kaspersky Interactive Protection Simulation

Большинство из них было посвящено отдельным документам, касающимся КИИ, их сертификации, категорированию, проверкам и ответственности за несоответствие. Так, регулятор объявил, что уже во втором полугодии этого года начнутся проверки по вопросам обеспечения безопасности значимых объектов КИИ. И по закону сведения о результатах государственного контроля по нарушению требований по безопасности, которые создают предпосылки для возникновения инцидентов, будут направляться только в НКЦКИ, а не в следственные органы.

На фоне вопросов о предстоящих проверках аудитория не могла «пройти мимо» внесения изменений в КоАП в части административных нарушений за невыполнение требований законодательства по безопасности КИИ. Когда наконец примут данные изменения, Виталий Лютиков комментировать не взялся. Вместе с тем он отметил, что регулятор давно их ждёт. И пока у него нет в планах ужесточать штрафы и наказания, поскольку необходимо дождаться правоприменительной практики. Детальнее ознакомиться с ходом телемоста и его основными выводами можно на информационном портале <https://ib-bank.ru/bisjournal/>.

ПРАВОВЫЕ АСПЕКТЫ

В первый же день форума тема нормативно-правового регулирования была поднята на щит в ходе телемоста с Виталием Лютиковым. Позже, во второй половине дня, эта тема была подхвачена и развита заместителем начальника управления ФСТЭК Еленой

Торбенко, не только рассказавшей о сложившейся практике применения законодательства о безопасности КИИ с трибуны, но и в реальном времени консультировавшей гостей Форума.

В последний день мероприятия правовая тема также превалировала в повестке дня. Ключевыми оказались обсуждения противоречий между строгостью вступившей в силу «нормативки» (как в части требований, так и сроков) и такими обстоятельствами, как отсутствие чётких определений некоторых понятий; вопросы к регламентации практической реализации нормативных положений; конфликты реальных возможностей по исправлению недостатков в рамках имеющихся временных, финансовых и кадровых ресурсов.

ПРАКТИКА ЦЕЛЫЙ ДЕНЬ

Второй день Форума был насыщен до предела и отличался завидным разнообразием. Он полностью был посвящён практической кибербезопасности. Компания Deiteriy провела воркшоп Practical Security Village, в ходе которого ведущие пентестеры компании рассказали об уязвимостях ИС предприятий, предложили максимально эффективные способы защиты и познакомили с инструментарием, которым пользуются для поиска и эксплуатации уязвимостей.

Проходившая параллельно игра Kaspersky Interactive Protection Simulation продемонстрировала реальную роль кибербезопасности в непрерывности и доходности бизнеса. Причём акценты были расставлены на наиболее актуальных и показательных для отрасли угрозах.

Также участники Форума познакомились с решениями Fortinet для защиты промышленных инфраструктур. Краткий обзор решений сменился полуторачасовой лабораторной работой по настройке этих решений. Равнодушных не было.

Вишенкой на торте стали штабные киберучения от Алексея Лукацкого. Разбившись на команды, участники форума искали ответы на вопросы, с которыми службам ИБ приходится сталкиваться ежедневно. Пройдя по нескольким типичным сценариям атак, они получили знания и навыки, которые потом смогут эффективно переложить на бумагу, разработав планы реагирования, которые, среди прочего, требуются и в соответствии с законодательством о безопасности критической информационной инфраструктуры.

ПОДВОДЯ ИТОГИ

Как отметил в подведении итогов Форума Александр Баранов, хотя данная конференция не первая в области ИТ и ИБ для промышленности, в целом она получилась отличной.

«И вообще принимаются другие такие же интересные темы для нашего обсуждения, потому что все они, на самом деле, связаны одновременно и с более серьёзными вещами. И если мы в качестве резолюции внесём поддержку такой тематики, что промтехнологии должны нами дальше укрепляться, развиваться и исследоваться, и в том числе обсуждаться на конференциях, это будет правильно», — заключил Александр Баранов.

Фото: <https://forumifin.ru>

iFin 2021

ВЫХОДИМ ЗА РАМКИ ДБО?

На форуме iFin 2021 «Электронные финансовые услуги и технологии» была совершена провокация. В пылу дискуссии один из самых креативных лидеров отечественного системного финтеха заявил, что бизнесмену от банка требуется всего две услуги: быстро провести платёж и быстро оформить кредит. И совсем не нужно назойливого навязывания безразмерного меню опций.

Сам автор этой реплики отнюдь не является консерватором или ретроградом, он даже открыто приветствовал грядущее «убийство» карточных сервисов... в угоду СБП-подобных технологий.

Но мысль-то прозвучала!

УСТАЛОСТЬ ОБЩЕСТВА РОЖДАЕТ ПРОРОЧЕСТВА

Важный вывод, который нельзя не сделать при подведении итогов iFin 2021: в обществе накопилась усталость от

изобилия сервисов, рождённых причудливыми фантазиями архитекторов «суперприложений» и «маркетплейсов». Фантазиями, так и не подкреплёнными острой нуждой клиентов, зато обильно питаемыми поставщиками услуг в рамках этих самых «суперприложений» и участниками цепочек услуг на сторонних «маркетплейсах».

В то же время всей этой невнятной — искусственной — эклектикой надстраивают фундамент «классических» представлений о банках — институтах доверенного сохранения денег. Надстраивают с упорством, достойным лучшего применения. Например, хотя бы для совершенствования технологий ИБ в финансово-кредитной сфере.

В этой ситуации ободряет, что всё смелее звучит пророчество о перенасыщении банков «сходными реализациями сходных технологий сходных услуг». На iFin 2021 о таком развитии

событий говорил, в частности, представитель Сбера Сергей Иванов в ходе доклада «Тренды потребления банковских продуктов для юридических лиц в цифровых каналах».

ИЗВИНИТЕ, ФИНТЕХ ПЛОХО ГОВОРIT... ПО-РУССКИ

Об определённом кризисе жанра и в финтехе в целом, и в терминологии финтеха свидетельствовало развитие событий на финальном круглом столе «Выходим за рамки ДБО. Тренды развития цифровых каналов и технологий».

Круглый стол этот не вылился в каскад эффектных словесных дуэлей о «трендах развития». Эксперты даже не смогли убедительно «выйти за рамки ДБО»! Не смогли, потому что представления об этих рамках разнятся, как оказалось, и в головах экспертов на сцене, и в головах гостей в зале. Что указывает, в частности, на

необходимость перехода от общения и изложения идей на «птичьем языке» финтеха к нормальной русской речи с чётко артикулированными запятыми и однозначно трактуемыми терминами. Ведь банковские сервисы строятся для людей? Или во имя развития индустрии финтеха?

ЗДРАВСТВУЙ, «КРОКОЗЯБРА»!

Большой опасностью в нынешней кризисной ситуации становится утрата контроля за безопасностью: транзакционного фундамента, транзакций безналичных платежей, транзакций документов с электронными подписями разного назначения.

И в самом деле, несколько последних лет было потрачено на то, чтобы отучить людей от спонтанного импульсивного принятия решений, развить внимательность при изучении реквизитов платежей на интернет-страницах и реквизитов самих этих интернет-страниц (во имя безопасности), а к чему мы приходим?! К оформлению кредита или осуществлению дорогостоящей покупки на основе технологии быстрого сканирования не поддающейся анализу «крокозябры» QR-кода, причём с помощью смартфона, который никак не назовёшь доверенным устройством!

НА МЕЛИ

В дополнение к этому обрастают «дырами» новые микросервисные разработки и стыки сложных кооперативных связей в рамках «суперприложений» и «маркетплейсов»! Об этом рассказал директор департамента систем безопасности BSS в ходе своего выступления «Новые комбинированные виды атак на банковские приложения. DDoS как ввод в заблуждение». Он же анонсировал намерение своей компании собрать банковских «безопасников» для обсуждения назревших вопросов, связанных в том числе и с переходом цифровых клиентских платформ банков на так называемые инхаусные технологии разработки.

Эти технологии могут иметь свои особенности в разных банках, но должны соответствовать единым требованиям регуляторов. Об этих единых

требованиях напомнили гостям форума доклады «Экспертная оценка систем ДБО в соответствии с новыми требованиями» (НПО «Эшелон»), «Как не сесть на мель, или Грамотное управление ресурсами при оценке соответствия новым требованиям ЦБ» («Интерком»).

Компания Digital Security на iFin 2021 представила тревожный доклад об уязвимостях систем эквайринга, который наряду с уже набившей оскомину темой уязвимости банкоматов рисует неприглядную картину состояния кибербезопасности «классического» платёжного сервиса. Ведь упомянутые в докладе под анонимными брендами «Альфа», «Браво» и «Чарли» терминалы занимают около 90% отечественного рынка.

ЗА ГОД ВМЕСТО ПЯТИ

Более чем не идеальны и собственные ДБО банков.

Ещё на конференции MOBILE FORENSICS DAY 2019 среди пяти анонимизированных попавших «под раздачу» банков из топ-10 лишь один получил 3,5, а два — так и вообще «единицу» (по пятибалльной системе). Хотя ошибок можно было избежать, если бы разработчики ознакомились с рекомендациями некоторых международных стандартов.

Но этого не было сделано, а 2020 год не оставил времени на штудирование «теорий»: за год пришлось реализовывать планы технологического переоснащения ДБО, которые ранее планировались на пятилетку! Об этом ускорении было рассказано на круглом столе «Новые вызовы для электронного банкинга в 2021 году».

Уязвимости ускоренной разработки обостряются тем, что за последние годы сложился устойчивый тренд на формирование в банках собственных команд-разработчиков. В контексте безопасности новых разработок этот тренд сопровождается «разбавлением» компетентности вновь формируемых команд, ибо повышения качества образования не наблюдается, а идеологией кадровой политики становится «звёзд не набирать!». Лидеры же банковских проектов меняют места работы как перчатки — об

этом можно было судить по самопрезентациям некоторых докладчиков iFin 2021. Да и на других мероприятиях, что греха таить, усматривается то же обстоятельство.

А могут ли квалифицированно оценивать инновации с позиций требований ИБ те из них, для кого выглядит вполне допустимым штатное внедрение биометрической идентификации на базе «зоопарка» смартфонов с неконтролируемыми характеристиками оптических объективов и микрофонов и трактов обработки поступающей через них информации?!

ПОДРАЖАЯ ХОДЖЕ НАСРЕДДИНУ

Ещё один вопрос, поднятый на круглом столе «Новые вызовы для электронного банкинга в 2021 году», касался процессов импортозамещения в банковских ИТ-системах и приведения информационных систем финансовых организаций в соответствие с требованиями 187-ФЗ и других нормативных документов БР в сфере ИБ.

Судя по обсуждению (замедленная речь, расплывчатость формулировок, банальность и шаблонность аргументов в пользу «против»), эксперты предпочитают занимать в вопросах импортозамещения позицию Ходжи Насреддина в его опытах по обучению языкам ханского ишака.

Впрочем, засунуть головы в песок в полной мере участникам круглого стола не дал Андрей Бурдинский, официальный и духовный лидер iFin. Он напомнил, что 2024–2025 годы только кажутся далёкой перспективой, и призвал лидеров рынка к эффективным действиям для реализации регуляторной «маршрутной карты» по импортозамещению.

* * *

В заключение нельзя не отметить, что народу на iFin 2021 собралось много, гости форума добросовестно, как на работу, два дня являлись в здание на площади Европы, 2. Утренние и вечерние мероприятия собирали одинаково полные залы. Всё указывало на то, что общество устало от неумеренного дистанцирования.



Виктор ВЯЧЕСЛАВОВ
технический директор
Innostage



Владимир ДМИТРИЕВ
руководитель SOC CyberART

THE STANDOFF 2021

18 МАЯ НАЧНЕТСЯ КИБЕРБИТВА ЗА ЦИФРОВОЙ ГОРОД

Как ни парадоксально, но именно ковидная паранойя вывела The Standoff на большую арену: несколько лет подряд этот киберполигон был обязательной составляющей международной конференции Positive Hack Days, а в прошлом году превратился в самостоятельное, действительно масштабное онлайн-мероприятие в сфере ИБ.

МАЛЕНЬКОЕ РАССЛЕДОВАНИЕ

Подробностей предстоящего в мае киберсражения пока немного. Поэтому BIS Journal провел свое маленькое расследование.

Изучив киберсражение прошлого года, мы обратили внимание на команду защитников «КиберТатары и Московские мастера» (или СТ&ММ), а потом и на подготовивший ребят Центр кибербезопасности (SOC) CyberART, входящий в группу компаний Innostage.

Напомним, команда СТ&ММ опоздала и вступила в бой на киберполигоне что называется «с колёс», имея минимальное время для подготовки, но выступила успешно, эффективно применяя инструментарий, предоставленный организаторами (в основном продукты Positive Technologies — PT Application Firewall; PT Network Attack Discovery; PT Sandbox; MaxPatrol 8; MaxPatrol SIEM и др.).

И вот, используя этот инструментарий, «blue team» СТ&ММ по итогам шести дней обеспечила один из самых высоких показателей доступности ИТ-инфраструктуры — 96%, зафиксировала

49 инцидентов (второй показатель среди защитников) и завершила наибольшее число расследований бизнес-рисков, реализованных атакующими.

Эти официальные данные рассказали нам лишь об одном из эпизодов жизни СТ&ММ, а вот о том, что это не случайность свидетельствовало другое: хорошая «родословная» команды. И продолжать поиск следовало именно в этом направлении.

Раз уж мы заговорили об умелом использовании инструментария, принесшем успех татаро-московской команде, стоило выяснить, что технологическим ядром SOC CyberART, в котором выросла и оттачивает свои компетенции СТ&ММ, является программное обеспечение Innostage IRP, позволяющее реализовывать важнейшие функции ИБ (управление ИТ-активами; управление инцидентами ИБ; управление уязвимостями; взаимодействие с ГосСОПКА) на основе высокого уровня автоматизации рабочих процессов.

Отсюда следующее заключение. Атмосфера работы в современном автоматизированном SOC CyberART позволила ГК Innostage создать коллектив, который, будучи выведенным на учения The Standoff 2020 что называется «по тревоге», сумел подготовиться к работе на незнакомой ИТ-инфраструктуре за 10 дней (срок в три раза меньший, чем потратили на изучение полигона другие участники), проведя за это время инвентаризацию ИТ-активов и анализ их защищённости, с последующим закрытием «брешей» в рамках правил, принятых на полигоне.

В связи с последними, кстати, работа защитников на киберполигоне некоторым образом напоминала «бег в мешках», так как легенда киберучений подразумевала, что в инфраструктуре присутствуют риски (уязвимости, настройки доступа, особенности конфигурации), которые исправлять нельзя, а можно лишь «учитывать».

При таких непростых «начальных» условиях успех «blue team» СТ&ММ весьма впечатляет.

Результаты исследования привели BIS Journal к руководству компании из Татарстана. И первый вопрос был прямым, ибо от ответа на него зависела судьба нашего маленького расследования.

ЗОЛОТАЯ ЖИЛА

BIS Journal. Учитывая опыт прошлого года, планирует ли компания Innostage сотрудничать с The Standoff?

Виктор Вячеславов, технический директор Innostage. Да, в планах Innostage — стать стратегическим партнёром The Standoff. Уже сейчас наша компания является оператором учений, которые состоятся в мае 2021 г. Мы выполняем широкий круг задач, начиная от развёртывания и технического сопровождения ИТ-инфраструктуры киберполигона The Standoff и заканчивая ролью арбитра для половины команд защитников и атакующих, принимая и оценивая отчёты об их действиях.

Мы планируем и далее наращивать сотрудничество в этом направлении, и в перспективе, совместно с компанией Positive Technologies, организовывать киберполигоны The Standoff на различных

площадках и с разными форматами участия, как широкодоступными, так и приватными, исходя из требований и задач различных компаний — участников и заказчиков подобных киберполигонов.

BIS Journal. Как в компании Innostage оцениваются перспективы киберполигонов для повышения квалификации и развития навыков служб ИБ?

Виктор Вячеславов. Киберполигон The Standoff сейчас — наиболее эффективный способ повышения квалификации сотрудников всех уровней: от технических специалистов до руководителей служб мониторинга.

Он позволяют моделировать реальные ситуации и отрабатывать решения практических задач по компьютерной безопасности, что называется, на «мышечном уровне». Выявлять потенциальные узкие места и уязвимости не только в программном обеспечении систем и средствах их защиты, но также и в архитектуре систем, и в процессах компании по обеспечению кибербезопасности.

Важное преимущество киберполигона The Standoff перед пентестами на реальной инфраструктуре — это возможность «дойти до конца»: когда атакующие не ограничены в методах и возможностях реализации рисков и могут попытаться вывести из строя даже реально работающий макет — «цифровой двойник» какой-то критически важной для компании системы. Например, системы автоматизации транспортного узла или системы снабжения газом потребителей, что в реальной жизни вызвало бы техногенную аварию. При этом защитники могут пробовать разные методы и подходы к выявлению и предотвращению атак, пока не найдут те, что не будут мешать корректно работать существующим бизнес- или технологическим процессам компании.

Благодаря этому киберполигоны в ближайшее время станут неотъемлемой частью систем обеспечения компьютерной безопасности всех компаний, которые стремятся выстроить результативную защиту и эффективно противостоять киберугрозам.

УРОКИ ВИРТУАЛЬНОЙ ЖИЗНИ

BIS Journal также обратился к руководителю Центра кибербезопасности

CyberART Владимиру Дмитриеву, попросив его прокомментировать опыт, полученный его командой в ходе киберучений The Standoff 2020.

Владимир Дмитриев, руководитель SOC CyberART. В ходе учений The Standoff 2020 команда CyberART получила уникальный практический опыт защиты сложной, распределённой и многокомпонентной ИТ-инфраструктуры на примере «цифрового двойника» современного большого мегаполиса — виртуального делового центра города.

В защищаемом нами виртуальном деловом центре были «небоскрёбы», оборудованные управляемой подсветкой, большими рекламными экранами и умными системами климат-контроля. Здесь была регулируемая автодорожная сеть и парк развлечений с системой онлайн-касс и различными аттракционами, которые находились под центральным контролем. Также в зону нашей ответственности попала и управляющая компания, предоставляющая сервисы для жителей через портал услуг, на котором хранились и обрабатывались персональные данные жителей города. Атакующие старались реализовать в инфраструктуре делового центра виртуального города бизнес-риски из реальной жизни: украсть персональные данные, удалить информацию по штрафам, нарушить систему кондиционирования в небоскрёбах, остановить работу светофорной сети, разрушить колесо обозрения в парке развлечений и вызвать сбой в работе онлайн-касс.

В ходе учений команда CyberART защищала свои объекты, выявляя и отражая атаки на их инфраструктуру. Это позволило нам проверить навыки наших специалистов по выявлению и расследованию реальных кибератак со стороны профессиональных хакеров, а также провести стресс-тест и оценить возможности нашей команды по противостоянию множественным атакам. Все это позволяет нам быть уверенным, что при возникновении аналогичных инцидентов в инфраструктуре реально защищаемых нами компаний, похожие стресс-ситуации никак не повлияют на способность наших специалистов отработать оперативно и без ошибок, чтобы своевременно заметить возникновение нештатной ситуации и

не допустить реализацию нежелательных событий для защищаемых нами компаний.

ЧЕГО ЖДАТЬ В МАЕ?

BIS Journal. Учитывая, что Innostage в этом году выступает в роли организатора The Standoff, чего нового ждать участникам на The Standoff 2021?

Виктор Вячеславов. The Standoff в этом году снова пройдет вместе с Positive Hack Days и продемонстрирует работу с реальными атаками еще нагляднее. В условиях «тумана войны» на киберполигоне мы планируем испытать в деле нашу разработку Innostage IRP, которая поможет нам, как команде оператора. С помощью интеграции IRP с MaxPatrol SIEM наша команда сможет регистрировать и собирать статистику по всем инцидентам, полученным автоматизировано из SIEM, также мы планируем подгружать в Innostage IRP выявленные инциденты ИБ из отчетов команд. Таким образом, на основании собранной информации, сможем вести полную базу всех инцидентов ИБ на вверенной нам зоне мониторинга. Так что, на случай апелляции от команд, у нас будет полная база инцидентов ИБ в рамках всего мероприятия. Кроме того, использование IRP даст возможность отображать статистику и ключевые показатели противостояния на вверенной нам зоне мониторинга: топ атакуемых объектов защиты с разбивкой на критические и нет, количество инцидентов ИБ и динамика их возникновения и так далее. Больше данных — больше информации для дальнейшей работы.

В рамках The Standoff предусмотрен и формат менторства: команду сопровождает эксперт, который помогает по ходу учений с подготовкой в целом, дает рекомендации по настройке средств защиты, консультирует по организации процессов внутри команды, делится экспертизой в процессе расследования инцидентов и проводит завершающий мастер-класс с результатами киберучений. И в этом году команда Innostage может выступить в роли такого ментора для кого-то из защитников.

Так что, пользуясь случаем, приглашаем всех на The Standoff 2021!

BIS Journal. Спасибо, обязательно будем!

ЗАКОН «ОБ ЭЛЕКТРОННОЙ ПОДПИСИ»: ЖИЗНЬ ПОСЛЕ ПРИНЯТИЯ



Иван ЯНСОН
эксперт BIS Journal

С ПРИНЯТИЕМ ЗАКОНА 476-ФЗ В ИСТОРИИ ЭЛЕКТРОННОЙ ПОДПИСИ В РОССИИ НАЧАЛАСЬ НОВАЯ ЭПОХА. ЧТО ПРИНЁС НОВЫЙ ЗАКОН И КАКИЕ ВЫЗОВЫ СТАВИТ?

НОВЫЕ ТРЕБОВАНИЯ К АККРЕДИТОВАННЫМ УДОСТОВЕРЯЮЩИМ ЦЕНТРАМ

Теперь удостоверяющим центрам (УЦ) необходимы собственные средства в размере не менее 1 млрд руб., если у УЦ нет разветвлённой филиальной сети, и не менее 500 млн руб., если у УЦ есть филиалы более чем в 75% субъектов РФ. Требования ужесточились в 140 и 70 раз соответственно. Увеличился и размер финансового обеспечения ответственности за убытки: теперь он равен 100 млн руб. (и дополнительно 500 тыс. руб. за каждое место осуществления лицензируемого вида деятельности), но при этом не более 200 млн руб. Ранее эти показатели составляли 30 и 100 млн руб. Кроме того, вводятся требования к деловой репутации руководителей, учредителей и самого УЦ.

Процедура аккредитации становится двухэтапной: сначала материалы рассматривает Министерство цифрового развития, связи и массовых коммуникаций РФ (Минцифра), затем специальная правительственная комиссия. Положение о такой комиссии было утверждено Постановлением Правительства РФ от 15.12.2020 № 2109 «О Правительственной комиссии, уполномоченной на принятие решения об аккредитации удостоверяющих центров», в частности, в целях более объективного рассмотрения вопросов об аккредитации, Постановлением предусмотрено, что 7 из 22 членов комиссии должны быть

представителями АНО Цифровая экономика. Предполагается, что это будут представители бизнес-сообщества. Пока что персональный состав комиссии не утвержден.

КОГДА НАЧНЁТСЯ АККРЕДИТАЦИЯ ПО НОВЫМ ТРЕБОВАНИЯМ

Новые требования по аккредитации вступили в силу 1 января 2021 года. Для начала работы правительственной комиссии должны быть утверждены требования к деловой репутации руководителя и учредителей (участников) удостоверяющего центра, которыми она должна руководствоваться при принятии решения. Проект требований уже разработан Минцифрой. Если указанный документ будет утвержден в ближайшее время, то во 2 квартале можно будет проходить аккредитацию по новым требованиям. Первые УЦ, аккредитованные по новым правилам, появятся, видимо, в конце 2 — начале 3 квартала 2021 года.

