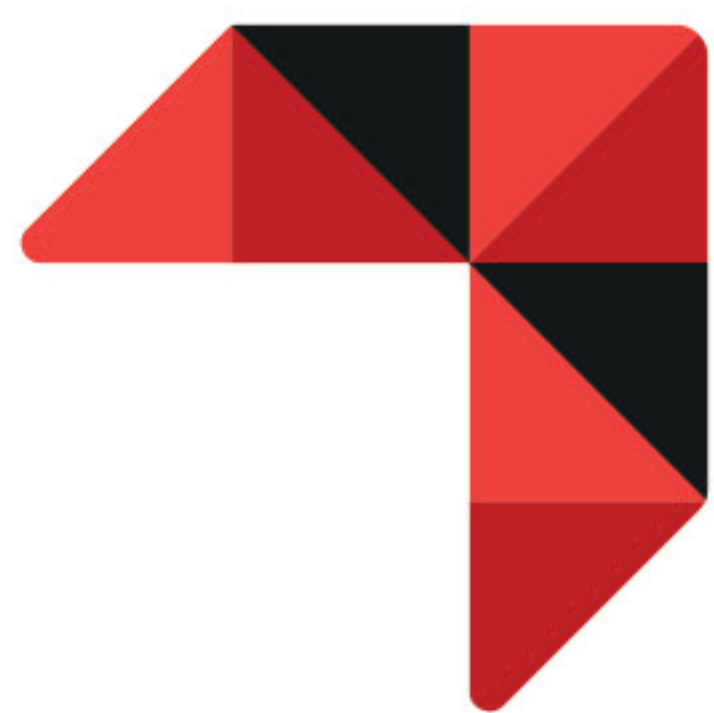




36

Василий ПИСКАРЕВ
Государственная Дума РФ
**Не дать погасить
«зарницы доверия»**

44

Василий ОКУЛЕССКИЙ
Банк «Возрождение»
Счастье для всех!



52

Андрей СТЕПИН
Компания «Актив»
**Новая эпоха
электронной подписи**

86

Рустэм ХАЙРЕТДИНОВ
Эксперт BIS Journal
**Проблему кадров в ИБ
решить можно...**

96

Сергей ВИХОРЕВ
ООО «ИТ-Экспертиза»
**Стакан наполовину
полон или наполовину
пуст?**

100

Александр БОДРИК
Cyberlands.io API Penetration
Testing Company
Заметки безопасника

BIG DATA: ИЩЕМ РАВНОВЕСИЕ



#socforum

#socforum

#socforum

#socforum

#socforum

7–8
декабря

FORUM

Узнай больше
ib-bank.ru/soc-forum2021

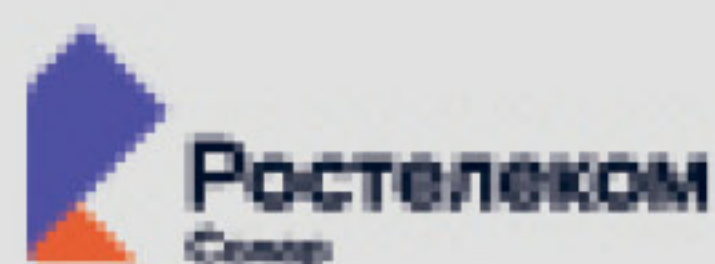


**SOC
ФОРУМ**

**Практика противодействия
кибератакам и построения
центров мониторинга ИБ**

г. Москва, Центр международной торговли

Генеральный партнёр



Организаторы

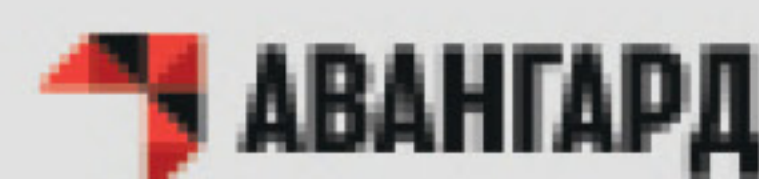


ФСБ России



ФСТЭК России

Оператор





Андрей КУРИЛО

заведующий кафедрой международной информационной безопасности Института информационных наук ФГБОУ ВО МГЛУ, кандидат технических наук, доцент