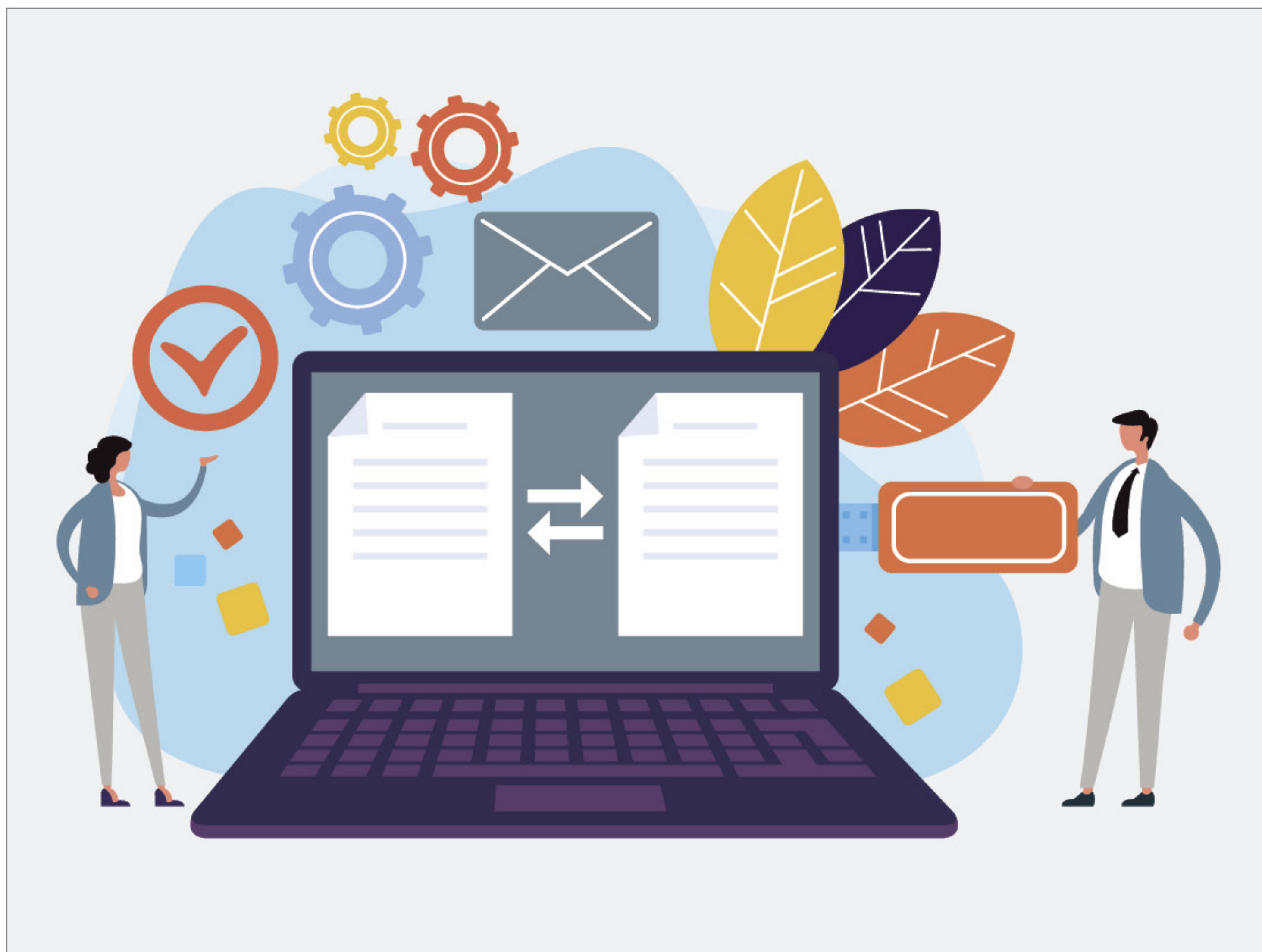
В рамках прежней аккредитации УЦ имеют право выпускать сертификаты квалифицированной электронной подписи (ЭП) только до 1 июля 2021 года (эта норма была введена дополнительно во время пандемии антикризисным законом 166-ФЗ от 08.06.2020 года). Таким образом, для обеспечения непрерывности своего бизнеса и работы обслуживаемых ими систем ЭДО УЦ должны переаккредитоваться до конца первого полугодия 2021 года, и есть риск коллапса при переаккредитации

во 2 квартале 2021 и нарушения сервисов по выпуску квалифицированных сертификатов как для ФЛ, так и для ЮЛ и ИП с 1 июля 2021 года. Отметим, что с 1 января 2022 года истекают все квалифицированные сертификаты, которые были выданы УЦ в рамках их старых аккредитаций. Это означает, что во втором полугодии УЦ в рамках своих новых аккредитаций будут должны перевыпустить всем своим клиентам сертификаты.

ЧТО ГОВОРИТ ЗАКОН ОБ ОБЛАЧНОЙ ПОДПИСИ

Облачная электронная подпись, наконец, с 1 января 2021 года попадает в правовое поле. Закон наделяет правом быть провайдерами облачной квалифицированной подписи только аккредитованные УЦ. Самого словосочетания «облачная подпись» в законе нет, однако есть право УЦ на хранение и использование по поручению владельцев ключей подписи. Чтобы воспользоваться этим правом, УЦ необходимо пройти отдельную процедуру аккредитации, в том числе, приобрести сертифицированные средства облачной подписи, и гарантировать выполнение более высокого уровня финансовой ответственности от 200 до 300 миллионов рублей.

Регулятор в области безопасности должен разработать и утвердить приказом отдельные требования к средствам облачной подписи. А вендоры средств УЦ в дополнение к уже имеющимся сертификатам ФСБ на средства



УЦ и ЭП должны будут получить заключение ФСБ о соответствии средств облачной подписи новым требованиям.

Практика показывает, что на получение подобных заключений у производителей обычно уходит не менее полугода. Таким образом, если регулятор подготовит требования к средствам облачной подписи к концу апреля 2021 года (как это предусмотрено планом-графиком издания подзаконных актов к 476-ФЗ), то с учётом отдельной процедуры аккредитации для облачной подписи, скорее всего, получить статус провайдера облачной подписи УЦ смогут не ранее начала 2022 года. Открытым остается вопрос о том, что делать с 1 января 2021 года и практически до конца 2021 года владельцам систем ЭДО, у которых уже сейчас есть облачные решения, сертифицированные по старым требованиям, и внедренные до 2021 года.

КАКИЕ ДИСТАНЦИОННЫЕ МЕТОДЫ ИДЕНТИФИКАЦИИ ВВОДИТ ЗАКОН

Изменения закона в части идентификации вызывают ряд вопросов и выглядят шагом назад. Новые требования для квалифицированных сертификатов уже вступили в силу с 1 июля 2020 года. Идентификация заявителя при выпуске квалифицированных сертификатов ЭП может быть произведена без его личного присутствия в трёх случаях: с использованием действующей квалифицированной подписи, с помощью единой системы идентификации и аутентификации (ЕСИА) и Единой биометрической системы (ЕБС), с помощью загранпаспорта нового поколения. Второй и третий способы не могут сегодня дать массового охвата. Получается, что основным способом идентификации становится очный, что уже отрицательно сказывается на клиентском опыте:

при перевыпуске сертификатов многим обладателям квалифицированной ЭП приходится совершать визит в офис УЦ.

Что касается неквалифицированных сертификатов, то новые требования по идентификации первоначально должны были вступить в силу с 1 апреля 2021 года. Законом предлагается использовать те же, что и для идентификации при выпуске квалифицированных сертификатов, дистанционные методы с помощью действующей квалифицированной ЭП, ЕБС и загранпаспорта. Дополнительно законом 183-ФЗ от 23.06.2020 предусмотрена возможность использования дистанционной идентификации с помощью ЕСИА. Другие, применяющиеся сейчас на практике, способы, например, такой классический РКІ-способ, как идентификация с помощью действующей неквалифицированной ЭП, не предусмотрены. На наш взгляд, применение данных норм

Дорожная карта изменения закона 63-ФЗ «Об электронной подписи»



Рисунок 1. Дорожная карта изменения закона 63-ФЗ «Об электронной подписи»

к неквалифицированной ЭП является нелогичным, так как её использование регулируется соглашением сторон. Так как неквалифицированная подпись применяется в ЭДО массово (например, практически во всех интернет-банкингах), то последствия от перехода к очной идентификации здесь будут более негативными, чем в случае квалифицированной ЭП. В этой связи Комитетом Государственной Думы по финансовому рынку был запущен законопроект № 1098313-7 по расширению способов идентификации. Но в процессе рассмотрения из законопроекта исчезли дополнительные способы идентификации, и он был утвержден в редакции закона № 50-ФЗ от 24 марта 2021, которым только переносится срок вступления новых требований для УНЭП с 1 апреля 2021 года на 1 января 2022 года.

ЧТО ГОВОРИТ ЗАКОН О ДОВЕРЕННОЙ ТРЕТЬЕЙ СТОРОНЕ

Доверенная третья сторона (ДТС) — новое понятие. Нормы, касающиеся ДТС, вступают в силу с 1 января 2021 года. Согласно закону, ДТС это

юридические лица, которые осуществляют деятельность по проверке электронной подписи для обеспечения доверия при обмене данными и электронными документами. Аккредитация ДТС должна проводиться согласно Административному регламенту Минцифры от 30.11.2020 N642. ДТС должны использовать средства, соответствующие требованиям Приказа ФСБ России от 4 декабря 2020 г. № 556 «Об утверждении Требований к средствам доверенной третьей стороны, включая требования к используемым доверенной третьей стороной средствам электронной подписи». К ДТС предъявляются те же требования по размеру собственных средств, что и к аккредитованным УЦ. Постановлением Правительства РФ от 15 декабря 2020 г. № 2101 для ДТС установлен размер финансовой ответственности — 300 миллионов рублей.

Наиболее актуально участие ДТС в трансграничном электронном документообороте, когда возникает потребность по проверке иностранных электронных подписей. Чтобы ДТС, УЦ или иное лицо получило право проверять

иностранные электронные подписи, оно должно быть явно прописано в международном договоре, и это сильно ограничивает возможности применения института ДТС. На наш взгляд, для развития трансграничного ЭДО было бы полезно дать право участникам трансграничного документооборота самостоятельно уполномочивать в рамках своих соглашений тот или иной аккредитованный государством ДТС на проведение проверки иностранных электронных подписей.

С учётом того, что подзаконные акты для ДТС уже выпущены, то от аккредитации кандидатов в ДТС отделяет только сертификация средств ДТС. Возможно, первые сертифицированные средства ДТС и аккредитованные ДТС появятся в 2–3 квартале 2021 года.

КАК ЗАКОН ИЗМЕНЯЕТ СХЕМУ ПОДПИСИ ЮРИДИЧЕСКИХ ЛИЦ И ИНДИВИДУАЛЬНЫХ ПРЕДПРИНИМАТЕЛЕЙ

Во-первых, теперь выпуск квалифицированных сертификатов для ЮЛ и ИП будет осуществляться не обычными аккредитованными УЦ, а тремя

государственными УЦ: ФНС России, Федерального казначейства и Банка России. Обязательным для исполнения это требование станет 1 января 2022 года.

Во-вторых, квалифицированные сертификаты ЮЛ будут выдаваться только их представителям, действующим от имени ЮЛ без доверенности.

В-третьих, обычный сотрудник ЮЛ будет должен подписывать документы своей личной квалифицированной ЭП, подтверждая свои полномочия с помощью машиночитаемой доверенности (МЧД), подписанной квалифицированной ЭП лица, действующего без доверенности. Это правило также вводится с 1 января 2022 года.

Отметим, что в случае УЦ ФНС законом предусмотрена возможность привлечения для осуществления всех действий от имени УЦ ФНС доверенных лиц (партнеров), которые должны быть аккредитованными по требованиям к облачной подписи УЦ и соответствовать дополнительным требованиям Постановления Правительства РФ от 31.12.2020 № 2409 и организационно-техническим требованиям по информационной безопасности, которые разрабатывает ФСБ России (<https://regulation.gov.ru/projects#npa=113228>). Порядок получения статуса доверенного лица УЦ ФНС определен Постановлением Правительства РФ от 02.12.2020 № 1987. На данном этапе получение указанного статуса по новым нормам закона пока что невозможно, так как еще не утверждены требования ФСБ и нет возможности получить статус УЦ, оказывающего услуги облачной подписи. Привлечение доверенных лиц УЦ ФНС нацелено на повышение доступности услуги по выпуску сертификатов для ЮЛ и ИП, а также на возможность обеспечения прозрачного клиентского опыта для клиентов таких удостоверяющих центров. В настоящее время ФНС России проводит вместе с несколькими УЦ пилот по выполнению функций доверенных лиц (участвует в этом пилоте и ПАО Сбербанк). Что касается, Федерального Казначейства и Банка России, то для них законом не предусмотрен институт специальных доверенных лиц. Тем не менее, УЦ Федерального казначейства (УЦ ФК)

создал сеть доверенных лиц, руководствуясь базовыми нормами закона. Отношения с такими доверенными лицами и требования к ним регулируются прямыми соглашениями с УЦ ФК. Сеть доверенных лиц УЦ ФК состоит только из государственных УЦ. Таким образом, ЮЛ и ИП, подведомственные Федеральному казначейству и Банку России смогут получить квалифицированные сертификаты ЭП только в государственных УЦ.

ЧТО ДОЛЖНО БЫТЬ СДЕЛАНО ДЛЯ ТОГО, ЧТОБЫ НОВАЯ СХЕМА ЗАРАБОТАЛА

Во-первых, должна быть завершена разработка недостающих подзаконных актов, в том числе, касающихся МЧД. Во-вторых, Минцифры и другие государственные и муниципальные организаторы ЭДО должны будут на основе нормативных требований к МЧД разработать формы МЧД. В-третьих, государственные и негосударственные операторы систем ЭДО должны будут внедрить в своих системах поддержку создания, использования и отзыва МЧД. И, напомним, что все это надо сделать до 1 января 2022 года (рис. 1).

НЕКОТОРЫЕ СОВЕТЫ ДЛЯ УЧАСТНИКОВ ВЫПУСКА КВАЛИФИЦИРОВАННЫХ СЕРТИФИКАТОВ И ИСПОЛЬЗОВАНИЯ КВАЛИФИЦИРОВАННОЙ ЭП

Советы для УЦ. УЦ необходимо до конца I полугодия 2021 получить новую аккредитацию.

Во II полугодии 2021 года, уже в рамках новой аккредитации, необходимо провести перевыпуск сертификатов своим клиентам ФЛ и ЮЛ, чтобы новый 2022 год они встретили с сертификатами, которые не прекратят свое действие 1 января 2022 года.

Если УЦ использует облачную подпись, то ему дополнительно будет необходимо получить, как только это будет возможно, аккредитацию провайдера услуг облачной подписи.

Кроме того, УЦ должен уже сейчас перестроить (если еще не перестроил) свои процессы выпуска квалифицированных сертификатов ЭП в части новых требований по идентификации

(перейти, там где это требует закон, на очную идентификацию). Аналогичные изменения в процессах в части идентификации необходимо внедрить к 1 января 2022 года и для неквалифицированной ЭП.

Советы организаторам ЭДО. Необходимо убедиться в том, УЦ, который выпускает квалифицированные сертификаты ЭП для ЭДО, планирует провести переаккредитацию до 1 июля 2021 года. Если у УЦ нет таких планов, то следует срочно подключиться к другому УЦ, который планирует остаться на рынке.

Чтобы смягчить последствия запрета на выпуск сертификатов по старым аккредитациям с 1 июля 2021 года (например, на случай, если УЦ не успеет вовремя переаккредитоваться), желательно до указанной даты перевыпустить сертификаты клиентам, у которых они истекают во II полугодии 2021 года.

Необходимо запланировать во II полугодии 2021 года миграцию всех пользователей системы ЭДО на новые сертификаты. При этом лицам, действующим от имени ЮЛ без доверенности (единоличным исполнительным органам — ЕИО) желательно выпустить сертификаты ЭП уже в УЦ ФНС (через инспекции ФНС, либо через одно из Доверенных лиц ФНС), либо в УЦ ФК или в УЦ Банка России (если ЮЛ подведомственно данным УЦ), а сотрудникам ЮЛ, не уполномоченным действовать от имени ЮЛ без доверенности, можно выпустить по два сертификата — один ещё на ЮЛ, а второй уже на самого сотрудника, как физлицо. Тогда ЕИО уже в 2021 году сможет начать пользоваться новой ЭП и беспшовно пересечет 1 января 2022 года. Что касается сотрудника ЮЛ, то он может до конца 2021 года пользоваться старой подписью, а с 1 января 2022 года сможет начать пользоваться своей новой подписью физлица. Если же по какой-то причине внедрение МЧД 1 января 2022 года не случится (например, будет перенесено из-за задержки с разработкой подзаконных актов), то сотрудник ЮЛ сможет продолжить пользоваться своей ЭП, выпущенной на ЮЛ, так как её сертификат будет выпущен уже по новой аккредитации и не истечет 1 января 2022 года.

Предъявление слишком высоких классов защиты к клиентским компонентам облачной подписи может стать стоп-фактором для внедрения облачной подписи, т.к. при завышении требований облачная подпись станет просто неудобна и неинтересна потребителям

Конечно, необходимо внедрить к 1 января 2022 года в системе ЭДО использование МЧД. Необходимо провести, как техническую доработку системы ЭДО, так и внедрение процессов создания, использования и отзыва МЧД пользователями системы ЭДО.

Советы для юридических лиц. ЕИО ЮЛ необходимо запланировать получение до 1 января 2022 года квалифицированного сертификата ЭП в УЦ ФНС (либо через инспекции ФНС, либо через Доверенные лица УЦ ФНС). При этом ЕИО ЮЛ должен быть готов к тому, что квалифицированный сертификат у него будет единственным (возможно такое требование будет внедрено УЦ ФНС по соображениям безопасности).

Сотрудники ЮЛ, которые используют квалифицированную ЭП, должны получить до 1 января 2022 года квалифицированные сертификаты ЭП как физлица, и должны быть готовы к использованию своих личных квалифицированных ЭП в служебных целях. В юрилице необходимо внедрить процесс безопасного использования и хранения личных ЭП сотрудников. Если ЮЛ использует квалифицированную ЭП для автоматического создания электронной подписи, то компания должна запланировать во втором полугодии 2021 года получение в УЦ ФНС сертификата ЭП и для таких целей тоже.

Если же юрлицо подведомственно в части выпуска сертификатов Федеральному казначейству (согласно Постановлению Правительства РФ от 10.07.2020 № 1018) или Банку России, то тогда ЕИО юрлица должен получить сертификат в УЦ ФК или в УЦ Банка России соответственно.

В компании также необходимо внедрить процесс подписания МЧД для сотрудников ЮЛ квалифицированной подписью ЕИО ЮЛ. Соответственно, ЕИО ЮЛ должен быть готов к тому, что теперь у него есть новая функция по подписанию МЧД своим сотрудникам.

ОТКРЫТЫЕ ВОПРОСЫ НОВОГО ЗАКОНА

Во-первых, закон ухудшает клиентский опыт в части идентификации, так как он по своей сути исходит из того, что основной способ идентификации это очная идентификация. На наш взгляд, необходимо рассматривать в качестве основного способа удалённую (дистанционную), а не очную идентификацию. Чтобы это произошло, необходимо разрешить массовые методы удалённой идентификации. Таким массовым методом может быть многофакторная идентификация, в том числе с использованием банковских систем и других систем, использующихся для идентификации в рамках 115-ФЗ. Целесообразно расширить перечень способов идентификации описанными выше способами и предусмотреть разработку новых многофакторных способов. Что касается неквалифицированной подписи, то необходимо разрешить для неё использование и действующей УНЭП, и ПЭП, полученной после очной идентификации, и других методов идентификации, определенных правилами УЦ.

Во-вторых, пока что очень много неопределённости в вопросах внедрения МЧД. В частности, необходимо предусмотреть возможность автоматизированного создания МЧД, так как в больших организациях с тысячами сотрудников невозможно вручную подписывать МЧД сотрудников ЭП руководителя организации.

В-третьих, необходимо решить вопросы о классах средств защиты, которые должны применяться для обеспечения безопасности применения облачной подписи. Предъявление слишком высоких классов защиты к клиентским компонентам облачной подписи может стать стоп-фактором для внедрения облачной подписи, так как при завышении требований облачная подпись станет просто неудобна и неинтересна потребителям. Также вызывают определенные вопросы с точки зрения обоснованности и некоторые проектируемые в подзаконном акте требования по информационной безопасности к Доверенным лицам УЦ ФНС.

ВЫВОДЫ

Изменения закона 63-ФЗ «Об электронной подписи» однозначно являются новым словом в области формирования и использования электронной подписи. Ряд положений очень нужен и полезен для бизнеса. К ним относятся, например, положения о технологии облачной подписи и институте доверенной третьей стороны.

Вносимые в закон изменения потребуют существенной перестройки процессов и систем ЭДО у юридических лиц и индивидуальных предпринимателей. Повысится роль и проникновение электронной подписи у граждан, так как их личная ЭП теперь будет применяться не только для их персональных операций, но и для операций, проводимых в интересах компании-работодателя. Закон должен повысить ответственность УЦ и снизить уровень мошенничества с электронной подписью. Вместе с тем, в законе есть и серьёзная проблема, связанная с использованием в качестве основного способа идентификации её очной формы, неоправданное применение требований по идентификации к неквалифицированной подписи, а также другие открытые вопросы.

Считаем, что для того, чтобы закон принес больше пользы, чем вреда, необходимо в течение 2021 года совместными усилиями бизнеса и государства закрыть озвученные открытые вопросы. Сбербанк уже работает по ним и планирует продолжить такую совместную работу.



Всеволод ШЕЙКИН
сотрудник ТК 26

ДРУЖЕЛЮБНЫЕ ПАРОЛИ

ЧАСТИЧНАЯ АУТЕНТИФИКАЦИЯ ПОЧТИ НЕ ИЗУЧЕНА,
НО ПОЛЕЗНА

Несмотря на то что биометрические системы являются более совершенными с точки зрения подделки относительно парольной защиты, они всё же имеют некоторые недостатки, не позволяющие здесь и сейчас отойти от паролей в пользу биометрии целиком и полностью.

ИЗЪЯНЫ БИОМЕТРИЧЕСКИХ СИСТЕМ

Современные банковские биометрические системы в России основываются на сиамской нейронной сети. Данная сеть необходима, когда требуется обучаться по единственному образцу — реальному изображению человеческого лица — и количество «тренировочного материала», в сравнении с которым можно однозначно установить, «подходит» ли данное лицо, ограничено.

Нейросеть представляет лицо в качестве массива основных (опорных) точек (это представление является закрытым и уникальным для каждого банка, именно поэтому, в частности, трудно применить один образец для разных банков — просто потому, что другая система может его не считать), после чего приводит указанный массив к дескриптору — уникальному набору характеристик человеческого лица, чаще всего представимому в виде n-мерного

вектора. Функция преобразования человеческого лица в дескриптор является однонаправленной, то есть по имеющемуся массиву восстановить исходное изображение невозможно. Такие сиамские нейронные сети, однако, допускают некоторое отхождение от стопроцентного совпадения (в частности, если попытку доступа в технологии FaceID произведёт легальный пользователь в солнцезащитных очках, то система, несмотря на имеющиеся опорные точки на переносице и глазах, представит глаза в виде модели чёрных кругов и всё равно аутентифицирует пользователя). При этом растущая публичность людей (огромное количество фото- и видеоизображений) вкупе с развитием технологий 3D-моделирования и 3D-печати позволит создать неидеальные, но близкие к этому образцы практически любого человека, что в силу имеющегося зазора погрешности может привести к успешной аутентификации нелегального пользователя. Математически это будет значить, что имеющийся дескриптор будет пренебрегать определённым количеством координат своего вектора и аутентификация всё равно будет успешной.

Указанный факт подтверждается тем, что, в частности, обойти технологию FaceID можно с помощью очков и

слепка лица или спящего человека (такая атака была показана на конференции Black Hat 2019).

Этим процессом подтверждается то предположение, что в действительности некой (зачастую значительной) частью координат в этих векторах пренебрегают без значительного ущерба для безопасности.

Дополнительной уязвимостью современных систем биометрической аутентификации в банках также является, к сожалению, человеческий, или, вернее сказать, организационный фактор: используемые камеры и микрофоны зачастую покупаются самые дешёвые, что даёт большую погрешность в сличении и сохранении образов.

СТОЙКАЯ СИСТЕМА ВОЗМОЖНА

Парольная защита же не допускает никакого отхождения от стопроцентного совпадения паролей. Современные администраторы безопасности, основываясь на политике безопасности, вынуждены искать определённый компромисс между стойкостью системы и удобством пользования ею. Давно установлено, что бесполезно пытаться заставить пользователя запомнить длинный, но стойкий пароль или же короткий пароль, который будет состоять из несвязанных символов. Однако существуют

методы, которые, используя некоторые предположения о неполном соответствии предъявляемого пароля верному варианту, а также опираясь на зависимость грамматики русского языка, без всякого ущерба безопасности будут предлагать пользователям стойкие и удобные пароли.

При этом рассматриваемые системы не противоречат устоявшимся в Российской Федерации терминам, в частности [1], поскольку нет ограничений на то, какая информация будет использоваться в качестве аутентификационной.

Резюмируя сказанное, можно прийти к очевидному выводу: при больших размерах аутентифицирующей информации (биометрических опорных точек или, в нашем случае, пароля) можно построить стойкую систему, устойчивую к определённому спектру атак, даже при условии некоего пренебрежения некоторыми координатами пароля.

ПОНЯТИЕ ЧАСТИЧНОЙ АУТЕНТИФИКАЦИИ

В настоящий момент в некоторых крупных организациях (в частности, в структурах Почты России) используется следующий механизм защиты: оператор может запросить некоторые символы из пришедших пользователю в сообщении для подтверждения операции. Таким образом, пользователь защищается от компрометации оператором или нарушителем, использующим Shoulder Surfing («атака через плечо» из социальной инженерии) или атаки, основанные на захвате клавиш, своего полного текстового сообщения и/или своего пароля/ПИН-кода.

В общем случае этот механизм обеспечивает защиту от подсматривания: даже зная целый пароль или секретную фразу, злоумышленник не может предугадать, сколько символов и какие из них необходимо в действительности вводить для доступа к системе. Указанный механизм ранее эксплуатировался, в частности, банковской системой Великобритании [2]. Такой механизм ввиду частых утечек баз данных банков в открытый доступ мог бы значительно уменьшить опасность компрометации при условии достаточно

хорошего генерирования необходимых последовательностей со стороны банка. Данная выборка символов называется partial authentication, или частичная аутентификация.

Частичной аутентификацией будет называться процедура аутентификации, в которой в качестве пароля выступает некое подмножество символов реального пароля.

Указанный выше пример с банками Великобритании является как раз относящимся к такой частичной аутентификации. Здесь и далее, чтобы привить устоявшуюся в западном мире терминологию и не вызывать путаницы, будем использовать такой же термин.

Рассмотрим два возможных способа частичной аутентификации.

I

Первый тип — указанный выше способ, когда в качестве пароля используется запрос неких символов из основного пароля.

Некоторые попытки исследовать такой тип аутентификации принимались на Западе. Одной из самых объёмных работ по данной тематике является работа [3]. Несмотря на приведённые выкладки, указанная система совершенно нестойкая. Проведён следующий тест: протестировано 110 000 симуляций с использованием паролей длиной более 8 символов. Отмечено, что 58 % паролей раскрываются полностью после 7 входов в систему, 90 % — после 12 и 99 % — после 19 входов в систему, если используется такая частичная аутентификация.

Однако напрашивается следующая идея: создать систему формирования стойких паролей, но таким образом, чтобы любое разумное подмножество такого пароля имело необходимую стойкость.

Здесь на помощь могут прийти парольные фразы.

Парольные фразы, очевидно, имеют гораздо большую стойкость в сравнении с классическими паролями, но при этом гораздо лучше запоминаются.

Парольные фразы тем не менее тоже подвержены атакам по словарю. Ещё одной значительной уязвимостью может стать следующий вариант.

Представим, что пользователь использует в качестве пароля какую-то распространённую фразу, к примеру, вступление из Евгения Онегина:

*Мой дядя самых честных правил,
Когда не в шутку занемог,
Он уважать себя заставил
И лучше выдумать не мог.*

Очевидно, что такой пароль будет являться крайне стойким и невзламываемым в течение нескольких тысячелетий, если не будет скомпрометирован. Однако такие распространённые фразы, а вернее их хеши, запросто могут быть скомпрометированы, а значит, и добавлены злоумышленниками в свои переборные базы.

К примеру, мы можем обратиться к Трою Ханту, который активно ведёт сайт <https://haveibeenpwned.com>. Трой Хант на указанном сайте выставляет в открытый доступ базы данных слитых почт и паролей, представленных в виде хеша. Изначально в базе данных было 2,6 миллиарда строк. После чистки базы от повторов и лишних записей Хант высчитал, что в ней содержится порядка 1,1 миллиарда уникальных комбинаций адресов электронной почты и паролей. Эти данные могут быть использованы при авторизации пользователя на сайтах. Так вот, первая строчка из четверостишья, указанного выше, пусть и представленная в виде «мой дядя самых честных правил», проверку данного сайта не прошла, то есть где-то она «отметилась».

Эту проблему можно очень хорошо решить с помощью частичной аутентификации, только в качестве запрашиваемых единиц будет не одиночный символ, а целое слово. В нашем примере, если мы запросим, к примеру, 1, 2, 5, 8, 10 слова, то получим «мой дядя правил занемог», что явно не будет иметь ни известный хеш, ни поддаваться обычной логике построения паролей, ни будет уязвимо к атакам по словарю, но при этом будет очень устойчивым паролем.

Дополнительным решением будет являться следующий подход: некая генерация легко запоминаемых предложений, которая будет поддаваться определённым правилам и давать необходимый результат, но при этом не быть распространённой.



Необходимо, таким образом, составить словарную систему, основанную на правилах русского языка и позволяющую генерировать стойкие пароли.

Такую систему можно представить в виде таблицы со столбцами «Прилагательное», «Существительное», «Наречие», «Глагол».

В данную таблицу заносится, к примеру, по тысяче слов, удовлетворяющих условиям. Каждому сотруднику организации, где необходимо организовать парольную защиту на местах, выдаётся по одному случайному слову (или его коду) из указанной таблицы. Условный сотрудник получает пароль вида «Синийслонбыстропишет» или даже «Синийслонбыстропишет $A_1A_2A_3A_4$ », где A_1 – A_4 — числовые коды слов, выданных сотруднику. Данный пароль будет легкозапоминаемым, но при этом очень стойким.

Таким образом, имеется два подхода к организации паролей на основе парольных слов:

1. Частичная аутентификация с запросом некоторого подмножества символов (слов) в распространённой фразе.
2. Создание таблицы парольных слов и выдача указанных паролей по собственным правилам организации сотрудникам.

II

Представим себе следующую ситуацию: некий пользователь ввёл верный логин, но некоторые из введённых символов неверны. При этом иногда даже легальному пользователю не всегда удаётся с первого раза при однозначном обладании паролем правильно аутентифицироваться. В современных условиях даже при спокойном наборе символов возможна ошибка, а в случае набора текста на смартфоне ошибки в нескольких символах появляются постоянно.

Приведённый пример вполне подпадает под определение частичной аутентификации: мы используем для неё

количественно столько же символов, что и для полного пароля, но позволяем себе некоторые из этих символов ввести неверно.

Указанное допущение открывает широкий простор для упрощения доступа к системе легального пользователя и, как ни странно, усложняет жизнь нарушителю (при выполнении определённых условий).

При этом более предпочтительным будет представление пароля в виде вектора (по аналогии с биометрией). Введём следующее определение:

Допустимым множеством паролей будем называть множество векторов, отличающихся от вектора верного пароля ровно на d координат ($d > 0$).

Величину d будем называть глубиной допустимости. Таким образом, мощность множества D допустимых паролей будет равна N^d , а вероятность ложной аутентификации станет равной $P = N^d / N^n$.

Конечно, данный факт значительно снижает стойкость системы.

В частности, для систем, в которых являются допустимыми в качестве символов пароля буквы русского и английского алфавита, цифры и спецсимволы, стойкость уже падает на 2 порядка за каждый d.

Однако надо вернуться к примеру с паролем телефона. В действительности пользователь, который является доверенным и знает пароль, если и ошибается, то чаще всего вводит символ в небольшой окрестности верного символа. Такой окрестный символ, хоть его и нельзя в полном смысле считать верным, всё равно показывает, что пользователь, скорее всего, легален.

В целом поведение легального пользователя отличается от поведения нарушителя. Легальный пользователь в основном авторизуется верно или с небольшими отклонениями («вводит допустимый пароль» в нашей терминологии). В связи с этим логичным выглядит дать легальному пользователю некие привилегии в сравнении с нелегальным.

Глобально возникает вопрос, который является скорее философским: имеет ли аутентификация ровно два исхода? Ведь если существует понятие частичной аутентификации, то можно и аутентифицироваться «не полностью». Получается, что существует некий кубит с точки зрения аутентификации, то есть не полный отказ и не полное подтверждение.

Решением данной проблемы вполне может стать разделение пользователей на уровни доверия (по аналогии с разделением на роли). Современные системы защиты информации вполне могут сохранять, анализировать и учитывать поведение пользователя.

Условно данное разделение может выглядеть следующим образом:

1. Пользователь предъявляет токен, но пароль вводит совершенно неверный (процент совпадения меньше фиксированной величины, не очень

большой или не совпадает длина пароля). Уровень доверия к такому пользователю будет условно *низкий*. При этом, конечно, предусмотрено как повышение уровня доверия (путём ввода верного пароля и вычисления в качестве процента совпадения, к примеру, среднего арифметического), так и понижение (если пользователь продолжает вводить неверные пароли). К такому пользователю разумно применять ограничения, не позволяющие использовать метод тотального опробования: осуществлять небольшую блокировку попыток доступа или полную блокировку, если процент совпадения не поднимается.

2. Пусть пользователь аналогично предъявляет токен, но вводит в качестве пароля другой, но с приемлемым d, при этом указанный процент совпадения у него хоть и невысок, но и не падает. Уровень доверия к такому пользователю будет условно *средним*. Тогда у указанного пользователя можно запросить несколько символов, которые были введены ошибочно, или предложить некий механизм удостоверения личности, доступный только легальному пользователю (к примеру, отправка сообщения с кодом на телефон).

3. Пользователь предъявляет токен и вводит пароль с одним-двумя неверными символами (для стандартного пароля из 8 символов), уровень доверия к такому пользователю назовём условно *высоким*. Такому пользователю, очевидно, нет смысла чинить препятствия во вводе пароля или замедлять его следующую попытку. Однако если такой пользователь ошибается в одном символе, причём неверные символы находятся в небольшой окрестности от верных (вокруг на клавиатуре) или не совпадает регистр/раскладка клавиатуры, то в зависимости от проводимой политики безопасности, если уровень доверия к пользователю традиционно высок, имеет смысл даже допустить его аутентификацию.

В действительности редкий легальный пользователь дойдёт до процедуры замедления или ввода условной капчи. При этом данная идея вполне коррелирует со сказанным ранее: если в наличии «опорные точки» (размерность пароля, количество букв/цифр/символов), но пользователь вызывает высокое доверие у системы на основании предыдущих попыток аутентификации, то не только не имеет смысла чинить ему препятствий, но и можно в некоторых случаях разрешить ему аутентифицироваться.

В зависимости от политики безопасности можно строить адекватные модели, которые можно обсчитывать и принимать в качестве величины «допустимости» для окрестных символов условное или вполне конкретное значение.

В таком случае идея с парольными фразами приобретает новый смысл. Таблицы, идея которых приведена выше, могут иметь в себе элементы, несоотносимые с точки зрения русского языка, например прилагательные, не сочетающиеся с существительными («белое кружка»). Такую конструкцию можно вполне использовать и данное решение не будет обосновано ни логикой, ни зависимостями в построении фразы, однако при достаточно длинной фразе можно будет принять её в качестве верной.

Эти идеи могут варьироваться и формулироваться индивидуально, однако глобально они, скорее всего, будут именно такими.

ВЫВОД

Частичная аутентификация, то есть использование подмножества символов реального пароля, в настоящее время почти не изучена. При этом при соблюдении некоторых правил, базирующихся на свойствах пароля, при использовании как парольных фраз, так и просто надёжных паролей, можно получить системы, дружелюбные к пользователю, и при этом достаточно стойкие.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 58833–2020. Защита информации. Идентификация и аутентификация. Общие положения.
2. UK Consumers Association: Bank websites: How safe is yours? Which? Magazine (September 2011), с. 24–27.
3. «Give Me Letters 2, 3 and 6!»: Partial Password Implementations & Attacks, David Aspinall and Mike Just.



Денис БАТРАНКОВ
эксперт BIS Journal

КИБЕРНАЁМНИК? СПЕЦСЛУЖБА? ХУЛИГАН?

АТРИБУЦИЯ КОМПЬЮТЕРНЫХ АТАК: КАК УЗНАТЬ
РЕАЛЬНОГО НАПАДАЮЩЕГО?

Журналисты и политики часто бравируют словосочетаниями «русские хакеры» или «китайские хакеры». Но все ли обвинения реально основаны на доказательствах или это всего лишь попытка найти ещё одну нацию, которая всегда и во всём виновата? Кибератаки проводятся конкретными людьми, с именем и фамилией. При расследовании взломов всегда ставится цель: выявить, кто провёл атаку. Такая задача называется атрибуцией.

ПРЕСТУПНИК ОСТАВЛЯЕТ СЛЕДЫ... ПО ВСЕЙ ПЛАНЕТЕ

Летом 2015 года Лаборатория Касперского сообщила об атаке вредоносного кода Duqu2 на свои сети. Была использована уязвимость нулевого дня. Подозрения пали на спецслужбы Израиля и США, но доказательства предоставлены не были¹.

Единственным достоверным доказательством может быть журнал с компьютера, на котором проводилась атака. Но

¹ <https://www.kaspersky.ru/blog/kaspersky-statement-duqu-attack/8125/>

как к этому компьютеру может получить доступ полицейский из Москвы, если атака идёт, например, из Австралии?

Интернет — глобальная сеть, соединяющая людей из всех стран мира, и атакующие часто используют вычислительные ресурсы в разных странах. Атакующий из одной страны для атаки может легко использовать компьютер из любой другой. Для выявления всей цепочки взаимодействий требуется участие правоохранительных органов всех стран, причём достаточно оперативное — злоумышленнику нельзя оставлять время на замечание следов.

ОРДЕР НА ОБЫСК... ЦРУ

Вот первая проблема атрибуции — скорость получения ордера на обыск. Во многих странах зайти в квартиру к подозреваемому можно только на основании официального запроса и соответствующего официального же ответа.

Вторая проблема атрибуции: в атаках часто обвиняют спецслужбы. Совершенно невозможно просить полицию помочь расследовать атаки, к которым, предположительно, причастно разведывательное управление этой же страны.

В 2013 году Эдвард Сноуден подтвердил, что телекоммуникационную компанию Бельгии взломали сотрудники британской спецслужбы. Это был пример реальной атрибуции и первый случай, когда одна европейская страна атаковала другую².

Если уж Британия ломает «дружественные» страны, входящие в единый блок НАТО, можно только гадать, что они себе позволяют делать по всему миру.

Согласно серии документов Vault 7, которая доступна на Wikileaks, в ЦРУ существует специальная коллекция атакующих утилит, получившая название Umbrage. Этот набор программ используется, чтобы отвести подозрения от себя, запутать расследование и выдать свои атаки за чужие³. Поэтому, если в дело вступают спецслужбы, провести атрибуцию практически невозможно: они будут атаковать из чужой страны чужими утилитами.

² <https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/>

³ <https://theconversation.com/wikileaks-vault-7-reveals-staggering-breadth-of-cia-hacking-74236>; https://ru.wikipedia.org/wiki/Vault_7#%D0%ABUmbrage%D0%BB



ПОДНЯТЬСЯ НА УРОВЕНЬ... КИБЕР-ООН

Ещё одну проблему атрибуции можно сформулировать так: хакеры не имеют национальности. Они часто действуют как обычные наёмники: кто заплатил, на того и работают. И единственной возможной защитой является учёт таких людей и проверка того, что они делали во время очередной глобальной кибератаки.

На мой взгляд, в России нужно создать спецподразделение, которое будет заниматься атрибуцией кибератак, учётом хакеров, сотрудничать со всеми странами по всему миру для быстрого реагирования на атаки. Кроме того, это подразделение могло бы выступать на уровне ООН с разоблачениями хакерских групп, основанными на реальных фактах.

К сожалению, на политическом уровне просвета не видно, но в мире на одну атаку спецслужб приходится 1000 атак обычных финансово мотивированных хакеров, которые ломают лишь для получения денег. Будет ещё

много взломов для шантажа и получения выкупа. Атаки криптолокеров уже славятся тем, что они просят за расшифрование данных компаний несколько десятков миллионов долларов. В новостях уже прошла информация о том, что компания Garmin заплатила выкуп 10 миллионов долларов за расшифрование своих данных. В новостях же была история о том, что полицейский участок в США заплатил злоумышленникам, чтобы получить доступ к своим данным.

БЕЗОПАСНИКИ ВСЕХ СТРАН, ОБЪЕДИНЯЙТЕСЬ!

Для отработки и нахождения таких групп злоумышленников требуется сплочённая работа всех стран. Спецслужбы должны обмениваться информацией, заниматься расследованием и поимкой преступников, которые являются международными. Усилиями одной страны в интернете защиту не наладить.

Поэтому атрибуция — это процесс, который должен работать в

каждой стране, работать синхронно, быстро и слаженно. Без этого киберпреступников не победить.

В нашей стране этот процесс пока находится на стадии становления. В Центральном банке работает обмен информацией об угрозах через ФинЦЕРТ. На уровне страны такой процесс должен работать на системе ГосСОПКА, за которую отвечает НКЦКИ ФСБ России. Осталось только найти людей, которые будут заниматься расследованием инцидентов на межгосударственном уровне и проводить атрибуцию кибератак. Без этого все сообщения о том, что очередная группировка атаковала какую-то страну, останутся лишь бездоказательными словами на бумаге либо обычной бравадой реальных хакеров, которые пользуются тем, что никогда не выезжают из своей страны и поэтому чувствуют себя безнаказанно.



Твоя сеть. Твои правила.

Гибкая защита — для растущего бизнеса.

Kaspersky Endpoint Security для бизнеса Универсальный защитит виртуальные и физические рабочие места в любом их соотношении и поддержит ваши планы по развитию корпоративной IT-инфраструктуры.



**Kaspersky
Endpoint Security
для бизнеса
Универсальный**

kaspersky

**АКТИВИРУЙ
БУДУЩЕЕ**

© АО «Лаборатория Касперского», 2020.
Зарегистрированные товарные знаки и знаки обслуживания
являются собственностью их правообладателей.

ДиалОгНаука

**СИСТЕМНАЯ ИНТЕГРАЦИЯ В ОБЛАСТИ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

dialognauka.ru

KASPERSKY.RU/BUSINESS



Ольга ЛИМОНОВА
психолог
ООО «Антифишинг»



Андрей ЖАРКЕВИЧ
редактор
ООО «Антифишинг»

КАК ПРОБУДИТЬ ДВИЖУЩУЮ СИЛУ

МОТИВАЦИЯ ПЕРСОНАЛА К ОБУЧЕНИЮ И ТРЕНИРОВКАМ ИБ

В различных организациях можно наблюдать любопытное явление: на словах все сотрудники согласны с важностью информационной безопасности, но когда дело доходит до обучающих курсов и тренировок, появляется негатив.

Причина такого отношения в том, что при планировании обучения сотрудников навыкам безопасного поведения никто не учитывал их мотивацию. Между тем именно мотивация — движущая сила связанных с персоналом процессов. Без неё невозможно добиться заданных результатов, особенно в долгосрочной перспективе.

В этой статье мы расскажем о значении мотивации при взаимодействии с сотрудниками, о видах мотивации и наиболее эффективных форматах применения мотивации для повышения осведомлённости сотрудников компании в области ИБ.

МОТИВАЦИЯ И ЕЁ ЗНАЧЕНИЕ В ФОРМИРОВАНИИ НАВЫКОВ ИБ

Цель повышения осведомлённости сотрудников в области ИБ — развитие базовых компетенций, то есть навыков, важных для решения

потенциальных проблем безопасности в компании. Инвестирование в человеческий ресурс путём систематического обучения и тренировки повышает уровень зрелости в реагировании на инциденты и улучшает защиту корпоративных ресурсов от кибератак, большая часть которых происходит через воздействие на сотрудников.

Таким образом, для улучшения защиты нужно научить людей реагировать правильно. Но как этого добиться?

Есть три ключевых элемента, влияющие на формирование навыков (рис. 1):

1. Знания — теоретическая база.
2. Умения — практическая отработка полученных знаний в реальной жизни.
3. Мотивация, которая формируется из понимания ценности приобретаемого навыка и становится драйвером для успешного освоения первых двух элементов.

И если знания можно получить на обучающих курсах, а умения — отработать с помощью имитированных атак, мотивация остаётся слепым пятном для большинства ИБ-специалистов, поскольку эту проблему сложно решить стандартными организационными или техническими средствами. Практика показывает, что без системы мотивации даже один короткий и качественный базовый курс по ИБ проходят меньше половины сотрудников.

Конечно, эта ситуация во многом зависит от типа организации. В более консервативных компаниях повлиять на сотрудников проще. Но если разобраться, то выяснится, что там просто эффективнее используется система мотивации по типу «кнута». В демократичных компаниях со смузи и печеньками предпочитают мотивацию «пряниками», но сути это не меняет. Именно система мотивации позволяет эффективно управлять сотрудниками.

В компаниях без корпоративной культуры о необходимости как-то стимулировать персонал часто вообще забывают, считая эти «психологические изыски» блажью руководителей и специалистов по обучению персонала, а не важным для организации элементом управления.



Рисунок 1. Ключевые элементы, влияющие на формирование навыков

Мотивация — это причины, которые побуждают человека к устойчивому целенаправленному действию.

Зрелые компании стремятся управлять мотивацией своего персонала, в том числе в области ИБ. Чтобы убедить людей серьёзно относиться к информационной безопасности и адекватно реагировать на угрозы или обязательное обучение, важно внедрять разные способы мотивации в процессы ИБ, в первую очередь — в программы обучения и информирования.

СПОСОБЫ МОТИВАЦИИ СОТРУДНИКОВ В ИБ

Мотивация никогда не бывает постоянной и одинаково ценной для всех сотрудников. К большому сожалению, в природе не существует лучшего или универсального способа мотивации. Способы мотивации — это инструменты, которые вовлекают людей в какой-либо процесс, делая его максимально гибким и дружелюбным для самого разнородного коллектива.

На практике нематериальные способы стимулирования помогают достичь желаемого результата быстрее, чем денежные. Исходя из этого, далее мы сосредоточимся на нематериальных способах мотивации, которые специалисты по ИБ могут использовать для выстраивания наиболее эффективного процесса обучения и тренировки навыков безопасного поведения сотрудников.

Сделайте обучение и тренировки ИБ частью корпоративной культуры. Внедрение информационной безопасности в корпоративную культуру компании требует последовательной системной работы. Выстроенная учебная программа должна наглядно показывать, что информационная безопасность является неотъемлемой частью работы каждого сотрудника, а ответственность за её соблюдение должна быть прописана в должностных инструкциях.

Угрозы и технологии атак постоянно изменяются, поэтому обучающие материалы и тренировочные атаки должны поддерживаться в актуальном состоянии. А чтобы сотрудники были в курсе этих изменений, стоит регулярно повторять обучение и проводить тренировки. Кроме того, у сотрудников всегда должен быть свободный доступ к данным материалам для дополнительного ознакомления.

Вплетая регулярное обучение и тренировки в рабочие процессы, постепенно можно добиться снижения негатива и более ответственного отношения к ИБ-процессам.

Очевидно, что проведение учебных занятий раз в год приводит к тому, что кибербезопасность — последнее, о чём думают сотрудники.

Редкие тренировки также создают ошибочное представление о том, что безопасность — это забота специализированного подразделения.

Определите глобальный смысл обучения для вашей компании. Каждый сотрудник вносит свой вклад в общий успех компании, но не все видят это. Сотрудники с ограниченным перечнем служебных обязанностей могут ощущать себя «винтиками», работа которых — банальная рутина, так что нет смысла тратить рабочее время на какое-то там назначенное обучение, лучше уж отсканировать пару лишних досье.

В связи с этим очень важно, чтобы учебная программа по ИБ имела смысл для каждого сотрудника. Если они не смогут понять, какова конечная цель их обучения, они не станут вкладывать в него свои силы и время.

Глобальный смысл обучения показывает сотрудникам, насколько жизненно важны их усилия для достижения определённых целей в масштабах всей организации. Такой целью может быть, например, защита компании от кибератак, и тогда обучение и тренировки ИБ-навыков приобретают смысл, создавая у сотрудников чувство сопричастности и ответственности за успех и прибыль всей компании.

Этот подход помогает сотрудникам стать более мотивированными и увлечёнными своей работой, поскольку они понимают, как ценна их работа для общего успеха компании.

Установите чёткие ожидания от обучения и тренировок. Если вы не можете определить конечную цель обучения и тренировок, прописать сценарии желаемого нового поведения сотрудников, обозначить, в чём и как оно должно проявляться, то и сотрудники не будут понимать, зачем им это обучение нужно. Важен наглядный, качественно ощущаемый результат, который позволит и вам измерять успешность обучения, и самим сотрудникам отслеживать его, давая возможность гордиться собой.

Внедряйте обучение через руководителей на местах. Привлекайте к внедрению обучения ИБ руководителей и ключевых лиц, принимающих решения. Они обеспечат соблюдение персоналом установленных правил ИБ и помогут проконтролировать процесс обучения, обеспечив дополнительную стимуляцию, поскольку для подчинённых они имеют больший авторитет, чем специалисты ИБ-отдела.

Руководители могут и должны подавать пример своим подчинённым. Эффективным решением может стать разработка отдельного курса обучения ИБ для руководителей, который будет давать углублённые знания для поддержания контроля на местах и противодействия



продвинутым атакам, целью которых часто являются именно руководители. Оптимально, чтобы такой курс был компактным по объёму, чтобы даже загруженный работой руководитель смог выбрать время для его изучения.

Используйте обучение для улучшения рабочих процессов. Многие сотрудники сталкивались с тем, что внедрение новых систем или процессов снижает их производительность, вынуждая задерживаться по вечерам или работать в выходные.

Новые процессы, связанные с обучением и тренировкой навыков ИБ, также могут временно сделать сотрудников менее эффективными, однако конечной целью обучения всё-таки должно быть улучшение рабочего процесса.

Во многих случаях сотрудники сами знают, как повысить производительность, и им просто не хватает инструментов или конкретных знаний для реализации своего потенциала. Обучение ИБ должно давать эти самые инструменты и знания. Будьте готовы принимать обратную связь от сотрудников, дайте им возможность вносить свои идеи, предложения и коррективы в политику безопасности компании. Это не только улучшит качество и результат работы, но и повысит вовлечённость персонала в процессы и сформирует здоровый энтузиазм.

Используйте в обучении контекст работы вашего персонала. При разработке материалов

для информирования по ИБ опирайтесь на реальный контекст работы ваших сотрудников. Избегайте абстрактных примеров, неприменимых к актуальной рабочей среде. Максимально релевантные отсылки и примеры из естественной среды компании создают практическую ценность для людей в процессе обучения.

Поддерживайте контакт с сотрудниками и между ними во время обучения. Введение социального элемента в обучение всегда полезно. У сотрудников должна быть возможность в режиме реального времени обсуждать возникающие вопросы в обучении как между собой, так и со специалистами по ИБ. Активное общение позволяет сотрудникам чувствовать себя частью группы, работающей над общей целью, и благотворно сказывается на уровне информационной безопасности компании.

Убедитесь, что у ваших сотрудников есть инструменты для поддержания дистанционного контакта между собой и с вами. Это может быть корпоративный чат для обмена мгновенными сообщениями, в котором поощряются неформальные разговоры между коллегами.

Давайте обратную связь по итогам обучения и тренировок. Отсутствие обратной связи по итогам обучения или тренировок оказывает демотивирующий эффект. У человека создаётся ощущение, что он напрасно потратил время, а все усилия бессмысленны.

Чтобы этого избежать, обязательно измеряйте, фиксируйте и давайте обратную связь сотрудникам по итогам обучения и тренировок. Моментальный фидбэк — лучшая форма поддержания контакта с персоналом.

Очень ценно публично делиться историями успеха пользователей, которые помогли предотвратить проблемы безопасности, например, обнаружили целевое фишинговое письмо. Это показывает практическую значимость используемого обучения и тренировок, позволяет сотрудникам почувствовать себя героями.

Такие истории могут быть реализованы в виде тематических рассылок или публикаций в корпоративном блоге, в которых показывается, сколько утечек информации произошло с момента последнего обучения или тренировки и сколько было устранено благодаря повышению уровня ИБ-навыков сотрудников.

Индивидуализируйте обучение. Каждый сотрудник должен научиться правильно реагировать на любые проблемы безопасности: выявлять угрозы и своевременно сообщать о них. Но если вы пытаетесь сформировать такое поведение у сотрудников посредством шаблонного типового обучения, это оттолкнёт их и усилит настроения «мне всё равно» и «это скучно». Людям трудно воспринимать знания, которые они не могут соотнести с собой, с тем, что они читают, видят или слышат.

Сегментируйте учебную программу в соответствии с имеющимися отделами. Добейтесь, чтобы содержание учебных курсов соответствовало фактической работе каждого человека. Ставя людей на первое место и персонализируя учебные материалы в соответствии с их ролью в компании, уровнем знаний и интересом к кибербезопасности, вы обеспечите обучение, которое вовлекает и мотивирует.

Определяйте сильные стороны сотрудников и акцентируйте на этом внимание. Положительные оценки усиливают вовлечённость, в то время как отрицательные почти наверняка вызовут психологическую отстранённость от процесса обучения.