Решение кадровой проблемы в отрасли ИБ требует ответа на ряд вопросов. Сколько рынку труда необходимо специалистов, каких специальностей и квалификации? Насколько отвечает этим запросам подготовка специалистов в вузах? Что и как нужно изменить в системе образования и программах подготовки учащихся для удовлетворения потребностей рынка? Не будет преувеличением сказать, что это вопросы государственной важности, от них зависит выполнение основной задачи — цифровизации страны.

В этом году вузы начинают готовить специалистов по информационной безопасности в соответствии с новыми федеральными образовательными стандартами Минобрнауки РФ. Уже несколько лет их требования сопряжены с профессиональными стандартами — трудовыми функциями, которые определяет Минтруд РФ.

Профстандарты предназначены для закрепления типовых отраслевых практик, однако их положения в значительной степени уже устарели. Преодолеть это отставание можно, только наладив тесное взаимодействие вузов и работающих на рынке компаний. Лучшее поле для этого — сотрудничество во всех видах учебной и производственной практики студентов.

Информационная безопасность не сводится к изучению математики, физики и технических дисциплин, это практическая деятельность с колоссальным количеством ответвлений. От программирования и исследований кода до анализа уязвимостей, трассировки атак и социальной инженерии. Эти умения совершенствуются только на практике, «на кончиках пальцев».

В выигрыше окажутся профильные организации, стратегически решающие кадровую проблему. При организации эффективного взаимодействия с вузами они смогут заблаговременно готовить и отбирать для себя лучших, перспективных студентов. Присматриваться к ним, проверять практически, оценивать способности к профессиональному росту и другие деловые и личные качества.

Драйвером решения кадровой проблемы отрасли видится создание «учебных консорциумов», интеграция вузов и профильных компаний. Успеху могут немало способствовать государственные гарантии трудоустройства лучших выпускников.

Нельзя забывать и о преподавателях. Специалисты с рынка пойдут в государственное образование тогда, когда их зарплата будет хотя бы сопоставима с уровнем зарплат в коммерческих образовательных учреждениях. При этом мы прекрасно знаем, что коммерческие учебные заведения практически не занимаются базовым образованием, сосредоточившись на дополнительном образовании или переподготовке.

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
Воробьева 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
Левиев Д.О. — председатель Совета НП «Партнерство 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)
Филипчук 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 «Аладин РД»
Сумманен К.Т. — директор по управлению проектами — вице-президент, Банк ВТБ (ПАО), кандидат физико-математических наук
Хайретдинов Р.Н. — директор по росту компании BI.ZONE

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: **Воробьева 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, Салаватова Я.М.**
 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 07.07.2021. Тираж 5000 экз. Заказ № 782021.
 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, законодательство, Сбер, банки, криминал

ТЕМА НОМЕРА: БОЛЬШИЕ ДАННЫЕ ГРАЖДАН

- 10 Елена Покатаева (BIS Journal)
Между энтузиазмом бизнеса и фобиями обывателей
- 18 Надежда Щеголева (Институт развития информационного общества)
«Ситуация гораздо проще, чем думается»
- 19 Сергей Плуготаренко (РАЭК)
«У рынка больших данных большое будущее»
- 22 Алексей Раевский (Zecurion)
«От бумажной отчётности к латанию дыр, через которые течёт»
- 24 Сергей Назаренко (Рексофт)
«Предстоит научиться управлять БД как обоюдоострым оружием»
- 26 Алексей Кубарев (Ростелеком-Солар)
«Концепция суверенной идентичности вселяет надежду»
- 27 Дмитрий Романченко (Rubytech)
«ИБ существует в параллельном с ИТ-технологиями мире»
- 29 Дмитрий Васильев (ВС Лаб)
«Проблема БД — это в первую очередь моральный вызов»
- 31 Андрей Арефьев (InfoWatch)
«Гражданин должен знать, кто и зачем запросил его данные»