Если во время обучения у сотрудника повышается чувство собственного достоинства, компетентности и самоопределения, его внутренняя мотивация возрастает. Чтобы добиться такого эффекта, выдавая обратную связь, акцентируйте внимание на сильных сторонах сотрудника, на его успехе, способствуя лояльности и удержанию внимания.

Когда обратная связь наполнена ошибками и неудачами, у сотрудника появляется неуверенность в себе, снижается самооценка и портится настроение. Разумеется, в таком состоянии

нет никакого желания продолжать обучение, а задетые чувства в дальнейшем могут влиять на поведение сотрудников, начиная с конфликтов и заканчивая совершением небезопасных действий «назло».

Подчеркивайте долгосрочные перспективы обучения и его влияния на карьерный рост. Личный интерес всегда превалирует над общественным, поэтому важно, чтобы, кроме понимания смысла обучения ИБ для компании, сотрудники видели личную выгоду данного обучения, понимали, как оно влияет на их карьерные перспективы.

Покажите сотрудникам, какие преимущества даст им обучение ИБ, как оно поможет им в повседневной работе, какие ценные знания и навыки они приобретут в краткосрочной и долгосрочной перспективе.

Предлагайте сотрудникам возможности карьерного роста. Например, в корпоративных стандартах можно прописать, что для получения руководящей позиции требуется пройти на N часов/курсов обучения больше, чем требуется для рядового сотрудника. Соответственно, каждый сотрудник, желающий стать руководителем, будет проявлять больший энтузиазм и усерднее обучаться ИБ, что логически соответствует возрастающему уровню ответственности.

Разумеется, такие перспективы должны быть настоящими. Если всё это останется только бумажным обещанием, в качестве мотивирующего фактора оно не сработает. При отсутствии реальных и релевантных преимуществ страстная вовлечённость в обучение маловероятна.

Также для сотрудников будет ценно понять важность кибергигиены не только на рабочем месте, но и дома. Учите пользователей конфиденциальности, безопасности и тому, как уроки, полученные на работе, могут применяться дома и в личной жизни. Это повысит ощущаемую ценность обучения и мотивацию к нему.

Делайте из сотрудников экспертов-помощников. Скорее всего, в вашей компании уже есть скрытые эксперты-помощники, которые обладают знаниями в области ИБ благодаря пройденному обучению или личному интересу. Выявляйте и используйте этот потенциал для улучшения процессов безопасности. Признание приобретённого опыта важно, как и возможность обмена им с другими сотрудниками.

Используйте обучающую платформу, чтобы выделять экспертов-помощников, так называемых ИБ-чемпионов. Их можно определять по активному взаимодействию с отделом ИБ и другими сотрудниками и высоким оценкам за обучение и тренировки.

Это один из шагов в направлении развития культуры обмена знаниями. Как только вы это сделаете, эксперты-помощники почувствуют себя полезными и нужными, а другие сотрудники увидят, к кому можно обратиться на местах по вопросам ИБ. Часто задать вопрос коллеге из своего отдела психологически проще, чем обратиться к незнакомому сотруднику из «грозного» отдела ИБ.

Включите в систему обучения элементы соревнования. Дух соревнования — отличный способ мотивации подчинённых. Люди любят, когда им бросают вызов. Они хотят чувствовать себя сильными, способными, полезными, умными. Для них важно чувствовать, что они чего-то достигают и способны выполнять сложные задачи.

Информируйте коллектив о личных достижениях каждого работника. Составляйте рейтинги, например, топ-5 «ИБ-сильных» отделов в компании или сотрудников в отделе, проводите ежегодные мини-соревнования с символическим вознаграждением. Это поможет интегрировать информационную безопасность в корпоративную культуру и сделает её нескучной для рядовых сотрудников.

Избавьте людей от страха неудачи. Для многих людей изучение нового материала является тревожным опытом. Работник может опасаться, что приобретение новых навыков добавит ему ответственности после обучения. Контекст обучения и негативная обратная связь тоже могут вызывать стресс, особенно если у сотрудника проблемы с самооценкой и уверенностью в себе.

Чтобы противостоять страху неудачи, помогите сотрудникам понять, что новые знания — признак силы, который демонстрирует высокую степень самосознания, готовности совершенствоваться и становится образцом для других.

Важно, чтобы выгода от обучения была более значимой, чем ошибки и неудачи. Проваленная имитированная атака не должна становиться «пятном позора». Наоборот, стоит объяснить сотруднику, что его «насмотренность» теперь выше, чем у тех, кто не сталкивался с атаками. В обучении и тренировках важна выдержка и готовность ошибаться, не теряя энтузиазма.

Работайте с негативом. Соппротивление переменам и всему новому — естественная реакция, в том числе в процессе обучения и тренировки навыков ИБ. Необходимо планомерно преодолевать убеждение, что «компания проводит обучение ради обучения». Собирайте типовые жалобы, оправдания и претензии сотрудников по поводу системы обучения ИБ и формируйте базу аргументированных ответов.

Если сотрудник испытывает негатив по отношению к обучению, значит, вы не донесли до него пользу и значимость данного процесса.

Используйте гибкий график обучения и тренировок. Гибкий график обучения даёт множество преимуществ, главные среди которых — комфорт сотрудников и возможность оптимально управлять своим временным ресурсом. В случае дистанционного обучения это достигается путём предоставления относительно длительного интервала обучения, чтобы сотрудники смогли выбрать оптимальный момент для обучения или тренировок.

Используйте разные интерактивные материалы и геймификацию в обучении. Обучение не должно быть скучным. Используйте разные форматы для разных сотрудников: подготовьте печатные материалы, привлекательные информационные бюллетени для рассылок по электронной почте, смонтируйте видео, запишите подкаст или разработайте обучающую корпоративную игру. Это не так сложно, как принято считать.

Главное — убедиться, что эти инструменты обучения предназначены для привлечения различных типов людей, которые работают в вашей компании. Молодые сотрудники лучше реагируют на геймифицированное обучение. Зрелые сотрудники могут предпочесть традиционный подход к обучению, связанный с печатными раздаточными материалами. Качественное интерактивное обучение всегда персонализировано и направлено на определённую категорию людей, а не «для всех одно и то же».

* * *

Мотивированный сотрудник показывает лучшие результаты в обучении и служит катализатором в интенсификации обучающего процесса для своих коллег. Именно поэтому мы считаем построение правильной мотивации важнейшей частью процесса обучения и тренировки навыков безопасного поведения сотрудников.

Рассмотренные в статье способы мотивации можно использовать в любом порядке, главное — подходить к процессу творчески, учитывая как сложившиеся в трудовых коллективах традиции, так и уровень подготовки сотрудников и даже особенности взаимоотношения между подразделениями.

В любом случае время, потраченное на построение системы мотивации, окупится сторицей в виде повышения уровня защищённости компании от кибератак, а также в виде развития корпоративной ИБ-культуры.

ОБМАНУТЬ, ЧТОБЫ ЗАЩИТИТЬ

БАЗОВЫЕ ПРИНЦИПЫ СОЗДАНИЯ ИМИТИРОВАННЫХ ФИШИНГОВЫХ АТАК

Один из распространённых способов проверки защищённости корпоративной сети от кибератак — проведение тестирования на проникновение. Для этого обычно нанимаются независимые компании или эксперты, которые применяют для проверки инструменты, аналогичные тем, которые применяют киберпреступники в реальных атаках. Такая проверка называется пентестом — от Penetration Testing (тестирование на проникновение).

Используя уязвимости оборудования, операционных систем и приложений, а также ошибки в их конфигурации, пентестеры проникают в сеть компании и далее могут провести внутри сети дополнительные проверки в зависимости от договорённости с заказчиком. Полученные в результате пентеста замечания обычно становятся руководством по устранению недостатков защиты и уязвимых настроек для ИТ- или ИБ-подразделений.

И хотя технические векторы по-прежнему широко используются в ходе кибератак, все эксперты отмечают стремительный рост фишинга в качестве способа для первичного проникновения в систему или кражи учётных данных от корпоративных систем.

Наиболее эффективным способом повышения устойчивости сотрудников к фишингу является тренировка навыков безопасного поведения с помощью имитированных атак. По итогам проведённого «Антифишингом» исследования выяснилось, что сотрудники, которые прошли такие тренировки, вели себя безопасно в 49% случаев, в то время как сотрудники, получившие только теоретические знания, — всего в 9% инцидентов.

Таким образом, проведение тренировок сотрудников навыкам безопасного поведения является необходимым условием повышения защищённости корпоративной сети.

От качества имитированной атаки напрямую зависит уровень получаемых сотрудниками навыков: если атаки будут слишком простые, люди будут легко их распознавать, а столкнувшись с более сложными вариантами, окажутся в роли жертвы. Именно поэтому построение

имитированных атак требует взвешенного подхода с учётом тонкостей, о которых мы поговорим далее в этой статье.

ОБ ИМИТИРОВАННЫХ АТАКАХ

Имитированная фишинговая атака — своеобразный пентест сотрудника. Она отличается от реальной только отсутствием вредоносного «заряда». В результате успешной имитированной атаки компания не понесёт финансовых потерь или репутационных рисков, её работа не остановится. Единственной реальной жертвой таких атак будет сотрудник, ставший жертвой обмана. Но и в этом случае этот обман становится мощным мотивом для повышения осведомлённости в сфере безопасности и дополнительной тренировки навыков распознавания мошеннических посланий.

Процесс создания имитированных фишинговых атак можно описать как игру или соревнование. Как и в случае с реальной кибератакой, задача создателя имитированной атаки — перехитрить пользователя и убедить его выполнить целевые небезопасные действия.

Рассмотрим несколько принципов создания имитированных фишинговых атак, которые делают их успешными.

ПРИНЦИП 1. ЗНАТЬ СВОИХ ЖЕРТВ И ПОНИМАТЬ ИХ ПСИХОЛОГИЮ

От специалиста, который создаёт имитированные фишинговые атаки, требуется не только иметь психологические навыки и владеть приёмами социальной инженерии, но и уметь ставить себя на место других людей. Только таким образом можно с достаточной степенью

Сотрудники, которые прошли тренировку навыков безопасного поведения с помощью имитированных атак, вели себя безопасно в 49% случаев, в то время как сотрудники, получившие только теоретические знания, — всего в 9% инцидентов



**Виталия
ДЕМЕХИНА**
разработчик
имитированных
атак
ООО «Антифишинг»

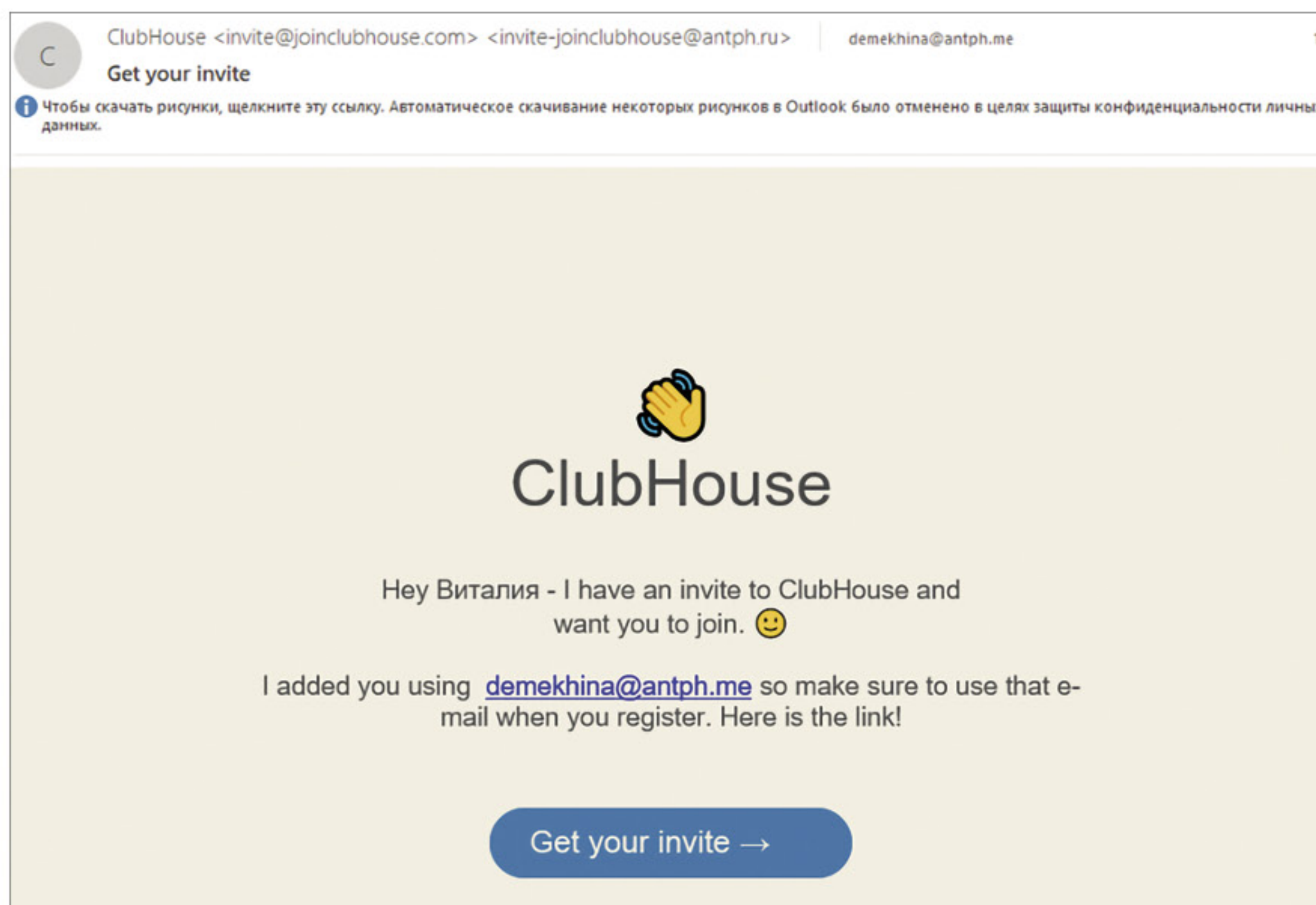


Рисунок 1. Атака, имитирующая приглашение в новую социальную сеть ClubHouse

достоверности понимать, вызовет ли текст письма необходимые эмоции или нет.

Если в компании значительная часть сотрудников — женщины в возрасте до 35 лет, имеющие 1–2 детей, то с большой вероятностью эффективными будут письма, в которых предлагаются различные льготы, скидки или подарки, связанные с «детской» темой. Например, сильный отклик наверняка вызовет предложение принять участие в конкурсе на освободившиеся места в корпоративном детском саду с углублённой подготовкой к школе.

Для молодёжной аудитории более эффективными будут имитированные атаки, связанные с модными трендами.

Например, атака, имитирующая приглашение в новую социальную сеть ClubHouse (рис. 1), с большой вероятностью покажет высокую эффективность в компаниях с молодыми сотрудниками. Однако есть вероятность, что и более взрослая аудитория попадётся на это приглашение, поскольку ClubHouse в течение некоторого времени присутствовал в новостях телевизионных каналов.

В компаниях с сотрудниками возраста 50+ также можно возбудить интерес к данной социальной сети с помощью связки из двух фишинговых писем, первое из которых создаёт любопытство, сообщая о запуске сети, а вторая уже непосредственно атакует человека через поддельное приглашение.

ПРИНЦИП 2. ЗНАТЬ МАТЧАСТЬ

Подготовка имитированной фишинговой атаки практически полностью включает в себя этапы, аналогичные разработке реальной. Один из обязательных этапов — сбор информации о компании-жертве и её сотрудниках. От полноты собранной информации напрямую зависит её результативность, а значит, специалисту необходимо знать матчасть — уметь искать информацию и сопоставлять собранные сведения.

Для сбора информации из открытых источников используются методы OSINT — Open Source Intelligence. Это направление киберразведки предполагает использование социальных сетей, форумов, игровых платформ, а также публикаций в СМИ для поиска информации о человеке.

Поиск и обработка таких объёмов информации вручную — весьма трудоёмкое занятие. Для автоматизации процесса имеется ряд утилит, которые с пристрастием ищут заданного человека на сотнях или даже тысячах сайтов, например:

- ◆ Snoop — 1600 сайтов;¹
- ◆ Spiderfoot — 350 сайтов;
- ◆ Sherlock — 350 сайтов;
- ◆ Whatsmyname — 290 сайтов;
- ◆ Namechk — 100 сайтов.

¹ <https://habr.com/ru/post/488432/>

Помимо поиска, специалист должен иметь целый набор дополнительных технических навыков для составления шаблона письма, вёрстки фишинговой страницы и убедительной имитации реальной атаки.

ПРИНЦИП 3. СОСТАВЛЯЙТЕ СЦЕНАРИИ И ВЕДИТЕ ЖЕРТВУ ЗА РУЧКУ

Эффективная имитированная атака требует серьёзных затрат времени. Просто набросать продающий нейрокопирайтинговый НЛП-текст недостаточно. Люди давно перестали верить таким письмам, даже если к ним обращаются по имени. Многочисленные утечки данных о клиентах банков в 2019–2020 годах и последовавшие массовые рассылки и обзвоны выработали у многих граждан своеобразный цифровой иммунитет. Они уже не поддаются на примитивные схемы.

Для создания сильных эмоций нужно применять приёмы из арсенала драматургов и сценаристов, прорабатывая модель обстоятельств, в которых находится жертва, а также её душевного состояния.

Мы используем двухэтапное проектирование. По нашему опыту, это оптимальный способ. На первом этапе создаётся сценарий: мы проектируем структуру атаки, определяем, какие эмоции нужно задействовать у жертвы и какие психологические «крючки» для этого можно использовать.

Второй этап — визуализация разработанного сценария в виде шаблона атаки. Сильный сценарий → сильный шаблон → успешная атака.

Если атака базируется на слабом сценарии, даже супервизуализация не поможет сделать сильный шаблон. Сильный сценарий ведёт жертву за ручку по заданному пути с момента возникновения эмоций до выполнения целевого действия.

ПРИНЦИП 4. ИСПОЛЬЗУЙТЕ ИНФОПОВОДЫ

Происходящие в мире, стране или компании события просто кладёшь в возможные сценарии для атак, которые активно используют злоумышленники. Например, тема пандемии коронавируса лидировала не только в заголовках новостей, но и в темах фишинговых писем в течение 2020 года.

Специалист по созданию имитированных фишинговых атак также просто обязан использовать любые информационные поводы для создания новых шаблонов. Для этого следует отслеживать события, наполняющие жизнь потенциальных целей атак.

Многочисленные утечки данных о клиентах банков в 2019–2020 годах и последовавшие массовые рассылки и обзвоны выработали у многих граждан своеобразный цифровой иммунитет

Кроме случайных инфоповодов, есть и регулярные. Это праздничные дни и различные знаковые даты — Новый год, Рождество, День святого Валентина, чёрная пятница, спортивные события, например чемпионаты по различным видам спорта. В эти дни почтовые ящики переполнены письмами с поздравлениями, выгодными предложениями, акциями и скидками. Среди них с лёгкостью могут спрятаться письма мошенников и специалистов по имитированным атакам.

К регулярным инфоповадам также можно отнести и события, связанные со сменой сезонов. Например, летом многие семьи стремятся выехать на отдых на море, а значит, на них может сработать «выгодное предложение» тура в роскошный отель.

Поскольку ни один праздник не приходит неожиданно, шаблоны имитированных атак, приуроченных к таким дням, можно использовать повторно каждый год, творчески дополняя с учётом изменившихся трендов и локальных инфоповодов.

ЗАКЛЮЧЕНИЕ

Слишком простые атаки могут создать у обучаемых опасную иллюзию полученного навыка. При реальном инциденте это приведёт к тому, что они не смогут распознать мошенническое письмо, обеспечив киберпреступникам возможность похитить учётные данные или проникнуть в систему.

Обеспечить разумный баланс между уровнем сложности и эффективности имитированных атак поможет следование приведённых в статье принципов:

1. Изучайте своих жертв и их психологические особенности.
2. Научитесь профессионально использовать инструментальные средства для создания имитированных атак.
3. Уделите время разработке качественного сценария имитированной атаки, который будет удерживать внимание жертвы и создавать необходимые эмоции.
4. Следите за информационными поводами и календарными праздниками, чтобы создавать реалистичные и результативные имитированные атаки.

«СЕРЕБРЯНАЯ ПУЛЯ» ПРОТИВ МОШЕННИЧЕСТВА

КРОСС-КАНАЛЬНАЯ СИСТЕМА
ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВУ



Игорь ШУЛЬГА
директор центра
противодействия
мошенничеству
компаний
«Информзащита»

Согласно отчёту ФинЦЕРТ Банка России, процент мошенничеств по отношению к физическим лицам с использованием методов социальной инженерии (смишинг, вишинг, фишинг, подмена номеров телефонов, переадресация вызовов, компрометация корпоративных электронных почтовых ящиков, кража личности, в том числе цифровой, и др.) составил порядка 97 % от общего объёма, и это около 1 млрд рублей с начала по декабрь 2019 года. Данные предоставлены финансовыми институтами в рамках обязательной ежемесячной отчётности по форме 0403203, в рамках которой отображаются именно причины зафиксированных несанкционированных операций.

ВВЕДЕНИЕ

Бурное развитие рынка дистанционных каналов предоставления услуг клиентам, появление новых продуктов и услуг значительно увеличило поверхность атаки для мошенников. В то же время усилилось именно адресное фокусирование мошенничества с учётом информации об уязвимостях того или иного продукта или услуги. Наряду с ростом профессиональной подготовленности мошенников, их организованности в группировки (в том числе совместно с криминальными структурами и с распределённой юридической подотчётностью, что усложняет их привлечение к ответственности), значительных инвестиций в R&D для улучшения своих инструментов, большую роль в этом сыграла инсайдерская информация (внутреннее мошенничество). Эти факты часто находили отражение в докладах профильных специалистов по изучению теневого рынка в сети Интернет.

Всё это требует концентрации внимания финансовых институтов над этой проблематикой. Необходимо взвешенно подойти к вопросам внедрения своих продуктов, услуг, а также проектирования систем противодействия мошенничеству. В настоящий момент в большинстве случаев такие системы являются моноканальными, то есть одна система предназначена для банковских карт, вторая — для системы

дистанционного банковского обслуживания физических лиц, третья — для внутреннего мошенничества и так далее. Параллельно с ними существуют в своём контуре системы информационной безопасности и сессионного антифрода, интеграция с сотовыми операторами. Да, систем много, все они нужны, но проблема в том, что мошенники активно стали развивать и использовать кросс-канальные атаки.

Что такое кросс-канальные атаки? Простой способ для мошенников, но практически нерешаемый для систем противодействия мошенничеству и систем информационной безопасности в их текущем исполнении. Это происходит из-за природы развития атаки: начинается она со звонка в кол-центр банка с номера телефона клиента, продолжается попыткой регистрации на себя приложения мобильного банка клиента, затем сопровождается звонком с номера телефона банка клиенту. Далее возможны попытки входа в кабинет интернет-банка с устройства реального клиента, и только потом могут последовать операции с платежами, переводами. Возможно, эти попытки будут зафиксированы во всех перечисленных выше системах, но они никак не будут связаны как одно мошенническое действие, происходящее в определённый отрезок времени по отношению к конкретному клиенту или устройству клиента. Таким образом, атака, возможно, будет замечена только транзакционной системой противодействия мошенничеству. Идеальных систем такого рода не существует. Даже при хороших аналитиках и настройках системы будут пропускаться мошеннические операции.

Напрашивается очевидное, но непростое с точки зрения проектирования и процессов интеграции решение по кросс-канальному мониторингу в единой системе противодействия мошенничеству (рисунок 1).

Следует отметить, что расчёт оценок подозрительности операции может вестись с абсолютно разными метриками. Их нормализация и корреляция друг с другом может быть отдельной задачей, которая зачастую ложится на решение сотрудника, то есть свои ошибки вносит человеческий фактор.

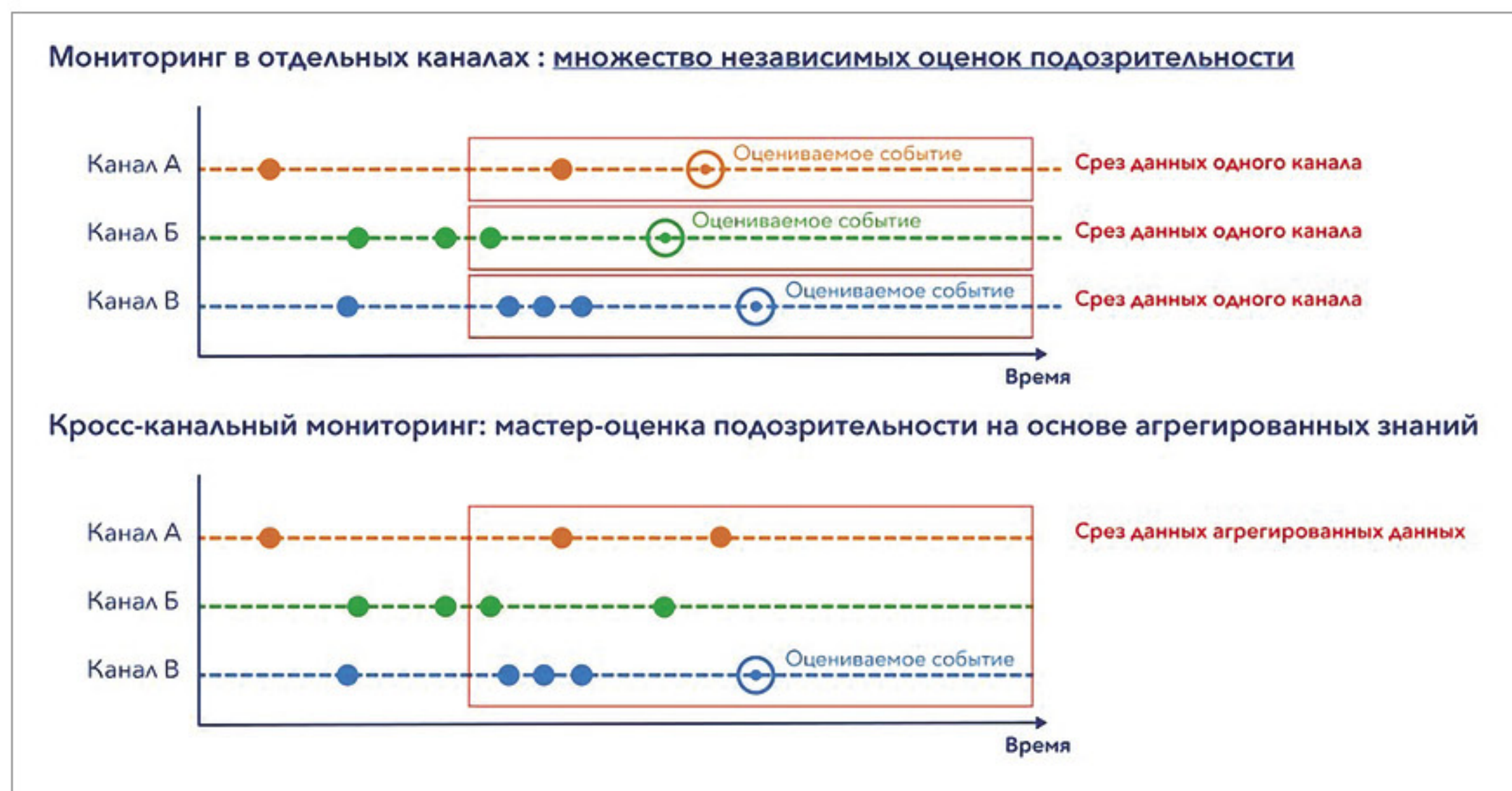


Рисунок 1. Концепция построения единого профиля клиента во времени

ОТ ТЕОРИИ К ПРАКТИКЕ

Преимущества мультивендорных систем и негативное влияние на концепцию единого профиля.