- 33 Андрей Тимошенко (Accenture)
«Цифровой суверенитет человека — это миф»
- 34 Игорь Ашманов (Крибрум, «Ашманов и партнёры»)
«Интернет — это новое пространство, и ему требуется свой кодекс»



10



36

РЕГУЛЯТОРЫ

- 36 **Государственная безопасность**
Василий Пискарев (Государственная Дума)
Не дать погасить «зарницы доверия»
- 42 **Социальная инженерия**
Вадим Уваров (Банк России)
ИБ финансовой сферы: что именно хочет донести ЦБ до участников рынка

БАНКИ

- 44 **Нормативная документация / Дискуссия**
Василий Окулесский (Банк «Возрождение»)
Счастье для всех!
- 46 **Нормативная документация / Дискуссия**
Сергей Вихорев (ИТ-Экспертиза)
Не дай нам Бог жить в эпоху перемен
- 48 **Нормативная документация / Дискуссия**
Александр Велигура (Ассоциация
российских банков)
Задача выглядит непосильной, но...
- 50 **Вредные советы**
Екатерина Рачкова (Банк ВТБ)
Рубите сплеча!



74

УГРОЗЫ И РЕШЕНИЯ

- 52 **Электронная подпись**
Андрей Степин (Компания «Актив»)
Новая эпоха электронной подписи
- 54 **Электронная подпись**
Павел Мельниченко (SafeTech)
Реальность, похожая на миф
- 57 **Системы защиты**
Кай Михайлов (iTPROTECT GROUP)
ПроКАТить хакера!
- 60 **Повышение квалификации**
Евгения Колодина (ЦИБИТ)
Обучение в сфере ИБ



57

ИНФРАСТРУКТУРА

- 62 **Деловые мероприятия**
Корней Реут (BIS Journal)
Форум DLP+
- 64 **Деловые мероприятия**
Павел Никифоров (BIS Journal)
PHDays 10
- 66 **Деловые мероприятия**
Валерий Куликов (BIS Journal)
The Standoff 2021
- 70 **Деловые мероприятия**
Павел Никифоров (BIS Journal)
CTCrypT 2021
- 72 **Деловые мероприятия**
Николай Кольский (BIS Journal)
AntiFraud Spring Russia 2021
- 73 **Деловые мероприятия**
Марк Новоначный (BIS Journal)
CISO-Форум 2021
- 74 **Удалёнка**
Денис Батранков (BIS Journal)
«Домашний арест»



СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

- 76** **Обучение персонала**
Андрей Жаркевич (Антифишинг)
Human firewall

ОБРАЗОВАНИЕ И КАРЬЕРА

- 82** **Обзор иноСМИ**
Марина Бродская (BIS Journal)
Возвращение к азам
- 86** **От первого лица**
Рустэм Хайретдинов (BIS Journal)
Только слушая бизнес



СУБЪЕКТЫ

- 90** **История**
Борис Столпаков (историк криптографии)
Сосредоточение перед взлётом
- 96** **Эссе**
Сергей Вихорев (ИТ-Экспертиза)
Стакан наполовину полон или наполовину пуст?
- 100** **Заметки безопасника**
«Спаси рядового санкциями!»
Александр Бодрик (Cyberlands.io API Penetration Testing Company)