Следует выделить следующие преимущества:

- ♦ возможность максимально выполнить техзадание;
- ♦ конкурентное снижение стоимости решения;
- ♦ различные компенсации за доработки;
- ♦ диверсификация рисков.

Но в тот же момент начинают увеличивать своё влияние и негативные факторы:

- ♦ отсутствие общей архитектуры решений;
- ♦ недостаток компетенций сотрудников по работе комплекса систем;
- ♦ непонимание сути интеграционного взаимодействия и моделирования данных для единого профиля;
- ♦ разрозненные проектные команды;
- ♦ разные команды сопровождения продуктов;
- ♦ сильно растянутое по времени внедрение интегрируемых систем;
- ♦ отсутствие единого идентификатора клиента в интегрируемых системах;
- ♦ разные и несогласуемые форматы временных меток в источниках событий;
- ♦ отсутствие синхронизации времени между интегрируемыми системами;
- ♦ наличие значительного количества связанных данных, что понижает эффективность алгоритмов машинного обучения.

В связи с этим следует принять следующие принципы качественного решения указанных факторов и построения кросс-канальной системы противодействия мошенничеству:

- ♦ обеспечение разработки архитектуры решения с учётом особенностей каждой системы;

- ♦ формирование единой проектной команды, установка тесного взаимодействия всех участников с ролью «Архитектор» и их максимальная доступность для согласования внесения изменений в проект;

- ♦ ведение единой проектной документации по интегрируемым системам и оперативное отражение в ней всех согласованных изменений;

- ♦ все изменения в системах вести с учётом их интеграции в кросс-канал как минимум следующих параметров:

- изменение логики взаимодействия систем;
- изменение набора полей, передаваемых между системами;
- изменения требований к обязательности полей;
- изменение форматов полей;
- изменение наименования полей / их тегов;
- изменение в возможном содержании данных в полях.

ВЫВОД

Кросс-канальная система противодействия мошенничеству — это своеобразный уровень зрелости и ответственности, так как требует согласованного действия многих подразделений в разных компаниях, способных работать не в только в моменте, но и на долгие годы вперёд. Только так решение будет обладать достаточным качеством, чтобы стать «серебряной пулей» в борьбе с мошенничеством посредством социальной инженерии, а также высокотехнологических способов мошенничества.



Марина БРОДСКАЯ
обозреватель BIS Journal

ЭТО CYBER EDTECH, ДЕТКИ!

НОВЫЕ ТЕХНОЛОГИИ НА ЗАЩИТЕ СТАРЫХ ОБРАЗОВАТЕЛЬНЫХ ПОДХОДОВ

EDTECH — НОВЫЕ ТЕХНОЛОГИИ

Ещё десять лет назад многие полагали, что практика внедрения IT-инструментов для создания более увлекательного, инклюзивного и индивидуализированного процесса обучения мало применима в школах. Со временем и особенно с приходом COVID-19 взгляды на EdTech изменились.

Принятие решений EdTech в учебных заведениях стремительно растёт с ростом требований к дистанционному обучению, на которое перешли миллионы школьников и студентов по всему миру. Новые образовательные технологии перестают быть головной болью для преподавателей и становятся неотъемлемой частью работы с онлайн-аудиторией, пишет в своей статье на сайте Forbes.com Майкл Мониз, генеральный директор компании Circadence, лидера в области обучения и обучающих решений по кибербезопасности.

В области ИБ EdTech используются давно и успешно, однако с переходом в виртуальные аудитории они получили новый импульс. В условиях пандемии EdTech способствовали расширению сотрудничества между учителями и студентами за счёт увлекательных, интерактивных и даже реалистичных сред киберпространства.

EdTech предоставили три основных преимущества, считает эксперт.

1. Доступность дистанционного обучения. Традиционные лабораторные занятия перешли в онлайн, преподаватели используют маршрутизаторы и точки доступа Wi-Fi для виртуализации учебных классов и киберполигонов с помощью инструментов EdTech. Новые «лаборатории» на основе браузера помогли вести занятия учителям, а студенты смогли по-прежнему получать практические навыки работы в области кибербезопасности. Более того, инструментарий Cyber EdTech дал возможность создавать преподавателям динамичные и интерактивные учебные среды для студентов. Учителя смогли обеспечить непрерывность обучения, а учащиеся получили практические знания и навыки, необходимые для успешной работы в будущем, и смогли проверить их на практике.

2. Расширенное общение между учителем и учеником. Инструменты EdTech не только обеспечивают обучение, но и столь необходимое сотрудничество в онлайн-формате. Некоторые инструменты Cyber EdTech позволяют организовать многопользовательские мероприятия, объединить студентов в цифровом формате и привлечь их внимание. При этом учитель имеет возможность отслеживать и оценивать уровень знаний и прогресс в обучении каждого студента.

3. Вовлечение студентов. Инструменты EdTech часто помогают заинтересовать студента и поддерживать вни-

мание и интерес к предмету. Некоторые инструменты EdTech в области кибербезопасности позволяют студентам оттачивать навыки и повышать квалификацию за счёт эмуляции реальных условий на рабочем месте. Обучение в такой обстановке помогает студентам понять и почувствовать, чем они будут заниматься в будущем. В результате студенты получают практические навыки, а менеджеры по найму сразу получают кандидатов, готовых к работе.

ИГРОВОЙ ПОДХОД

Какие шаги предлагает сделать Майкл Мониз для успешного внедрения Cyber EdTech в образовательный процесс в области ИБ? По его мнению, надо переходить к обучению на базе игр, даже если речь идёт о высшем образовании. Такой подход к обучению всё шире применяется в деловом мире. Киберучения под руководством опытных тренеров из числа сотрудников, ежедневная командная отработка заданий — всё это наилучшим образом сказывается на процессе обучения. Автор выделяет три ключевых момента.

1. Руководители групп по обучению ИБ должны иметь чёткое представление о бизнес-стратегии и поддерживающих её целях, чтобы адаптировать к ним учебные программы.

2. Руководители IT-подразделений должны интегрировать обучение ки-

бербезопасности в планы работ, чтобы обеспечить постоянное повышение квалификации IT-специалистов и специалистов в области ИБ.

3. После того как преподаватели поставят навыки и умения сотрудников с профессиональными требованиями, Cyber EdTech помогут устранить пробелы в знаниях и отработать навыки как на учебных платформах, так и в ходе интерактивных учебных мероприятий, требующих от слушателей навыков критического мышления для решения серьёзных проблем сетевой безопасности, обнаружения вредоносных программ, криптографии, криминалистики и тестирования на проникновение, а также опыта командной работы.

Таким образом, хотим мы или нет, очно или онлайн, инструменты EdTech незаменимы для преподавателей. Они важны для обучения в XXI веке и обеспечивают высокий уровень подготовки кадров независимо от того, как проходит обучение.

НОВАЯ УЧЕБНАЯ ПРОГРАММА

Новая программа киберкриминалистики стартует в Юго-западном колледже, Калифорния, осенью 2021 года. Предполагается, что она поможет научить студентов методам обнаружения хакеров или вредоносного ПО, присутствующего в системе безопасности, а также превентивным методам, чтобы остановить хакерские вторжения в будущем. Эта программа единственная в своём роде, поскольку требует студенческих стажировок.

«Раньше люди думали, что киберкриминалист будет отслеживать сексуальных маньяков на компьютере, — приводит слова профессора Майкла Спейрера сайт Юго-Западного колледжа. — Сейчас у киберкриминалистики гораздо больше возможностей. Мы учим наших студентов, как предотвратить взлом».

Программа включает 32 модуля, по завершении обучения студенты получают степень младшего специалиста в области естественных наук. Программа рассчитана на 2 года и включает курсы по юриспруденции, цифровым системам и компьютерным информационным системам.

В программу входит стажировка и проверка полученных знаний. Студенты узнают, как использовать Python и другое современное ПО, которое используют многие федеральные агентства. По окончании курса молодые люди будут иметь как минимум один год практического опыта.

НА БЛАГО РОДНОЙ КАЛИФОРНИИ

«Кибербезопасность — быстро развивающаяся дисциплина, которая становится всё более востребованной», — говорится на сайте колледжа. Согласно отчёту Burning Glass Technologies за 2019 год, количество объявлений о вакансиях в сфере кибербезопасности с 2013 года выросло на 94%. На каждую вакансию в сфере кибербезопасности приходится всего 2,3 претендента, что очень мало по сравнению с другими областями занятости.

Согласно ежегодному отчёту, подготовленному кадровой компанией ADP, эксперты в области ИБ могут зарабатывать более \$100 тыс. в год. Burning Glass Technologies сообщает, что 13% всех IT-вакансий находятся в сфере кибербезопасности, а с 2010 г. было размещено 1,5 млн новых вакансий.

В связи с огромным спросом на специалистов по кибербезопасности и информационной безопасности Southwestern College возлагает большие надежды на подготовку будущих специалистов в этой сфере. В ближайшем будущем в колледже планируют сделать эту программу полностью онлайн, чтобы удовлетворить максимум потребностей работодателей и абитуриентов.

Используя рекомендации Калифорнийского проекта развития карьеры и подготовки кадров в области кибербезопасности, преподаватели Юго-Западного колледжа надеются скоординировать и связать все программы обучения, профподготовки и развития персонала для расширения возможностей и партнёрских отношений между разными субъектами системы: образовательными учреждениями, ключевыми компаниями из государственного и частного сектора, неправительственными организациями в рамках штата, заинтересованными в повышении киберустойчивости родной Калифорнии.

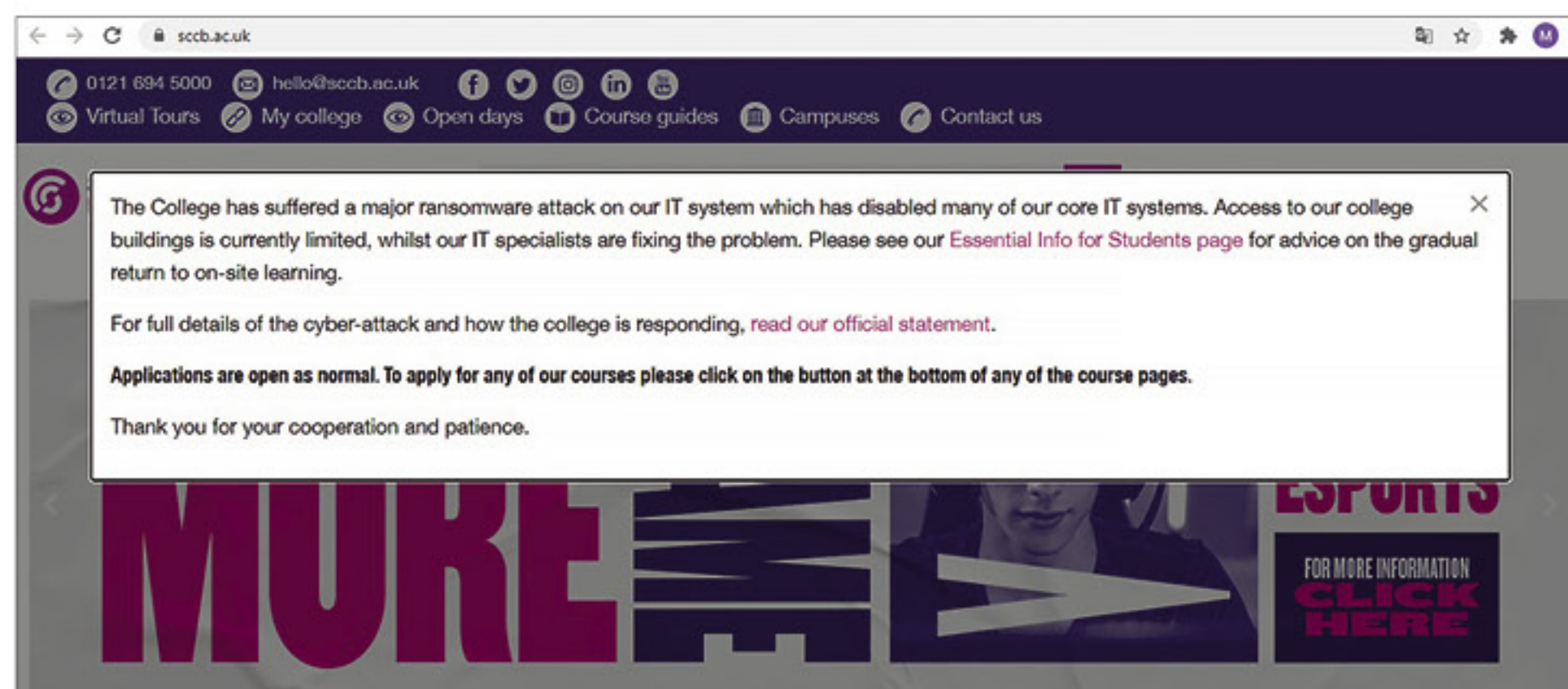
УРОКИ ОДНОЙ АТАКИ

13 марта 2021 года в 3 часа утра местного времени ответственные сотрудники Южного Городского колледжа Бирмингема (South & City College Birmingham, SCCB) получили сообщение о том, что сервер колледжа вышел из строя. Когда утром весть дошла до ректора учебного заведения Майка Хопкинса, он назвал ситуацию катастрофической: «Весь ад вырвался наружу». 13 тысяч студентов были вынуждены продолжить учёбу дома.

Вечером того же дня в социальных сетях на странице учебного заведения появилось объявление:

«Колледж подвергся серьёзной атаке хакеров, которая вывела из строя многие IT-системы. Кампус будет закрыт для студентов в течение недели, чтобы специалисты могли решить проблемы.

Занятия начнутся 15 марта в формате онлайн по всем направлениям. Просьба получить доступ к онлайн-урокам с понедельника, как вы это делали во время



Сообщение о взломе на сайте колледжа SCCB

блокировки. В случае сбоев просим вас быть терпеливыми и связаться с кураторами, если возникнут проблемы. Спасибо за сотрудничество и терпение.

Следите за нашими объявлениями».

Несмотря на все оптимистичные заявления о скором возобновлении работы, спустя неделю, 21 марта, сайт колледжа сообщал о том, что учебное заведение по-прежнему закрыто.

Издание FE Week рассказало подробности. Атака на сервер произошла около 3 часов в ночь с пятницы на субботу. Неизвестный хакер воспользовался найденной уязвимостью и проник в сеть колледжа с правами администратора.

Взлом представлял собой так называемую атаку программы-вымогателя, когда преступники ограничивают доступ к данным до тех пор, пока жертва не заплатит выкуп, поскольку хакер «зашифровал все системы и файлы».

Сотрудники колледжа не могли получить доступ к финансовым и кадровым службам, поэтому пришлось применять альтернативные способы работы с заказами и счетами. Непосредственно финансовая часть колледжа не пострадала. Более того, хакеры не потребовали от руководства учебного заведения традиционного выкупа. Обычно он составляет 2 млн фунтов, которые жертва переводит на счёт в биткоинах.

Первое, что сделали сотрудники колледжа, — защитили компьютеры от дальнейшего заражения по сети, поскольку включение даже одного из них вызвало непредсказуемые последствия.

SCCB — один из крупнейших колледжей в Англии, он появился в результате слияния двух учебных заведений и состоит из восьми кампусов и центров по всему Бирмингему. В колледж принимают студентов от 14 лет и старше, всего в нём учатся 13 тыс. учеников. Учитывая ситуацию, руководство учебного заведения было вынуждено закрыть колледж. Дистанционное обучение стало возможным, поскольку колледж восстановил доступ к программам Microsoft, таким как Office и Teams, а позже и к электронной почте.

Для анализа ситуации и оценки последствий кибератаки на системы колледжа были проинформированы специалисты Национального центра

кибербезопасности, Управления комиссара по информации и финансовым органам и эксперты по образовательным технологиям Jisc.

Пока нет точной информации о последствиях кибератаки: украденных персональных данных или иной информации, неизвестны и точка проникновения, и возможные последствия.

В конце недели в кампус вернулись студенты, участвующие в практических программах, иностранные студенты и социально незащищённые ученики. Колледж продолжает давать студентам в аренду ноутбуки и интернет-ключи, каждую неделю увеличивая количество студентов. Соседний Бирмингемский столичный колледж предоставил коллегам помещения для сдачи плановых экзаменов. Однако, когда колледж SCCB сможет вернуться к полноценной работе, его ректор сказать не может.

Необходимо установить, что произошло, и проверить каждый из десятков тысяч компьютеров на предмет заражения. Ожидается, что этот первый этап продлится до Пасхи.

Ещё одна проблема — Covid-19. Работу местного центра тестирования на коронавирус пришлось приостановить, студентам были отправлены наборы для тестирования дома. Однако Covid отчасти и спас колледж, поскольку люди привыкли работать и учиться дома, а сотрудники IT-департамента смогли восстановить доступ к учебным материалам, ранее выделенным в отдельный массив для удалённой работы.

Команда SCCB смогла быстро отреагировать на кибератаку и минимизировать её последствия. Но другие колледжи в прошлом были застигнуты врасплох. Согласно данным Департамента цифровых технологий, культуры, СМИ и спорта, в 2019 году 80 % учреждений дополнительного и высшего образования подверглись кибератакам или у них были выявлены нарушения кибербезопасности. В некоторых случаях сотрудники даже не знают, где расположен сервер организации, и не понимают, что происходит в компьютерных системах колледжа. Кто-то готов сэкономить на сайте, где-то самостоятельно пишут программное обеспечение для внутренних систем, без учёта опыта и

особенностей организации. О том, что системы, созданные профессиональными разработчиками, будут регулярно тестироваться, руководство колледжей не задумывается.

Устаревшее программное обеспечение также может стать проблемой после взлома системы. Ещё один колледж использовал для веб-сайта мало распространённую систему управления контентом, для которой он смог найти только семь разработчиков. Это означает, что в случае взлома сайт обойдётся колледжу в круглую сумму. Кроме того, такую систему будет легче взломать, поскольку она реже тестируется и обслуживается, реже осуществляется резервное копирование.

* * *

Чтобы помочь колледжам не стать жертвами хакеров, FE Week попросила экспертов Infuse Technology дать основные советы по предотвращению кибератак. Вот они.

1. Давать новым сотрудникам только необходимые права и разрешения, повышать их осведомлённость в ИБ.

2. При увольнении своевременно удалять все права доступа, включая доступ к облаку.

3. Обновлять программное обеспечение на серверах и компьютерах, закрывая уязвимости или ошибки, обнаруженные после выпуска приложения или программного обеспечения.

4. Ввести двухфакторную авторизацию.

5. Реализовать эффективную стратегию аварийного восстановления.

6. Использовать управление устройствами для защиты конфиденциальных данных, ограничить доступ к устройствам, на которых хранятся конфиденциальные данные.

7. Проверять хранилище данных вне зависимости от того, как они хранятся — на месте или в цифровом месте в облаке.

8. Удалить общие аккаунты.

9. Минимизировать права доступа к данным.

10. Защитить электронную почту, поскольку 95 % угроз проникают в системы через неё.

АБИТУРИЕНТ-2021

НОВЫЕ ПРАВИЛА ПРИЁМА В ВУЗЫ

Пандемия COVID-19 внесла много изменений в нашу жизнь. Переход на удалённую работу заставил работодателей пересмотреть отношение к обеспечению кибербезопасности. И тут же возник вопрос нехватки квалифицированных кадров.

Более 3,5 млн человек требуются в мире на должности в сфере ИБ в 2021 году. Более половины (51%) руководителей со всего мира и 42% руководителей из России, опрошенных в рамках глобального исследования «Доверие к цифровым технологиям — 2021», проведённого компанией PwC, заявляют, что в течение этого года они планируют увеличить численность штатных специалистов по ИБ. 22% респондентов в мире и 18% российских респондентов говорят о повышении числа таких сотрудников на 5% и более. Откуда их взять, если не со студенческой скамьи?

ВСЁ НЕМНОГО НЕ ТАК

Министерство науки и высшего образования утвердило новый порядок приёма на обучение по программам бакалавриата, специалитета и магистратуры. Изменения вступают в силу в 2021/2022 учебном году. Соответственно, университеты внесли изменения в свои правила приёма абитуриентов. Изменения заметные.

Как и прежде, абитуриент может подать документы в пять университетов. Но если раньше он мог выбрать максимум три направления подготовки в каждом из вузов, то с 2021 года можно выбрать до 10 направлений в каждом из пяти учебных заведений.

Университеты могут проводить единый конкурс по нескольким родственным специальностям, а не по отдельно взятым направлениям. Таким образом, вузы смогут выбирать сильных абитуриентов на глобальное направление обучения в целом и уже потом проводить деление по специальностям.

Вузы смогут самостоятельно устанавливать вступительные испытания

по нескольким предметам на выбор, а абитуриент сможет сам выбирать, результат ЕГЭ по какому предмету лучше предоставить. Например, теперь в большинстве университетов можно выбрать, какой из профильных предметов — физику или информатику — учитывать при поступлении на специальности «Информационная безопасность». В ряде вузов наряду с этими предметами учитывают и баллы по иностранному языку.

Теперь университеты вправе самостоятельно устанавливать разные требования к минимальным баллам для тех, кто поступает на бюджет, и тех, кто идёт учиться за деньги. И если план приёма на бюджет строго регламентирован приказами и согласованиями, то число студентов на платных отделениях ничем не ограничено.

Новыми правилами уточнены требования к баллам за индивидуальные достижения. Внесены изменения и в порядок учёта достижений абитуриентов на олимпиадах. Победителям и призёрам олимпиад, возможно, придётся подтвердить право на особые условия приёма: они должны получить не менее 75 баллов на профильном ЕГЭ или при необходимости пройти дополнительное вступительное испытание, если потребует вуз.

Уточнены требования и по числу мест в пределах квот приёма на обучение по программам бакалавриата и специалитета за счёт бюджета. Для ребят, имеющих особое право на приём в пределах квоты, выделяются не менее 10% от объёма контрольных цифр по каждой специальности или направлению подготовки. Число мест по целевому обучению определяется вузом самостоятельно или устанавливается учредителем. Если целевая квота не была установлена ранее, предполагается выделение максимального количества мест. В случае если количество мест, оставшееся после выделения целевой квоты, недостаточно для выделения особой квоты, проводится отдельный

конкурс для претендентов на указанные места.

Учебные заведения принимают самостоятельное решение, какие внутренние вступительные экзамены нужны для поступления в вузы выпускников колледжей и техникумов. И эти предметы не обязательно должны совпадать со списком предметов по ЕГЭ.

В 2020 году многие университеты принимали документы в электронном виде из-за ограничений, связанных с карантином. Согласно новым правилам, с 2021 года все учебные заведения обязаны принимать документы в электронном виде, чтобы расширить возможности для поступления абитуриентов из отдалённых регионов. Для тех, кто не верит в «цифру», сохраняется возможность подачи документов лично или по почте.

Проще станет и внесение изменений в заявление о приёме — для этого не надо отзываться ранее поданное заявление и подавать документы вновь.

Особо нервным абитуриентам и их родителям легче будет следить и за конкурсной ситуацией. Обновление информации со списками поступающих должно происходить не реже пяти раз в день. Ранее эти сведения обновлялись раз в сутки.

Внесены изменения и в порядок зачисления. С 2021 года не будет двух волн приёма в университеты на общих основаниях.

Зачислять на первый курс по программам бакалавриата и специалитета будут в два этапа. Сначала тех, кто поступает вне конкурса (по квотам на бюджетных местах) и по целевому приёму. Их зачислят в вуз 30 июля. Второй этап — основной — пройдёт 5 августа. Он больше не будет делиться на первую и вторую волну. И попытки переложить оригиналы документов в другой вуз у провалившихся уже не будет. Зачисление на платной основе большинство университетов производит с конца июля по 31 августа при условии, что абитуриент набрал на ЕГЭ

минимальное количество баллов согласно правилам приёма в вуз.

Утешение для тех, кто не поступил на очную форму и не начал учёбу с 1 сентября: университеты получают право проводить набор, в том числе и дополнительный, на очную и очно-заочную формы обучения до 31 декабря.

Ещё одно нововведение — обезличенные списки поступающих. Вместо имени и фамилии университеты могут указывать либо индивидуальный номер абитуриента, присвоенный вузом, либо его СНИЛС. Также из конкурсных списков могут исчезнуть имена тех, кто сразу сдал оригиналы документов.