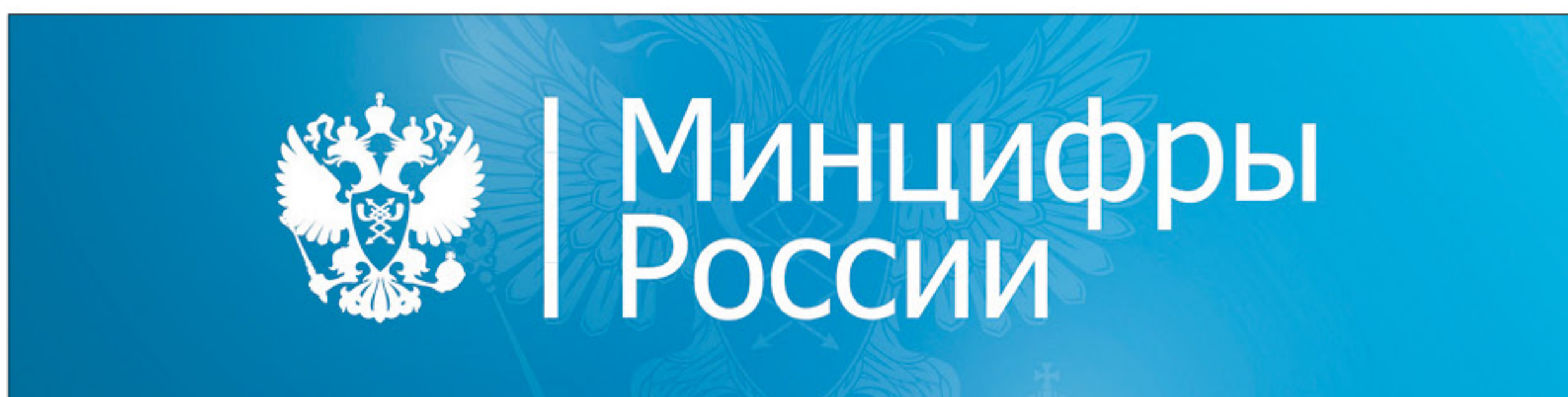


МИНЦИФРЫ БУДЕТ ВЫДАВАТЬ ЭП

Минцифры подготовило пресс-релиз, в котором сообщается, что ведомство предполагается наделить полномочиями по созданию и выдаче усиленной неквалифицированной электронной подписи.

«Законопроектом предусматривается наделение Минцифры России дополнительными полномочиями по созданию и выдаче усиленной неквалифицированной электронной подписи на безвозмездной основе участникам электронного взаимодействия, зарегистрированным в единой системе идентификации и аутентификации, в порядке и случаях, установленных правительством РФ», — сообщили в пресс-службе Минцифры.

«Указанный инструмент должен повысить доступ граждан к получению сервисов, при которых важно гарантированное обеспечение неизменности волеизъявления гражданина, за счет бесплатности использования гражданами. В данном случае бесплатность выгодно отличает этот инструмент от использования усиленных квалифицированных электронных подписей, которые в настоящее время выдаются коммерческими аккредитованными удостоверяющими центрами на возмездной основе. Получение УКЭП связано с финансовыми издержками со стороны гражданина», — пояснили представители ведомства.



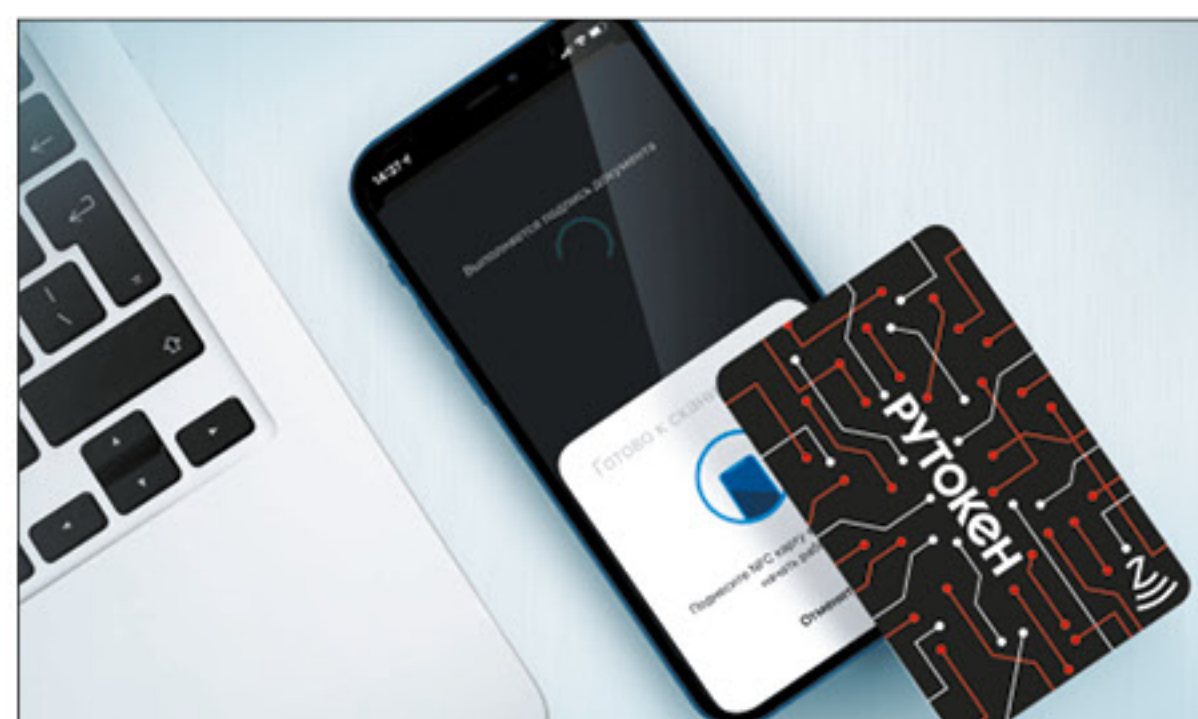
РУТОКЕН ЭЦП 3.0: НИ ШАНСА НА ОБМАН

Компания «Актив» объявила о запуске новой линейки продуктов Рутокен ЭЦП 3.0. В её состав вошли кроссплатформенные токены и смарт-карты с дуальным интерфейсом для двухфакторной аутентификации и электронной подписи на базе технологий NFC и Bluetooth LE.

Новые продукты Рутокен для криптографической защиты адресованы пользователям, ориентированным на значительную мобильность и одновременно предъявляющим высокие требования к защите данных и операций в рабочих процессах, в том числе в условиях удаленного офиса.

В состав линейки вошли принципиально новые токены и смарт-карты, предназначенные для электронной подписи, защищенного электронного документооборота и двухфакторной аутентификации на ПК с ОС Windows, macOS, Linux и мобильных устройствах с iOS, Android, Аврора. Линейка

также включает семейство продуктов Рутокен ЭЦП 3.0 Flash, которые позволяют создавать безопасные удаленные рабочие места и использовать аппаратное шифрование для усиленной защиты чувствительных данных. Токены и смарт-карты Рутокен ЭЦП 3.0 гармонично дополнили считыватели смарт-карт Рутокен SCR 3101 для контактного и бесконтактного взаимодействия, а также виртуальный считыватель VCR 3001 NFC, позволяющий подписывать документы электронной подписью на iPad с помощью токена или смарт-карты.



ВАКЦИНАЦИЯ КАК АВТОРИЗАЦИЯ

Минтранс потребовал от российских авиаперевозчиков реализовать авторизацию пассажиров по сертификату о вакцинации от SARS-CoV-2. Соответствующее поручение дала вице-премьер Татьяна Голикова.

Опция должна предлагаться при продаже билетов на сайтах авиакомпаний. Данные о вакцинации при таком типе авторизации, по плану, будут предоставляться порталом госуслуг. Позже норму могут распространить и на другие виды транспорта.

Пока вопрос использования сертификата о наличии «антиковидной» прививки при приобретении билета обсуждается. К вопросу также подключилось Минцифры.



ИИ И ГОСДАННЫЕ ПОДРУЖАТСЯ

Минцифры представило рабочей группе «Цифровая экономика» проект концепции, предполагающей платный доступ к госданным для разработчиков ИИ-решений.