Есть и ещё кое-что — по новым правилам вузы не обязаны публиковать приказы о зачислении в свободном доступе. Решение об этом принимает ректор.

В ОЖИДАНИИ НАЧАЛА КАМПАНИИ

В соответствии с требованиями федерального законодательства университеты ещё осенью опубликовали новые правила приёма. В большинстве случаев эти правила дублируют порядок приёма на обучение по программам бакалавриата, специалитета и магистратуры, утверждённый министерством, с учётом специфики университета. Однако есть и различия. Одни вузы вводят повышенные требования к минимальным баллам по ЕГЭ, с которыми можно подавать документы. Другие расширяют список предметов, которые учитываются при зачислении.

Так, большинство университетов, где есть специальности по направлениям «Информационная безопасность» (10.00.00), требуют от абитуриентов

итогах профильного экзамена по математике: чаще всего это не менее 39 баллов. Однако для подачи документов, например, в НИЯУ «МИФИ» надо иметь не менее 68, а по ряду специальностей — 76 баллов. Повышенные требования к математике в НИУ «МФТИ», ВШЭ, МВТУ им. Баумана и СПбПУ. Они же требуют высоких знаний по информатике или физике, а также по русскому языку. Большинство же университетов готовы принимать абитуриентов с 39 баллами по физике, 44 — по информатике и 40 — по русскому. В Волгоградском государственном университете (ВолГУ) на специальности по ИБ примут итоги ЕГЭ по химии (не менее 39) и иностранному языку (30). С такими же баллами по языку примут и в Казанском (Приволжском) федеральном университете (КФУ).

Согласно новым правилам, университет вправе принять на платное отделение всех желающих, однако многие учебные заведения устанавливают конкретные значения в контрольных цифрах приёма, ориентируясь на опыт прошлых лет. Чаще всего планируется принять на платное отделение 1–2 группы студентов (или дополнить до 2 полноценных групп с учётом бюджетников), однако в ряде университетов смотрят далеко в будущее. Например, в МИРЭА, где представлены практически все специальности по «Информационной безопасности», на платной основе запланировано от 111 до 282 мест. Для сравнения, в прошлом году на специальность «Обеспечение информационной безопасности автоматизированных систем» (10.02.05) поступили 55 человек, а на следующий год планируется принять 111.

Аналогичное двукратное превышение запланировано и на направление «Информационная безопасность автоматизированных систем» (10.02.03). Близки к реальности цифры приёма на платное отделение бакалавриата на специальность «Информационная безопасность» (10.03.01). Здесь планируется принять 282 первокурсника против 256 в прошлом году. Сколько из них завершит образование через 4 года?

Большинство вузов ведут приём и иностранных граждан — в общем порядке или выделяя для них специальные места (например, ВШЭ). Однако ряд университетов ограничивает приём иностранных граждан и лиц без гражданства на обучение по образовательным программам, содержащим сведения, составляющие государственную тайну. Приём осуществляется только в пределах квоты на образование иностранных граждан с соблюдением требований, предусмотренных законодательством РФ о государственной тайне. Часто эта фраза не расшифровывается, однако в ряде случаев перечень направлений прописывается в правилах приёма или при выборе специальностей на сайте. Так, в МАИ отсекается ряд специальностей из направлений «Информационные технологии» и «Информационная безопасность».

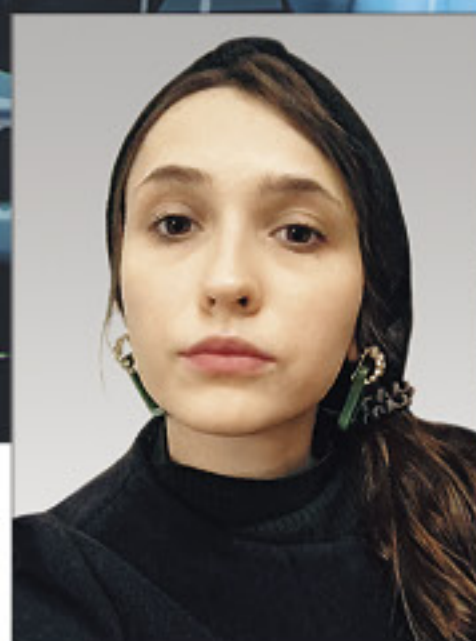
Традиционный вопрос наших обзоров, сколько из поступивших на первый курс студентов доучатся до конца и пойдут на работу по специальности, как всегда, остаётся без ответа.

BIS-СПРАВКА

По данным информационного сервиса для поступающих <https://vuzoteka.ru/>, по направлению ИБ существует 262 программы обучения. Только по направлению обучения укрупнённого направления «Информационная безопасность» (10.03.00) высшего образования уровня «бакалавриат» существует 14 профилей обучения, по которым работают 103 вуза. 54 университета принимают студентов на специальность 10.05.03 «Информационная безопасность автоматизированных систем», в 32 учат по направлению 10.05.01 «Компьютерная безопасность», а в 29 — по программе 10.05.02 «Информационная безопасность телекоммуникационных систем». 16 университетов готовят специалистов по 10.05.05 «Безопасность информационных технологий в правоохранительной сфере». И всего 13 — 10.05.04 — «Информационно-аналитические системы безопасности».



Анастасия МОСКОВКИНА
студентка кафедры
коммуникационных технологий МГЛУ



Дарья ЧУБ
студентка кафедры
коммуникационных технологий МГЛУ

ЮЗЕРЫ ПРОТИВ ХАКЕРОВ

ЦИФРОВАЯ ГРАМОТНОСТЬ СТАНОВИТСЯ ЧАСТЬЮ
ОБРАЗОВАТЕЛЬНОГО МАСТ-ХЭВА

В условиях массового обучения в онлайн-формате школьники и студенты были вынуждены осваивать новые средства коммуникации. Мирные сетяне столкнулись с проблемами, оказавшимися глубже педагогического бэкграунда большинства учебных заведений.

Дистанционный формат обучения в московских школах, колледжах и вузах закончился. И хотя пакет мер, направленный на безопасность учащихся, был исполнен, нарушения безопасности в Сети оказались неприятной неожиданностью для многих российских школ. По заданию BIS Journal мы провели социологический опрос

на тему кибербезопасности и сетевых угроз в условиях пандемии и массового онлайн-обучения. В опросе приняли участие школьники и студенты московских и региональных учебных заведений. Цель исследования — выявить наиболее частые угрозы и уязвимости юзеров в Сети за время тотального онлайн-обучения.

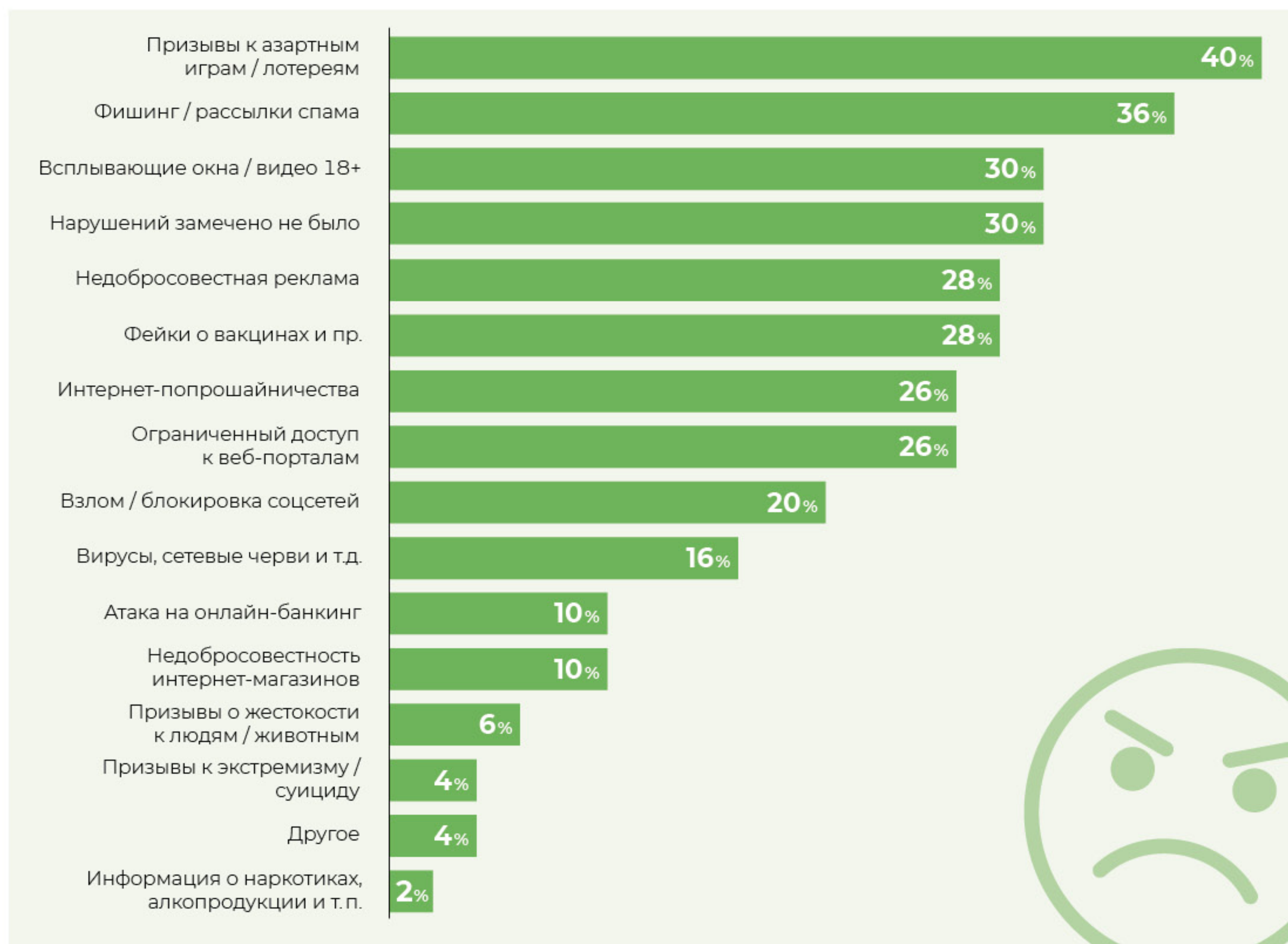


Рисунок 1. Проблемы, с которыми сталкивались респонденты в период пандемии

ЧТО УГРОЖАЛО И РАЗДРАЖАЛО

Топ-3 проблем, с которыми сталкивались респонденты в период пандемии, выглядит так: призывы к азартным играм и лотереям (40%), фишинг и рассылки спама (36%), всплывающие окна или видео, содержащие информацию 18+ (30%).

Второй сектор угроз в сети заняли: недобросовестная реклама и фейки о вакцинах, режиме самоизоляции, масочном режиме (28%).

На третьем месте интернет-попрошайничество и ограниченный доступ к веб-порталам, блокировка сайтов (26%), взлом или блокировка социальных сетей и личных аккаунтов (20%).

В числе наименее выявленных уязвимостей в Сети: вирусы, сетевые черви (16%), атаки на онлайн-банкинг (10%), недобросовестность интернет-магазинов (10%), контент, содержащий

насилие и жестокость по отношению к людям или животным (6%), призывы к самоубийству, беспорядкам, экстремизму, разжиганию расовой ненависти (4%), информация о производстве и распространении наркотиков, алкогольной продукции, психотропных веществ (2%). В свою очередь, 30% опрошенных вообще не заметили нарушений в Сети (рис. 1).

Несмотря на то что большая часть респондентов не заметила нарушений в процессе дистанционного обучения (54%), практически половина всё же смогла припомнить случаи подрыва безопасности в Сети.

Верхнюю строчку топ-угроз во время занятий заняли: наличие посторонних пользователей в эфире (28%), отсутствие доступа к конференции по веб-ссылке (23%), недобросовестная реклама (21%). Второй сектор нарушений: ненормативная лексика в эфире

(18%), всплывающие окна/видео, информация для взрослых и предложения о регистрации на сторонних сайтах (13%). В числе наименее выявленных нарушений: вирусы, сетевые черви и троянские программы (8%), блокировка соцсетей (5%) (рис. 2).

ЗУМБОМБИНГ. СПРАВИТСЯ ДАЖЕ ШКОЛЬНИК

Популярная проблема, с которой столкнулись участники онлайн-конференций, — посторонние пользователи (28%) и ненормативная лексика в эфире (18%), — зачастую была связана с так называемый зумбомбингом (Zoombombing).

Зумбомбинг — явление, охватившее Интернет и мейнстримом ворвавшееся в онлайн-пространство российских конференций Zoom, Google Meet, реже Discord. Буквально зумбомбинг означает захват видеоконференции, то есть



Рисунок 2. Топ-угрозы во время онлайн-занятий

захват экрана, создание помех с помощью аудиоподкастов через программу для записи и редактирования звуков Soundpad, зачастую содержащих ненормативную лексику и видеопroduкцию 18+.

«На уроке русского языка на экран включилось видео для взрослых. На алгебре неизвестный пользователь говорил всякие гадости про учителя. После обращения в поддержку никаких изменений не было. Проблема не была устранена». Аня, ученица школы № 1253

По несложной механике пранкеры искали в открытом доступе ссылки на конференции, забирались в общий видеоконференц-зал и наводили «шороху». Чуть позже к «вольным» хулиганам стали присоединяться и сами учащиеся. Платформами для тусовок зумбомберов служили VK и Telegram. В период «жаркого сезона» учебного процесса километровые чаты в Telegram, куда

присылались ссылки, собрали многотысячную аудиторию. Культура пранкеров в таких чатах гласит: не переписываться на посторонние темы, не ругаться и не присылать информацию 18+, да и в целом писать сообщения строго и по делу. Сами пранкеры видят цель своих действий в шутке ради шутки. Некоторые администраторы таких групп открыто указывают на проблему образовательного онлайн-процесса:

«Браток, если я кидаю в группу ссылки, которые учителя на стену кидают, проблема как раз таки не во мне, а в учителях, которые это кидают».

Пострадавшая же сторона перебивалась временными методами защиты от нападений: перезапуск конференций, перенос урока на другие даты, отмена занятий с домашним заданием по WhatsApp. Не все преподаватели понимали ситуацию правильно, ведь бомберы часто использовали фамилии

учащихся, которые отсутствовали. Так, Даниил, 15-летний ученик средней школы, поделился:

«На уроке физкультуры онлайн пришли тролли под именем одноклассников. Включали посторонние звуки с матом. Сорвали урок. Было смешно, но потом класс вызвали к директору».

Бомберы подрывали покой пользователей разных платформ. Некоторые нападали на онлайн-курсы. Александр, проходивший в период пандемии курс обучения на платформе Sterik, попал на фишинговый сайт через рекламу в социальных сетях, после чего ему на почту стали приходить нигерийские письма, а в группах постоянно шла реклама заработка в сети. В поддержке ему посоветовали удалять или блокировать такой контент.

С наплывом ботов на свой открытый вебинар в Zoom столкнулась коуч по личностному росту Ирина:

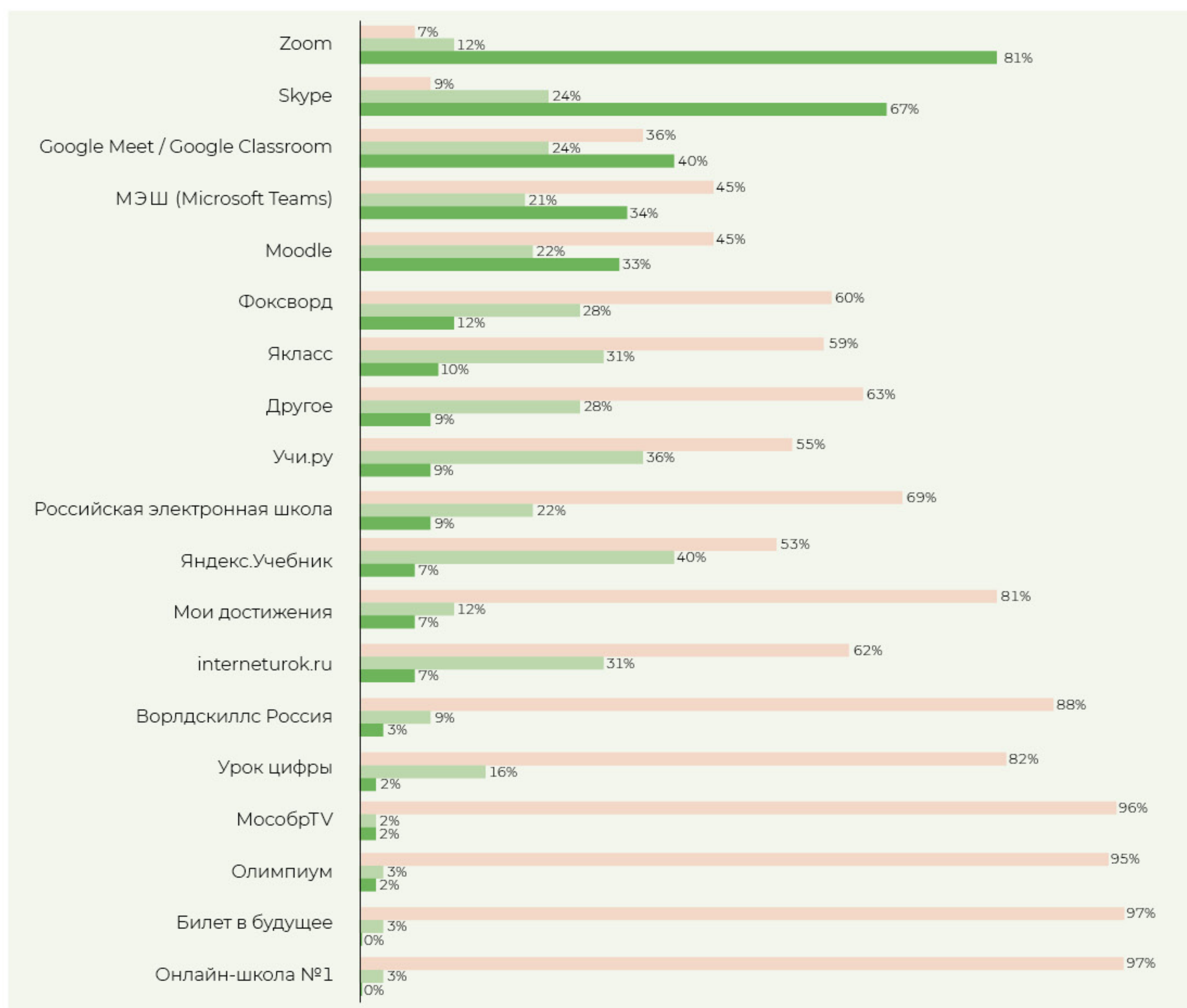


Рисунок 3. Популярность онлайн-платформ (■ никогда не слышал(а); ■ не пользовался, но слышал(а); ■ пользовался)

«Это был бесплатный вебинар, аудитория 150 человек. Открытое мероприятие. Но пришли боты, стали рисовать на экране мужские достоинства, а затем взламывать участников и от их имени писать непристойности. Удаляли, но не помогало».

Таким образом, платформы, которые оказались востребованы в период дистанционного обучения среди российских педагогов, были недостаточно защищены от несложных манипуляций — пранков, с которыми может справиться даже школьник.

МЕСТО ВСТРЕЧИ

Наше исследование показало, что среди платформ, используемых для

онлайн-обучения, наиболее популярными являются три: Zoom (81%), Skype (67%), Google Meet (40%). Среди прочих пользователи отметили: Cisco Webex Meetings, Discord, образовательную онлайн-платформу IBLs, открытое образование OpenEdu, платформы Stepik и Skyeng.

Наименее востребованными оказались платформы МЭШ (34%), Moodle (33%), «Фоксфорд» (12%), «Якласс» (10%), РЭШ (9%), «Учи.ру» (9%), «Яндекс.Учебник» (7%). Большая часть респондентов не сталкивалась или никогда не слышала о платформах InternetUrok.ru, «Мои достижения», союз «Молодые профессионалы», «Ворлдскиллс Россия», «Олимпиад»,

телеканал Мособртв, «Урок цифры», онлайн-школа № 1 и портал «Билет в будущее» (рис. 3).

АТАКУЮТ МОШЕННИКИ

Всевозможные фейки о самоизоляции, истории об обязательной дезинфекции, взломы личных страниц аккаунтов — всё это усилилось во время пандемии, доведя Сеть до болезненной лихорадки. Онлайн-мошенники также не отставали от общих трендов и на волне перемен продемонстрировали новые способы «разводок» мирных сетян.

В мае 2020 г. у известного ютубера HappyZerG (Святослава Власюка) мошенники угнали аккаунт. Как объясняет сам Святослав, ему на почту пришло

письмо от якобы рекламодателя, в котором ютуберу предложили протестировать приложение по изменению голоса. Ссылка в сообщении не вызвала подозрений, тем не менее, с установкой начались сложности. Святослав пробовал загрузить приложение на разные устройства, но не удавалось. Вскоре появились проблемы посерьёзнее. С утра стали приходить сообщения от системы по замене пароля для аккаунта и двухфакторная аутентификация ютуба. Система восстановления и резервная почта не спасли положение. В итоге стиллер (вредоносное ПО, предназначенное для кражи сохранённых в системе паролей), который атаковал гугл-почту ютубера, получил доступ к ютубу, и канал с подписчиками на глазах хозяина продали. Святослав месяц пытался восстановить доступ к каналу. Ему помогла служба поддержки YouTube в Twitter, а также преданные подписчики, которые кидали репорты на украденный канал. Инцидент сильно ударил по аудитории стримера: «Многие отписывались от канала, так как не понимали, какой аккаунт угнан и на что они вообще подписаны и почему».

«Рекомендую в первую очередь помнить, что в мире есть мошенники, которые хотят вас обмануть и что-то украсть. Мыслить «ой, да кому я нужен» или «да у меня не особо популярный канал/аккаунт» нельзя, так как мошенники придумают, что сделать с вашим аккаунтом и как на этом заработать».

Ксения Астахова — преподаватель IT-курсов в Международной компьютерной академии по разработке игр, программированию и дизайну — тоже стала жертвой аккаунт-воров. Ксения часто сталкивалась с попытками взлома, для неё и её друзей они уже стали чем-то вроде местной шутки, но этот случай выбил из колеи.

«Тревожный сигнал поступил от друзей по телефону: «Ксюша, что у тебя случилось? С твоего аккаунта просят деньги на похороны твоей мамы». Как выяснилось, взломали страницу в VK, написали фейковый пост и прикрепили отфотошопленную карту от моего имени с просьбой перевести деньги».

Как объяснила Ксения, карточка — это фейк, «электронный счёт, который

невозможно отследить, тем более вернуть с него деньги». Мошенник не просто разместил пост в VK, он писал в личку друзьям, отвечал на их соболезнования и не стеснялся просить ещё денег. Хотя аккаунт удалось оперативно заблокировать с помощью функции «пожаловаться» и через час Ксения получила к нему доступ, некоторые её друзья уже успели перевести деньги мошеннику.

Приведённые случаи не являются по сути новыми, подобное случалось и раньше. Однако именно пандемия послужила спусковым механизмом для усиленной эксплуатации уже имеющихся прорех в киберпространстве.

ШАГ К БЕЗОПАСНОМУ ИНТЕРНЕТУ

Эксперты кибербезопасности сходятся во мнении, что Интернет — сеть небезопасная. Необходимо соблюдать определённые превентивные инструкции. Пренебрежение этими правилами может поставить вас и ваши данные под угрозу. Но, к сожалению, хотя общие правила безопасности и легко найти в открытом доступе, они не всегда удобны и понятны для пользователей.

СОЦИАЛЬНЫЕ СЕТИ

Наши социальные сети хранят достаточно много личной информации. Важно всегда устанавливать вручную настройки конфиденциальности в профиле аккаунта, регулировать приватность своей страницы, доступ других пользователей к фотографиям, сообщениям и друзьям. Время от времени также важно проверять обновления соцсетей и в случае необходимости менять их и настраивать их под себя.

ЗАЩИТА ДАННЫХ В БРАУЗЕРЕ

Системы браузеров часто предлагают сохранять логин и пароли от сайтов, которыми вы пользуетесь. Эта удобная функция, как ни удивительно, таит в себе большую опасность. Браузер по умолчанию обрабатывает и хранит информацию о ваших интересах, интернет-перемещениях и запросах. Маркетинговые специалисты с помощью этой информации моделируют для себя ваш покупательский профиль и адресную рекламу. Несмотря

на многие плюсы режима инкогнито, он не защитит от информационного сбора, поэтому используйте специализированные инструменты. Советуем не хранить личные данные в файлообменниках и сервисах для совместной работы, а также использовать антивирусные программы для защиты вашего сёрфинга в Интернете, такие как Kaspersky, Dr.Web и др.

Желательно не использовать личную почту и номер телефона для регистрации на сайтах онлайн-магазинов и прочих интернет-сервисов, так как среди тонны спама и рассылок могут приходить фишинговые письма. Лучше всего иметь дополнительную почту или отдельную сим-карту для таких целей.

КАК ЗАЩИТИТЬСЯ ОТ ЗУМБОМБЕРОВ

Важным правилом открытого видеоконференции является генерация случайного идентификатора конференций, наличие пароля, зал ожидания и ограничение доступа к экрану. Также рекомендуется не объявлять детали конференции по общедоступным каналам связи. Организаторам лучше ознакомиться с функциями платформы заранее или воспользоваться помощью модератора-напарника.

* * *

Атаки мошенников всегда представляли угрозу для пользователей, на фоне пандемии их число резко выросло. Однако отмена карантинных мер не снизила этот рост, поэтому СМИ неустанно продолжают публиковать сводки о новых видах мошенничества.

Период карантина и дистанционного обучения показал бреши в системе безопасности многих платформ и личной безопасности юзеров. Около 45 % заметили нарушения безопасности. Невозможно предугадать, когда и как мы столкнёмся с угрозой, однако всегда можно принять меры по её недопущению. Именно поэтому цифровая грамотность — один из ведущих тезисов сегодняшнего дня. Это безопасность не только единицы, но и всей системы, не только отдельного человека, но и государства.