Предоставлять доступ к государственным big data, по плану, будет специализированная госорганизация. Она станет формировать наборы данных на основании запросов разработчиков.

Помимо прочего госоператор будет отвечать за инфраструктуру доступа к данным и за то, какую информацию можно предоставлять тому или иному заказчику. Данные с определённой степенью секретности получают организации, аккредитованные профильными ведомствами, например, ФСБ.

Для коммерческих пользователей услуги этого оператора будут платными. Стоимость будет выводиться, исходя из сложности и объёма, а доступ к наборам данных с общедоступной информацией будет безвозмездным.

ЗАКОН О «ПОЛУ-МИЛЛИОНИКАХ»

Владимир Путин подписал закон, обязывающий иностранных ИТ-гигантов с суточной российской аудиторией более 500 тыс. пользователей открывать представительства в РФ. Под него подпадают Facebook, Instagram, TikTok, Twitter, WhatsApp, Telegram, Gmail и Wikipedia.

Согласно документу, зарубежные ресурсы будут должны: создать в России филиал, представительство или уполномоченное юрлицо; зарегистрировать личный кабинет на сайте Роскомнадзора; разместить у себя электронную форму для обратной связи с российскими гражданами или организациями. В случае нарушения доступ к ресурсу будет частично ограничен или полностью заблокирован.



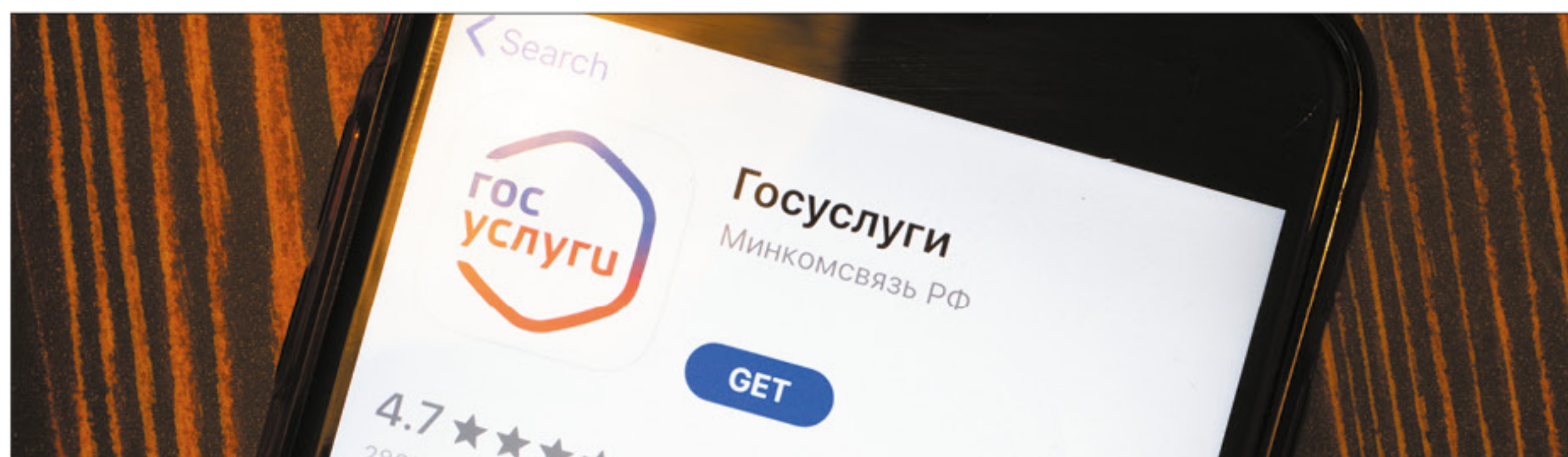
ЭП — НЕ ИГРУШКА!