Борис СТОЛПАКОВ
историк криптографии,
кандидат физико-
математических наук

ГИГАНТ МАТЕМАТИЧЕСКОЙ МЫСЛИ И ДЕЛА

ПАФНУТИЙ ЧЕБЫШЁВ: НЕУСТАННОЕ СЛУЖЕНИЕ
НА БЛАГО ОТЕЧЕСТВА

16 мая 2021 года исполняется 200 лет со дня рождения великого русского математика, механика и выдающегося деятеля российского образования Пафнутия Львовича Чебышёва (1821–1894). Юбилей П. Л. Чебышёва даёт нам повод и возможность вновь обратиться к отмечаемой 5 мая 100-летней памятной дате российской криптографии. Ведь именно трудами Чебышёва и его учеников был создан мощный теоретический фундамент, ставший прочной основой успехов советских криптографов.

НА ПУТИ К СЛУЖЕНИЮ

Пафнутий Львович получил своё редко звучащее ныне имя согласно православной традиции. Совсем рядом, 14 мая, памятный день преподобного Пафнутия Боровского, почитавшегося родителями новорождённого, да и родовое имя Чебышёвых, Окатово, располагалось неподалёку от знаменитого в Подмоскowie Пафнутьева Боровского монастыря. Спустя более полувека Пафнутий Львович вместе с братьями на месте старого родительского дома поставил оригинальный памятник — гранитную глыбу с надписью: «Здесь у Льва Павловича и Аграфены Ивановны Чебышёвых родилось пятеро сыновей и четыре дочери».

Пафнутий был старшим из братьев. Три его младших брата по семейной

традиции выбрали военное поприще. Со временем самые младшие, Николай и Владимир, стали известными генералами в артиллерии. А Пафнутий с детства прихрамывал, и путь к военной карьере для него был закрыт. В 1832 году Лев Павлович привёз старших сыновей Пафнутия и Павла из имения в свой московский дом, решив дать им домашнее образование и готовить к поступлению в Московский университет. В 1837 году оба стали студентами. Как известно, Пафнутий поступил на 2-е (математическое) отделение философского факультета. В 1841 году он окончил университет «отличнейшим из студентов», заслужив медаль за своё сочинение «О числовом решении алгебраических уравнений высших степеней». К этому времени Чебышёв уже почувствовал интерес и своё призвание к решению математических задач, связанных с практическими общественными потребностями.

НАСТАВНИКИ ВЕЛИКОГО УЧЕНИКА

Привлекли его внимание к подобным занятиям университетские наставники, прежде всего Н. Д. Брашман и А. С. Ершов. Они познакомили Чебышёва с практической механикой, новым прикладным научным направлением, и так увлекли, что Пафнутий Львович не расставался с теорией механизмов и конструированием до конца

своих дней. Тогда Ершов вернулся из командировки во Францию, где общался с одним из создателей практической механики и проективной геометрии, президентом Парижской АН Ж.-В. Понселе. Понселе интересовался Россией и энергично популяризировал русские счёты, заинтересовавшие его лёгкостью освоения и высокой эффективностью вычислений. Неведомые Европе счёты он открыл для себя, оказавшись в русском плену в 1812 году.

Спустя годы А. С. Ершов стал инициатором создания Московского высшего технического училища — одного из признанных лидеров отечественного инженерного образования, недавно отметившего своё 150-летие. Н. Д. Брашман известен как основатель Московского математического общества (1864) и старейшего российского математического журнала «Математический сборник» (1866). Во всех этих начинаниях бывшие наставники П. Л. Чебышёва пользовались его активной и авторитетной поддержкой. А в начале 40-х годов благодаря содействию Брашмана Чебышёв получил от попечителя Московского учебного округа С. Г. Строганова интересное поручение — написать доступный, но содержательный учебник по теории вероятностей для Демидовского лицея в Ярославле. Популяризация вероятностных методов в ту пору была связана с распространением в



П. Л. Чебышёв. 1860-е годы

России страхового дела, где эти методы эффективно применялись. Именно тогда Чебышёв почувствовал вкус к решению вероятностных задач и в 1845 году продемонстрировал своё мастерство в магистерской диссертации «Опыт элементарного анализа теории вероятностей».

«НАМ НЕ ДАНО ПРЕДУГАДАТЬ...»

Диссертация привлекла внимание петербургских академиков. Один из них, В. Я. Буняковский, сам являвшийся энергичным пропагандистом страхового дела и теории вероятностей, сразу высоко оценил потенциал молодого

математика и поспособствовал с приглашением на должность адъюнкта в Петербургский университет в 1847 году. Ещё раньше Буняковский пригласил Чебышёва вместе заниматься изучением рукописей Л. Эйлера, лишь недавно обнаруженных в архиве Академии наук. Погружение в заметки великого учёного, относящиеся к теории чисел, а также необходимость чтения лекций в университете по этой части алгебры глубоко заинтересовали Чебышёва и стимулировали его самостоятельные теоретико-числовые изыскания. Уже в конце 1848 года он представил к защите докторскую диссертацию «Теория сравнений». Её опубликование стало

событием для математической науки не только в России. «Теория сравнений» Чебышёва представляла собой первую фундаментальную публикацию по предмету на русском языке, позднее она не раз переиздавалась и переводилась. Книга содержала полное для того времени и стройное изложение теории чисел, не утратившее своё значение и в XX веке. Особенно много значат слова «теория сравнений» для криптографов, ведь эта теория лежит в основе алгебраических методов криптографии. Так, ещё в середине XIX столетия Пафнутий Львович стимулировал развитие математического направления, ставшего особенно актуальным в период «математизации» криптографии в 1940-е годы.

КАК ТЕОРИЯ ВЕРОЯТНОСТЕЙ СТАЛА «РУССКОЙ НАУКОЙ»

В возрасте 32 лет Чебышёв был избран в Петербургскую академию наук. 50-е и 60-е годы XIX века стали для него наиболее плодотворными. Его имя прочно связалось с самыми важными понятиями и достижениями теории вероятностей. Свой университетский курс по этой науке он впервые превратил в строгую математическую дисциплину. В последующие годы выдающимися трудами П. Л. Чебышёва и его учеников, особенно А. А. Маркова и А. М. Ляпунова, в мире сложилось отношение к теории вероятностей как к «русской науке». Мощный стимул получили исследования и по математической статистике. Ныне известно, что уже в конце XIX столетия российские криптографы эффективно использовали эти достижения в своей работе.

Особенно были востребованы вероятностные методы, да и математика в целом, в артиллерии. В конце Крымской войны Чебышёва на многие годы назначили от Академии наук в члены Военно-учёного и Артиллерийского комитетов. Это было время проблемного перехода от гладкоствольной артиллерии к нарезной. Многие из разработок Чебышёва, в том числе по теории вероятностей, вызывались именно насущными нуждами военных. Любопытен отзыв артиллеристов об участии Пафнутия Львовича в совместной работе:



Здание Петербургского университета

«Артиллерийское искусство во многих отраслях своих исследований, например, касающихся стрельбы (т.е. движения снаряда в воздухе, движения снарядов в канале орудия, оценки действительности стрельбы, основанной на теории вероятностей, действия орудия на лафет и т.п.), представляет трудности столь значительные, что для преодоления их становятся недостаточными усилия офицеров, хорошо знающих математические науки в обыкновенном их объёме, но нужно содействие великих геометров... Г. Чебышёв, признаваемый во всей Европе первостепенным геометром и составляющий славу и гордость России, продолжает собою ряд великих учёных, занимавшихся артиллерией, — факт тем более важный, что в настоящее время необходимо весьма многие части теории выработать вновь, а без теоретических оснований одна практика, требуя нескончаемых опытов и, следовательно, поглощая непомерные расходы и время, всё-таки не может представлять надлежащего исхода, не может дать никаких общих заключений.

Г. Чебышёв, во-первых, принял на себя руководство всех тех артиллерийских офицеров, как в Комитете, так и вне Комитета находящихся, которые занимаются математическими артиллерийскими работами; всякое



Профессора физико-математического факультета Санкт-Петербургского университета (фото 1868 года). Второй слева в первом ряду — П.Л.Чебышёв

затруднение преодолевается. Например, здесь можно указать на содействие его по предмету приложений теории вероятностей к артиллерийской стрельбе, приложений, которые дали в последнее время полезнейшие результаты, а также на пояснение вопросов, относящихся к теории вращательного движения, теории совершенно новой в артиллерии, столь трудной и столь для артиллерии необходимой теперь.

Во-вторых, г. Чебышёв предпринимает некоторые математические изыскания специально для Артиллерийского комитета. Так, например, он определил рациональными изысканиями, какую

наивыгоднейшую форму должен иметь удлинённый снаряд для того, чтобы, двигаясь без вращательного движения, он имел наибольшую устойчивость в воздухе. Данная им теория и произведённые на основании её опыты разъяснили весьма много вопросов о стрельбе продолговатыми снарядами из орудий с гладким каналом и дали основания для обсуждения многочисленных систем этих снарядов, предлагавшихся различными изобретателями.

Для облегчения составления таблиц стрельбы по данным, полученным из опытов, г. Чебышёв нарочно для Комитета составил свои знаменитые в

Европе формулы интерполирования, чрезвычайно упрощающие работу вычисления и тем не менее дающие весьма точные результаты».

ИНИЦИАТОР СИСТЕМЫ ОБРАЗОВАНИЯ, УСТОЙЧИВОЙ К РЕВОЛЮЦИЯМ И ВОЙНАМ

Пафнутий Львович совмещал много лет преподавание математики в Петербургском университете с неустанными трудами не только в Артиллерийском комитете, но и на поприще организации образования в России. Он известен как деятельный член Учёного комитета Министерства народного просвещения, с чьим именем связана система естественно-научного и инженерного образования, сложившаяся в России во второй половине XIX столетия. Возникшая тогда острейшая потребность в квалифицированных технических кадрах поставила перед российской властью вопрос о значительном наращивании числа подготавливаемых инженеров. Появилось предложение обучать инженеров на физико-математических факультетах университетов. Чебышёв выступил против этого предложения, считая более целесообразным сосредоточить подготовку инженеров в высших технических учебных заведениях, а в университетах готовить специалистов по фундаментальным наукам. Именно по этому пути создания значительного числа технических вузов различного профиля и пошла российская высшая школа. Занимаясь народным просвещением, Пафнутий Львович добивался увеличения окладов преподавателей, разрабатывал программы математического образования для средних и высших учебных заведений. Он обосновывал и отстаивал необходимость знакомства старшеклассников с понятиями комбинаторики, дифференциального исчисления и аналитической геометрии. В дальнейшем, как мы знаем, большие государственные вложения в образование стали приносить свои плоды. Учёные и инженеры России прочно утвердились на передовых позициях в мире. Общеизвестны российские корни самых громких достижений в области электротехники, радио, телевидения, авиации.

«ЭТА НАУКА ДЛЯ НАС, РУССКИХ, ПРЕДСТАВЛЯЕТ ОСОБЕННЫЙ ИНТЕРЕС...»

Ко второй половине XIX столетия Россия уже давно была интегрирована в культурную жизнь Европы. Достижения в науке, технике и образовании легко преодолевали границы. Пользовались успехом многочисленные научные и отраслевые технические журналы. Если раньше такая литература печаталась на французском и немецком языках, то с середины века в России приступили к изданию научных журналов на русском языке. Активизировались связи между учёными. Чебышёв тоже часто бывал в Европе. Общей тенденцией тогда стала организация научных обществ по математике, физике, химии и другим отраслям знания. Московское математическое общество по времени открытия даже опередило такие же общества в Лондоне и Париже. Чебышёв активно участвовал и в создании, и в деятельности Московского математического общества. Вот что он написал в своей докладной записке по поводу его финансирования:

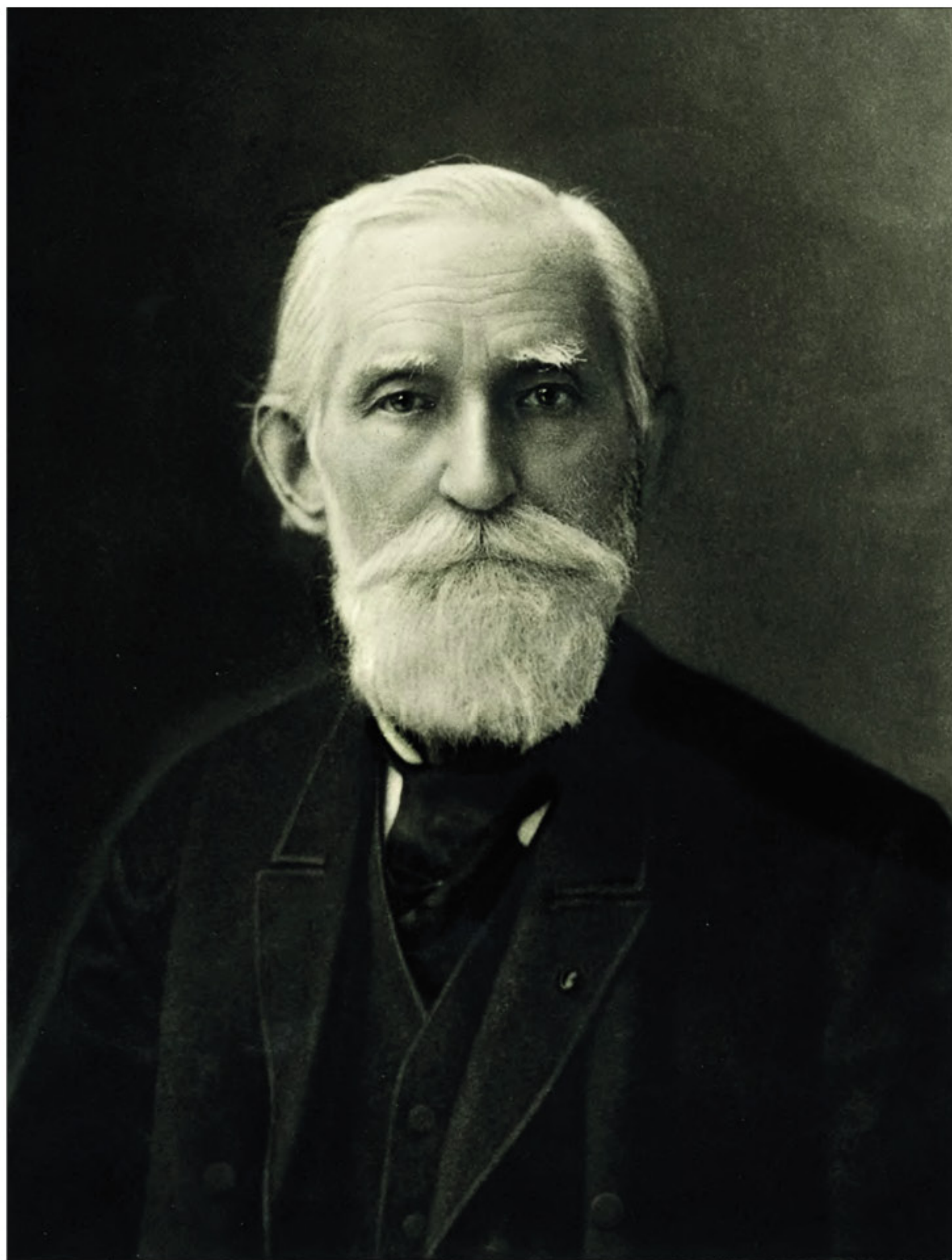
«Принимая в соображение всю пользу учреждения математического общества в России, нельзя не пожелать, чтобы существование его и необходимые для успеха его средства не были в зависимости от частной благотворительности. Я полагаю, что следовало бы испросить назначения Московскому математическому обществу ежегодно какой-нибудь суммы для покрытия хотя части его расходов на библиотеку и издание трудов. Кроме высокого значения математики в деле общего образования и пользы её практических применений, эта наука для нас, русских, представляет особенный интерес: это — наука, к которой, по отзыву иностранных учёных и по истории образования в нашем отечестве, мы русские, имеем особое призвание, и по этой науке, в большей или меньшей степени, мы можем состязаться с иностранцами. Такому состязанию в деле науки, лестному для национальной гордости, нельзя отказать в пособии, которым пользуются некоторые учёные общества по предметам, не представляющим ничего подобного».



Останки П.Л. Чебышёва похоронены на малой родине, в склепе под колокольной церковью Спаса на Прогнани. Фото: temples.ru

ЗАСЛУЖЕННОЕ ПРИЗНАНИЕ

Именно с Чебышёва как создателя крупной научной школы началась непрерывная череда выдающихся достижений российских математиков. Как много он сумел и успел сделать сам! Чебышёв предстаёт перед нами как великий математик, механик и основоположник современной картографии, как государственный деятель и создатель множества разнообразных механических устройств. Среди них оригинальный арифмометр, инвалидная коляска и стопоходящая машина, представленные на всемирных выставках. Научные труды Чебышёва ещё при его жизни получили широкое мировое признание. Он получил много наград, достиг вершины чиновной лестницы — стал действительным тайным советником, что соответствовало чину полного генерала. Повсюду — в академиях наук, научных обществах, университетах — он был избран почётным членом. В 1874 году его избрали действительным членом Парижской академии наук — первым из российских учёных в XIX столетии. Ему писали из Парижа, что французские математики считают его величайшим аналитиком столетия и преемником К. Гаусса. В 1890 году по предложению Парижской АН президент Франции



Пафнутий Львович Чебышев

наградила Чебышёва командорским крестом ордена Почётного легиона. По поводу этой награды президент Парижской АН Шарль Эрмит написал в письме к Чебышёву следующее:

«Дорогой собрат и друг! Я позволил себе большую вольность в отношении Вас, взяв на себя, как президент Академии Наук, смелость обратиться к министру иностранных дел с ходатайством о награждении Вас командорским крестом ордена Почётного Легиона, который и был Вам пожалован

Президентом Республики. Это отличие является лишь небольшой наградой за великие и прекрасные открытия, с которыми навсегда связано Ваше имя и которые давно уже выдвинули Вас в первые ряды математической науки нашей эпохи. Но мне хотелось напомнить Вам о себе и выполнить то, что я считал долгом дружбы. Все члены Академии, которым было представлено возбуждённое мною ходатайство, поддержали его своей подписью и воспользовались случаем засвидетельствовать

живейшую симпатию, которую Вы им внушаете. Все они присоединились ко мне, заверяя, что Вы являетесь гордостью науки в России, одним из первых геометров Европы, одним из величайших геометров всех времён».

«ТРУДЫ ЧЕБЫШЁВА НОСЯТ ОТПЕЧАТОК ГЕНИАЛЬНОСТИ»

Современники отмечали и высокие человеческие достоинства Пафнутия Львовича. В памяти учеников сохранились его слова, которым он сам неизменно следовал: «Честь дороже прибытка». Великий труженик скончался за письменным столом. Своё ощущение от общения с учителем ученики П. Л. Чебышёва А. А. Марков и И. Я. Сонин, сами уже ставшие академиками, выразили словами: «Труды Чебышёва носят отпечаток гениальности...».

ЗЕМНОЕ И ЗВЁЗДНОЕ НАСЛЕДИЕ ЧЕБЫШЁВА

О П. Л. Чебышёве напоминает система подготовки математических, естественно-научных и инженерных кадров, реализованная в России во второй половине XIX века по его предложениям, а также богатое теоретическое наследие, созданное им и его последователями. Но главным наследием стали его ученики, это целое созвездие выдающихся учёных! А. А. Марков и А. М. Ляпунов, Е. И. Золотарёв и Г. Ф. Вороной, Ю. В. Сохоцкий и Д. А. Граве... А за ними последовали новые поколения талантливых учеников. В военном 1944 г., в память 50-летия кончины великого математика и механика, правительство СССР позаботилось об издании полного собрания сочинений П. Л. Чебышёва. В этом решении отразилось не только признание масштабов его личности. Здесь видится и признание укоренённости военных успехов, достигнутых и будущих, в той научной и образовательной базе, которую создала Россия в прошлом, несмотря на все идеологические различия. Советские криптографы убедительно продемонстрировали свою неразрывную связь с наследием Пафнутия Львовича Чебышёва и его учеников и в предвоенные, и в военные, а особенно в послевоенные годы.



Картина «В. И. Ленин и Ф. Э. Дзержинский»
художника Б. Щербакова

В НАЧАЛЕ СТОЛЕТНЕГО ПУТИ

5 МАЯ 1921 ГОДА БЫЛ СОЗДАН СПЕЦИАЛЬНЫЙ ОТДЕЛ
ПРИ ВЧК — ПЕРВАЯ КРИПТОГРАФИЧЕСКАЯ СЛУЖБА
СОВЕТСКОЙ РОССИИ

5 мая 2021 года отмечается столетие постановления Совнаркома о создании Специального отдела при ВЧК. Это событие принято считать той точкой отсчёта, начиная с которой заявила о себе Криптографическая служба Советской России, затем СССР, а с 1991 года и современной России.

Вместе с тем представляется, что значение упомянутого постановления в момент его издания трактовалось заметно шире. Исследователи обоснованно считают, что принятые решения положили начало созданию системы защиты информации в нашей стране.

АКТ ЗАПОЗДАЛЫЙ И СВОЕВРЕМЕННЫЙ ОДНОВРЕМЕННО

Издание указа Совнаркома о создании Спецотдела было актом запоздалым и своевременным одновременно. Запоздалым, так как и с засекречиванием связи, и с защитой информации в советских органах власти дело обстояло неудовлетворительно.

Так, в августе 1920 года английское правительство через газету «Таймс» фактически официально признало факт чтения советской переписки.

Сложившееся положение ярко характеризует шифртелеграмма, посланная

М. В. Фрунзе в центр из Крыма 19 декабря 1920 года:

«Москва, Предсовнаркома Ленину, Предреввоенсовета Троцкому, Главкому, Наркоминдел Чичерину, ЦК РКП(б).

Из представленного мне сегодня бывшим начальником врангелевской радиостанции Ямченко доклада устанавливается, что решительно все наши шифры вследствие их несложности расшифровываются нашими врагами. Вся наша радиосвязь является великолепнейшим средством ориентирования противника. Благодаря тесной связи с шифровальным отделением морфлота Врангеля, Ямченко имел возможность лично

читать целый ряд наших шифровок самого секретного военно-оперативного и дипломатического характера; в частности, секретнейшая переписка Наркоминдела с его представительством в Ташкенте и Европе слово в слово известна англичанам, специально организовавшим для подслушивания наших радио целую сеть станций особого назначения. То же относится к расшифрованию свыше ста наших шифров. К шифрам, не подававшимся прочтению немедленно, присылались ключи из Лондона, где во главе шифровального дела поставлен англичанами русскоподданный Феттерлейн, ведавший прежде этим делом в России. Общий вывод такой, что все наши враги, в частности Англия, были постоянно в курсе всей нашей военно-оперативной и дипломатической работы. Копию доклада Ямченко препровождаю с нарочным. Изложенное докладываю для принятия соответствующих мер.

19 декабря Командвойск Укр Фрунзе».

Были и другие тревожные известия. Но телеграмма Фрунзе относится ко времени, когда положение в области защиты информации стало совершенно нетерпимым, поскольку оно уже значительно повлияло на срыв планов большевиков о переносе революции в страны Европы и стало одной из причин разгрома в польском походе Красной Армии в 1920 году.

Всё же создание в мае 1921 года Специального отдела как органа, ответственного за налаживание защиты информации в Советской России, явилось и вполне своевременным. Ведь только к концу 1920 года среди руководителей партии большевиков утвердилось, как известно, мнение о задержке мировой революции и необходимости серьёзного государственного обустройства на советской территории. До этого момента успех русской революции воспринимался вождями коммунистов лишь как проходной этап в достижении ближайшей цели — революционной победы в развитых европейских странах. При этом изначально сама Россия рассматривалась только в качестве ресурсной базы. С марта 1919 года в Москве действовал Исполком Коминтерна — штаб мировой революции. В нём были представлены все коммунистические партии, в том числе РКП(б). Исполком

Коминтерна сразу же активно занялся созданием своих организаций и боевых отрядов по всему миру. Но в конце 1920 года крестьянские восстания, а затем и военный мятеж в Кронштадте заставили власть руководствоваться не только партийными интересами, но и первостепенными задачами государственного строительства.

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ — НЕОТЛОЖНАЯ ЗАДАЧА

Одной из таких неотложных задач стало обеспечение защиты информации, актуальное и для партийных интересов, и для государства. Надо сказать, что обеспечение защиты информации первоначально фигурировало в документах как внутрипартийная задача, решавшаяся одновременно с реорганизацией аппарата ЦК при переходе от «военного коммунизма» к НЭПу. Согласно исследованиям Г.А. Куренкова, 2 августа 1920 года создаётся Шифрбюро Секретариата ЦК РКП. Оно «предназначалось для ведения зашифрованной секретной переписки с органами и отдельными ответственными сотрудниками РКП(б), ЦК коммунистических партий, Исполкомом Коминтерна, а также с государственными ведомствами, имевшими шифрсвязь. Шифрбюро изготовляло, хранило, рассылало и вело учёт шифров и инструкций по пользованию ими для партийных организаций, вело методическую и инструкторскую работу, зашифровывало и расшифровывало поступающую в Секретариат ЦК корреспонденцию». Шифрбюро входило в состав Секретного отдела Секретариата ЦК. На заседании Оргбюро от 20 октября 1920 года был рассмотрен вопрос о Секретно-оперативном отделе Секретариата ЦК РКП(б). Постановили: «а) Секретно-оперативный подотдел секретно-редактивной части преобразовать в самостоятельный отдел, б) Заведующим секретно-оперативным отделом назначить т. Г.И. Бокия». К сожалению, функции отдела в документах не отражены. По косвенным свидетельствам защита партийных секретов строилась под сильным влиянием традиций революционного подполья, в том числе с поиском предателей и вражеских агентов в своей среде.

«ОПЫТНЕЙШИЙ ПРОФЕССИОНАЛЬНЫЙ РЕВОЛЮЦИОНЕР»

Назначение Г.И. Бокия на такой ответственный пост подтверждает его высокий авторитет в ЦК РКП(б). Это был опытный профессиональный революционер: член РСДРП с 1900 года, 12 раз подвергался арестам за организацию и участие в вооружённых налётах, провёл два с половиной года в сибирской ссылке. С апреля 1917 по март 1918 года — секретарь Петроградского комитета РСДРП(б), руководитель Петроградской ЧК, организатор «красного террора» в Петрограде. С 1919 года в органах ВЧК на фронтах, видный деятель Коминтерна.

Вероятно, возглавив Секретно-оперативный отдел, Г.И. Бокий оказался на острие партийно-государственных забот о защите информации, даже более того, забот о качестве шифрованной связи. Связаны они были, среди прочего, и с расследованием хищений в созданном в феврале 1920 года Гохраном, куда стекались потоки конфискованных ценностей с целью их реализации за границей. Интересно, что довольно долго в Гохране не могли наладить учёт поступивших драгоценностей. Положение с их расхищением стало особенно нетерпимым после появления сообщений и даже зарубежных публикаций о дешифровании частной переписки некоторых руководящих работников, пытавшихся продать уворованное иностранным покупателям.

РОЖДЕНИЕ СПЕЦИАЛЬНОГО ОТДЕЛА

В январе 1921 года коллегия ВЧК выступила с инициативой созыва совещания представителей заинтересованных ведомств для подготовки предложений по воссозданию шифровальной и дешифровальной служб. В обсуждении вопроса принимали участие представители ЦК РКП(б), ВЧК и наркоматов. В результате этой работы к марту были подготовлены предложения об учреждении межведомственной шифровальной комиссии при Совнаркоме Республики, состоящей из представителей Наркомвоена, ВЧК, Наркоминдела и Наркомвнешторга под председательством представителя ВЧК. Размытая

ответственность в предложенном проекте стала причиной отклонения его в верхах. Тренд был другой. 29 марта 1921 года на Политбюро слушалось заявление Лежавы о разглашении секретных сведений. На заседании постановили: «Сообщение т. Лежавы принять к сведению, предложив ему передать весь материал с устными добавлениями т. Дзержинскому, которому поручить строго расследовать это дело. Доклад представить в Политбюро». ВЧК поручили и шифровальное дело. В резолюции по предложению Ленина записали: «Поручить начальнику шифровального отдела ВЧК принять меры к осуществлению надзора, контроля и руководства шифровальным делом в Республике и представить в Малый совет соответствующий проект Постановления, согласовав его с наиболее заинтересованными ведомствами в первую голову». 12 апреля на заседании Малого Совнаркома с проектом о создании Специального отдела при ВЧК выступил будущий начальник этого отдела, человек, которому предстояло стать организатором криптографической службы страны, — Глеб Иванович Бокий.

Текст этого проекта хорошо известен, прежде всего по популярной книге Т.А. Соболевой «История шифровального дела в России», напомним лишь его начало.

«Имея в виду: 1) Отсутствие в Республике центра, объединяющего и направляющего деятельность шифровальных органов различных ведомств, и связанные с этим бессистемность и случайность в постановке шифровального дела, 2) Возможность, благодаря этому при существующем положении широкого осведомления врагов Рабоче-Крестьянского государства о тайнах Республики, Совет Народных Комиссаров постановил:

Образовать при Всероссийской Чрезвычайной Комиссии «Специальный отдел», штаты в коем утверждают Председателем ВЧК. Начальник Специального отдела назначается Совнаркомом».

В круг ведения Специального отдела при ВЧК включили постановку шифровального и дешифровального дела в РСФСР. Все распоряжения и

циркуляры Специального отдела при ВЧК по вопросам шифровального и дешифровального дела стали обязательными к исполнению всеми ведомствами РСФСР.

Как мы знаем, Специальный отдел при ВЧК был учреждён 5 мая 1921 года постановлением Малого Совнаркома, начальником отдела назначили Г.И. Бокия. В момент создания Спецотдел фактически не подчинялся руководству органов безопасности и находился в ведении партии. Правда, с февраля 1922 года отдел именовался уже просто Спецотделом ГПУ, а с 1923 года — Спецотделом ОГПУ.

СТРУКТУРА СПЕЦОТДЕЛА

Отдел включал в себя семь отделений.

1-е отделение — «наблюдение за всеми государственными учреждениями, партийными и общественными организациями по сохранению государственной тайны, а также разработка руководящих и нормативных документов, регламентирующих различные стороны организации защиты государственной тайны в целом по стране».

2-е отделение — «перехват шифровок иностранных государств; радиоконтроль и выявление нелегальных и шпионских радиоустановок; подготовка радиоразведчиков». Кроме того, сотрудники 2-го отделения Спецотдела занимались разработкой шифров и кодов для ВЧК и всех заинтересованных учреждений страны. Отделение в первые годы работы состояло из семи человек.

Перед **3-м отделением** стояла задача «ведения шифрработы и руководство этой работой в ВЧК». Состояло оно вначале всего из трёх человек, руководил отделением бывший латышский стрелок Ф.И. Эйхманс, одновременно являвшийся заместителем начальника Спецотдела.

Сотрудники **4-го отделения**, их было восемь человек, занимались «открытием иностранных и антисоветских шифров и кодов и дешифровкой документов». Начальником этого отделения, четвёртым с момента основания, с сентября 1923 года утвердился на 15 лет А.Г. Гусев, соратник Г.И. Бокия. Всё это время он выполнял и обязанности помощника начальника Спецотдела, а временами и заместителя.



Начальник Спецотдела Г. И. Бокий

5-е отделение занималось проверкой ведения секретного делопроизводства и соблюдения режима секретности в партийных и государственных структурах, начальник — В.Д. Цибизов.

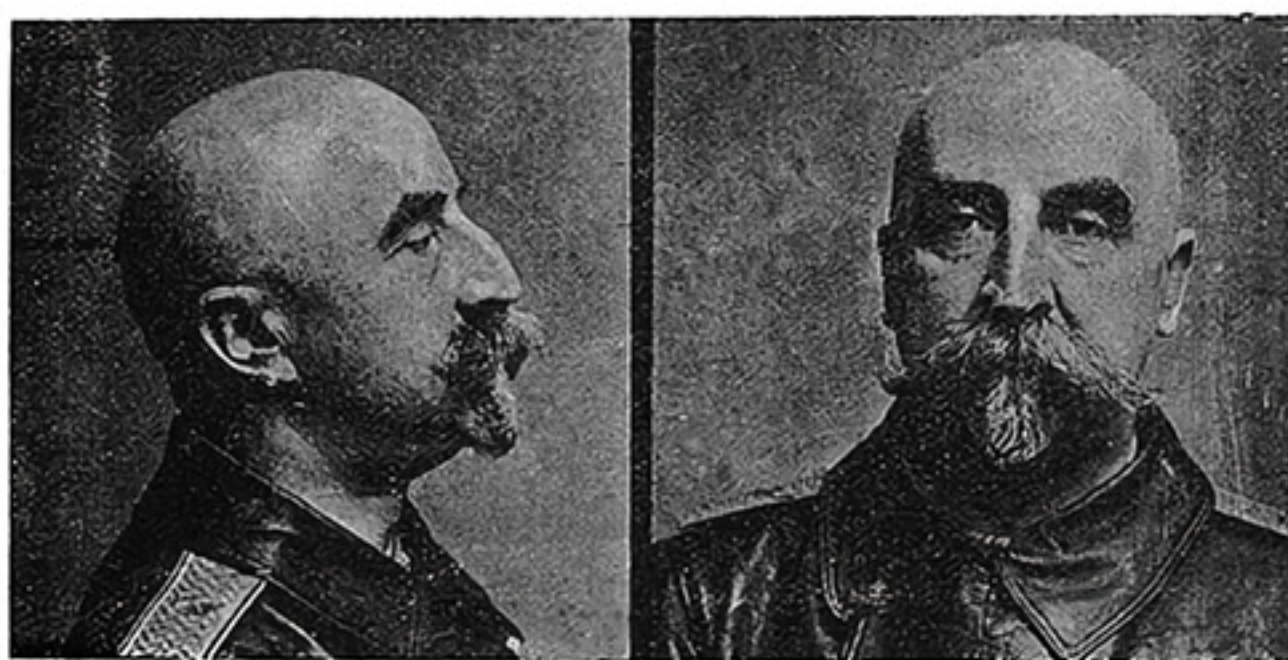
6-е отделение — «изготовление конспиративных документов». **7-е отделение** — «химическое исследование документов и веществ, разработка рецептов. Экспертиза почерков, фотографирование документов». Начальник — Е.Е. Гоппиус, он же заведовал наукой в отделе.

Было ещё вспомогательное, техническое отделение.

КАДРЫ РЕШАЮТ ВСЁ!

Фактически основной функцией отдела стало обеспечение защиты секретной информации в государстве и партии. Собственно криптографические задачи, в строгом понимании, решали только три отделения: 2-е, 3-е и 4-е. Постепенно основной состав Спецотдела стал включать около 100 сотрудников. Исследователи пишут и о негласном контингенте приблизительно такого же количества. Около половины негласных сотрудников использовались в работах трёх криптографических отделений, их именовали экспертами и переводчиками. Понятно, что Бокию стоило огромных усилий укомплектовать Спецотдел подходящими кадрами.

№ 207.

Кривошъ, Владимиръ Ивановичъ. Дактилоскоп. № 13. | 1/1 $\frac{41333}{42333}$ |

Ст. Сов., род. 1 Декаб. 1865 г. въ Венгрии, словакъ, правосл., ростъ 1 м. 74 с., обуч. въ Петрогр. Университ., служ. въ Государств. Совѣтъ, прож. въ Петроградѣ, Екатерингофск. пр. 61, женатъ на Антонии Ивановой Якинской; им. брата Ивана за границей.
Задерж. 6 Апр. 1915 г. въ г. Самборѣ по подозр. въ шпион. Зарегистр. 17 Мая 1915 г. въ Петр. Охр. Отд.

В. И. Кривош в 1915 году

Представляется очевидным, что и в разработке самого проекта создания Спецотдела приняли участие специалисты, а ведь их тоже сначала надо было найти. Их было мало, но среди них оказались В. И. Кривош, И. А. Зыбин и И. М. Ямченко. Вклад каждого из них в становление советской криптографической службы значителен, как и уникален опыт их прежней работы в шифровальном деле.

И. М. Ямченко принёс с собой успешный опыт морской радиоразведки. Свою службу он начал ещё на знаменитой Радиостанции особого назначения, расположившейся у входа в Финский залив и не давшей германскому флоту шансов в морском противоборстве на Балтике. В 1916 году Ямченко перевели в Севастополь для организации подобной же разведывательной радиостанции, он и возглавлял её до самого исхода врангелевских войск из Крыма в ноябре 1920 года и своего плена.

И. А. Зыбин, как известно, имел незаурядные способности и солидный опыт дешифровальной работы, он долгое время руководил ею в Департаменте полиции до своего увольнения за финансовые провинности.

«ЖИЗНЬ И ПРИКЛЮЧЕНИЯ ВЛАДИМИРА КРИВОША»

В. И. Кривош обладал таким широким спектром разнообразных способностей, знаний и опыта, в том числе дешифровального, что удостоился в наше время жизнеописания с

красноречивым названием «Сорок лет на секретной службе: жизнь и приключения Владимира Кривоша» (авторы А. А. Зданович, В. С. Измозик). Приведём кратко некоторые моменты его биографии.

В. И. Кривош (1865–1942) родился в нынешней Словакии, по национальности русин, в 1888 году принял подданство России. Служил в Санкт-Петербурге в почтовой цензуре, преподавал стенографию, затем переводчик-дешифровщик при секретном отделении Департамента полиции (1904–1906), сотрудник Особого делопроизводства (контрразведки) Морского Генерального штаба (1905–1911), уволен за финансовые злоупотребления. С начала Мировой войны переводчик при штабе 8-й армии (1914–1915), арестован в апреле 1915 года по подозрению в шпионаже. Выслан в Иркутскую губернию под гласный надзор полиции.

Вернулся в Петроград в апреле 1917 года и после 25 октября сотрудничал с советской властью. Вновь был арестован 25 января 1918 года и осуждён Ревтрибуналом к одному году заключения как «умышленно пытавшийся дискредитировать советскую власть». Освобождён по амнистии 21 мая 1918 года. Затем переводчик отдела военного контроля (с декабря 1918), сотрудник разведотдела при Штабе Западного фронта (с марта 1919), переводчик-дешифровщик Петроградской (с апреля 1919)

и Московской ЧК, заведомо проверки документов при Особом отделе ВЧК (с июля 1919). Новый арест — 28 июля 1920 года, по обвинению в получении взятки «за передачу пропуска в прифронтовую полосу неизвестному лицу, пытавшемуся нелегально переправиться за границу». Вместе с В. И. Кривошем арестовали его сына Романа, служившего в бюро пропусков ОО Московской ЧК. Именно он за переданную взятку незаконно достал пропуск. Постановлением Президиума ВЧК 29 декабря того же года В. И. Кривоша приговорили к высшей мере наказания, но по амнистии расстрел заменили десятью годами заключения. 14 апреля 1921 года он был освобождён и направлен на работу в Спецотдел в качестве эксперта. С этого времени В. И. Кривош добавил к своей фамилии приставку Неманич, её смысл понятен: нема нич — нет ничего. 13 ноября того же года он был арестован ОО ВЧК за принятие мер к выезде за границу. В тюрьме встретился с сыном Романом. Любопытная деталь: находясь в Бутырской тюрьме вместе со своим сыном, также уже сотрудником Спецотдела, Кривош-Неманич продолжал исполнять свои служебные обязанности, начальник дешифровального отделения приносил обоим работу в камеру. Освобождён постановлением коллегии ГПУ 13 мая 1922 года под домашний арест с использованием в Спецотделе. По новому обвинению в шпионаже, «за несанкционированные контакты с представителем чехословацкой миссии», арестован 23 марта 1923 года. Постановлением коллегии ГПУ от 27 июня того же года заключён в лагерь на десять лет. Отбывал наказание на Соловках. Постановлением коллегии ОГПУ 8 октября 1928 года был досрочно освобождён, продолжал работу в Спецотделе вместе с сыном Романом. 7 октября 1935 года по решению руководства Спецотдела ГУГБ НКВД «из-за возраста и пониженной трудоспособности» был переведён на пенсию, умер в Уфе в 1942 году. Романа Кривоша вновь арестовали в 1937 году по делу сотрудников Спецотдела и приговорили к восьми годам заключения, в Бутырской тюрьме он продолжал заниматься дешифрованием.

Освобождён в октябре 1941 года и эвакуирован в Уфу для занятий шифровальными делами. 3 апреля 1942 года в числе других работников ГУГБ НКВД за образцовое выполнение заданий Правительства Р. В. Кривоша наградили медалью «За трудовое отличие».

ВСЁ ПОЗНАЁТСЯ ПО ПЛОДАМ

Приведённые подробности очень показательны. Они позволяют хотя бы немного почувствовать обстановку 20-х годов и те условия, в которых вынужденно начиналось создание криптографической службы нового государства. Руководили созданием службы революционеры, и действовали они революционными методами, в том числе суда и наказания. Как известно, Г. И. Бокий курировал Северные лагеря, и Спецотдел участвовал в создании Соловецкого лагеря особого назначения (СЛОН) в 1923 году.

Среди руководителей отделений и отдела мы видим А. Г. Гусева и Ф. И. Эйхманса. Это ближайшие сподвижники Г. И. Бокия, им он доверял и с ними создавал отдел. Заметим, что, согласно архивным документам, начальник дешифровального отделения А. Г. Гусев имел лишь «низшее образование». Это ни в коей мере не умаляет его заслуг, но свидетельствует и о способностях, и о том, что роль малочисленного 4-го отделения была в основном организаторская, с чем оно довольно успешно справлялось. Ведь уже вскоре удалось открыть курсы по подготовке криптографов, использовавшие богатое наследие имперского периода в виде учебных пособий и инструкций к шифрам. Выпускники курсов создали в последующие годы ту разветвлённую структуру, которую мы именуем Криптографической службой страны. Среди первых курсантов мы знаем Б. А. Аронского и С. С. Толстого, ныне символизирующих успех советской криптографии в Великой Отечественной войне.

ПЕРВЫЕ ДОСТИЖЕНИЯ СПЕЦОТДЕЛА

В сохранившемся отчёте о работе Спецотдела за 1921 год указано, что за год было введено в действие на различных линиях связи 96 новых кодов.

Одновременно 3-е отделение отдела налаживало подготовку шифрработников на своих курсах, там в 1923 году обучались и шифровальщики ЦК РКП(б). Усилия по созданию новых шифров особенно активно поддерживались правительством. Так, секретарь ЦИК СССР А. С. Енукидзе писал Бокию 2 сентября 1924 года: «Поздравляю тов. Г. И. Бокия с окончанием составления «Русского кода» — этого громадного и сложного труда».

30 августа 1922 года Секретариат ЦК РКП(б) принял постановление и утвердил инструкцию «О порядке хранения и движения секретных документов». Исследователи констатируют, что это была первая общегосударственная инструкция по вопросам секретного делопроизводства. Для ведения секретного делопроизводства в партийных и государственных учреждениях создавались секретные части. Увольнение и перемещение в шифровальных частях, в том числе НКВД, разрешалось только с ведома Спецотдела. Постановление узаконило плановый характер проведения проверок. Проверке подвергались не только партийные комитеты и должностные лица, но и секретные подразделения ведомств. По согласованию с Секретным отделом ЦК проверку производил Специальный отдел ОГПУ. По результатам проверки Спецотдел ОГПУ составлял акт. В середине 1920-х годов под актами стояли три подписи: начальника Спецотдела ОГПУ Г. И. Бокия, заместителя начальника отдела А. Г. Гусева и начальника 5-го отделения Спецотдела В. Д. Цибизова.

КРИЗИС В ШИФРОВАЛЬНОМ ДЕЛЕ ПРЕОДОЛЁН

Вскоре после бегства за границу Б. Г. Бажанова, секретаря И. В. Сталина, в 1926 году, в обстановке обострения международных отношений, английское правительство приняло решение опубликовать избранные места из секретной советской переписки. Тогда в СССР была оперативно изменена система пользования шифрами в государственном масштабе, что выразилось, прежде всего, в переходе к одноразовым шифроблокнотам и разделению секретного и шифровального делопроизводства. В тот сложный



Знак «100 лет Криптографической службе Российской Федерации». Разработан Народным художником России, почётным членом Российской академии художеств В. Г. Никоновым

период Политбюро на своём закрытом заседании утвердило постановление «О пользовании секретными материалами». Специальному отделу ОГПУ поручалось «наблюдать за правильным использованием учреждениями и лицами имеющихся у них шифров», а также на него возлагался общий контроль за проведением в жизнь решений Политбюро по защите информации. Вскоре усилились контроль на местах и кадровое обеспечение со стороны Спецотдела, а затем функции секретного и шифровального делопроизводства целиком перешли в ведение ОГПУ.

* * *

Как следствие, после мая 1927 года английские криптоаналитики перестали читать шифрованную дипломатическую переписку СССР. И это было существенным успехом, говорившим о том, что кризис, связанный с кадровым, интеллектуальным, организационным и техническим отставанием в области криптографии, преодолён. Но на пути к созданию Криптографической службы страны ещё предстояло пройти долгие годы, полные напряжённого труда.

ТОП-12 МЕР БЕЗОПАСНОСТИ ДЛЯ API

ЗАМЕТКИ БЕЗОПАСНИКА



Александр БОДРИК
управляющий
директор
Cyberlands.io API
Penetration Testing
Company, CISA

Пока суд да дело, через API стали воровать деньги. Хороший пример — февральское хищение с пользовательских счетов через API, по поводу чего ЦБ РФ направил в банки предупреждающее письмо¹.

Мой тезис простой: в API-мире HTTP-запросы пользователей могут неожиданно меняться по объёму и скорости, что делает поведение back-end непредсказуемым. Это может быть результатом злонамеренных усилий, направленных на перехват управления системами, поэтому разумно применять меры безопасности API.

В этой статье описаны топ-12 мер, нацеленных на обеспечение конфиденциальности данных пользователей, защиты от манипуляции back-end через API и доступности цифровых услуг.

МЕРЫ ПРИ РАЗРАБОТКЕ

1. Документация по API. Правильная документация (например, Swagger) необходима для обеспечения устойчивости разработки и работы вашего API.

2. Проверка API Schema. API должен соответствовать принятому в отрасли стандарту (OpenAPI), и самый простой способ добиться этого — использовать проверки API Schema.

3. Аутентификация API. Используйте аутентификацию перед обработкой запроса — каждый запрос должен исходить от аутентифицированного пользователя. Тут хорошо помогут протоколы аутентификации, такие как OAuth.

4. API-авторизация — ещё один отличный инструмент, ограничивающий

доступ к тому, что необходимо для выполнения определённых задач. Это ограничивает площадь атаки для злоумышленника и ограничивает возможные финансовые потери, если ваш облачный провайдер выставит вам счёт за чрезмерное использование трафика (особенно актуально при serverless-вычислениях).

5. Логирование. Ведение журнала — это ваши глаза. Отсутствие полноценно заполненного журнала означает отсутствие подсказок, что и почему произошло с вашими API-эндпойнтами или другими компонентами и серверной частью системы.

ОПЕРАЦИОННЫЕ МЕРЫ

6. Лимиты API и политики управления использованием — это правила обработки запросов к API. Среди них — проверка геолокации, лимиты API — управление пиками количества запросов, ограничение (лимиты) количества одновременных запросов и квоты API.

7. Экранирование API. Ни один API не должен иметь прямого доступа из интернета. Мобильные приложения, CDN, API Gateway или WAF — популярные пути реализации политик управления лимитами и использованием API.

8. Мониторинг API показывает, насколько быстрым является ваш API, и позволяет видеть время, затрачиваемое различными уровнями вашего приложения (db, back-end etc) на обработку запроса.

КОНТРОЛИ БЕЗОПАСНОСТИ

9. Обнаружение API. Иногда службы безопасности оставляют API без надзора или даже существуют «теневые API». Мера по обнаружению находит

все API и сообщает о них вашей команде по кибербезопасности.

10. Тест на проникновение API. Тест на проникновение (пентест) — это наиболее гибкий способ тестирования средств контроля безопасности API. Как поставщик услуг тестирования на проникновение API, мы рекомендуем разработать и внедрить элементы управления безопасностью API, прежде чем заказывать тест на проникновение.

11. L7 DDoS-симуляция. Современные DDoS-атаки фокусируются на уровне приложений, а именно API. Мера симуляции проверяет способности back-end / API обрабатывать запросы пользователей, эффективность и правильность настройки лимитов и политики использования API.

12. Мониторинг безопасности API. Последний и самый продвинутый контроль безопасности — это мониторинг безопасности API. Это средство защиты призвано служить последней линией обороны: обнаруживать аномалии в последовательностях запросов API и запросах API.

Применение 12 средств контроля API позволяет защитить любое приложение, независимо от того, когда и как оно было создано. Тем не менее они лучше всего работают в сочетании друг с другом. Если вы хотите продолжить свой путь к защите своего цифрового стартапа / сервиса или пересмотреть существующую систему защиты, можно ознакомиться с нашим руководством «Cybersecurity for Fintech MVP»².

¹ <https://www.kommersant.ru/doc/4692079>

² <https://www.cyberlands.io/securityfintechmvp>



1–4 июня 2021 года

Московская область, Отель «Les Art RESORT»

ПОСВЯЩЁННЫЙ 100-ЛЕТИЮ КРИПТОГРАФИЧЕСКОЙ СЛУЖБЫ РФ

X симпозиум «Современные тенденции в криптографии»



Тематика симпозиума включает следующие вопросы (но не ограничивается ими):

- исследование криптографических алгоритмов и протоколов, в том числе являющихся международными стандартами;
- эффективная реализация методов анализа криптографических алгоритмов и протоколов;
- оценка криптографической стойкости российских криптографических алгоритмов и протоколов;
- эффективная реализация российских криптографических алгоритмов и протоколов;
- математические аспекты криптографии;
- криптография в «Интернете вещей»;
- квантовая криптография и квантовые вычисления;
- постквантовая криптография;
- криптография и технология блокчейн;
- криптографическая защита биометрических данных;
- другие актуальные и перспективные направления криптографии.



ОРГАНИЗАТОРЫ



TK26



МИАН

ГЕНЕРАЛЬНЫЙ ПАРТНЁР

ОФИЦИАЛЬНЫЕ ПАРТНЁРЫ

ПАРТНЁР

ОРГПОДДЕРЖКА



ctcrypt.ru

ZECURION DLP 11

Новая версия системы защиты информации от утечек и корпоративного мошенничества



Защита от фотографирования экрана

Модуль Screen Photo Detector с мгновенной реакцией на попытку сотрудника сфотографировать экран монитора



Модуль Staff Control

Собственный модуль учёта и контроля рабочего времени сотрудников, в т. ч. для крупных парков ПК (свыше 30 тыс. рабочих станций)



Поведенческий анализ (UBA) и аномалии

Система определяет профили типичного поведения и аномалии для более эффективного выявления подозрительного поведения сотрудников



Прогноз рисков

Уникальная для DLP-рынка система оценки рисков с возможностью оперативно видеть актуальные угрозы и работать в первую очередь с ними



Система постановки задач и IRP

Встроенный модуль расследований и удобный конструктор шаблонов задач для адаптации к реальным бизнес-процессам ИБ-отдела



Обновлённый интерфейс

Современный web-интерфейс для повышения удобства работы с массивами данных и скорости поиска нужной информации



Узнайте больше
о новой версии DLP 11

www.zecurion.ru

- 20 лет опыта на рынке ИБ
- Реестр Минцифры, сертификаты ФСТЭК, ФСБ
- Признание аналитиков IDC, Forrester, Gartner
- Работа в сетях более 200 000 рабочих мест



ZECURION

+7 495 221-21-60 | info@zecurion.com



facebook.com/ZecurionRUS