МВД РФ предложило ввести уголовную ответственность за преступления с электронной подписью. По данным правоохранителей, стабильно высокий показатель ИТ-преступлений связан с повышением популярности ЭП как технологии.

Ведомство разработало законопроект, ужесточающий все виды наказания за мошеннические действия с ЭП. Согласно документу, преступникам грозит штраф 100–300 тыс. рублей или лишение свободы на срок до трёх лет за неправомерное владение ключом ЭП или сертификатом ключа её проверки.

Наказание может быть применено и к сотрудникам удостоверяющих центров, умышленно не проверившим подлинность документов для выдачи ЭП. За это полагается штраф до 300 тыс. рублей или лишение свободы на срок от трёх до четырёх лет.

Также силовики считают, что необходимо ужесточить ответственность и за деяния, связанные с нарушением коммерческой, налоговой и банковской тайны.



ЛЕТНИЕ ИНИЦИАТИВЫ МИНЦИФРЫ

Минцифры предлагает упростить подтверждение учётной записи на портале госуслуг с использованием новых технологий взаимодействия между ответственными госорганами.

Изменения подготовлены в нормативные правовые акты правительства в части совершенствования процедуры регистрации в федеральной государственной информационной системе ЕСИА.

«Для регистрации на портале госуслуг гражданам не потребуется запоминать свой СНИЛС или ИНН: запрос этих сведений будет осуществляться автоматически из информационных систем ПФР и ФНС России

на основании уже указанных гражданином данных», — отметили в ведомстве.

Для иностранцев же предложено предусмотреть «проактивную» проверку сведений о документе, удостоверяющем личность — путём их верификации данных сразу после пересечения российской границы. Это предоставит им доступ к важным гос-сервисам ещё до оформления СНИЛС и подтверждения аккаунта.

Также обозначена возможность получения простой ЭП, которая используется для предоставления госуслуг, аккредитованными филиалами и представительствами иностранных юрлиц.

РОСФИНМОНИТОРИНГ ВЗЯЛСЯ ЗА ПЕРЕВОДЫ

Переводы из ряда стран в РФ могут попасть под контроль Росфинмониторинга. Парламентарии предлагают внести соответствующие изменения в закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

Согласно инициативе, контролироваться будут переводы из определённых стран физ- и юрлицам (за исключением кредитной организации), а также иностранным организациям без образования юрлица.

В ведении Росфинмониторинга перевод окажется, если он «поступает от плательщика и (или) обслуживающего плательщика банка с территории иностранного государства или административно-территориальной единицы иностранного государства, обладающей самостоятельной правоспособностью».

Список стран должен утвердить уполномоченный орган. Вероятно, это станет информацией ограниченного доступа, которая будет доводиться до кредитных организаций в порядке, определённом Росфинмониторингом по согласованию с Банком России.



СБЕР ПОЛУЧИЛ НАГРАДЫ

Сбер получил престижную международную премию в сфере кибербезопасности Global Infosec Awards.

Наград удостоены сразу три продукта Сбера.

Киберметодология — в номинации Compliance. Разработка позволяет в автоматическом режиме контролировать соответствие двух млн элементов инфраструктуры банка более полутора тысячам требований российских и международных регуляторов в области кибербезопасности.



Антифрод-система — в номинации Fraud Prevention. Антифрод-система выявляет 99% попыток мошенничества, обеспечивая защиту 100 млн клиентов. Система включает в себя модели проверки операций в режиме реального времени, интерфейс для анализа графовых связей, инструментарий аналитики.

Сервисы безопасности в СберБанк Онлайн — в номинации Security Project of the Year. Вооружить клиента инструментами и знаниями для защиты от мошенников необходимо в той же среде, где он проводит свои финансовые операции, — в мобильном банке. С этой целью в приложении СберБанк Онлайн существует ряд сервисов кибербезопасности, направленных на обучение клиентов, гибкое управление настройками безопасности финансовых инструментов и возможность взаимодействия с банком по вопросам кибермошенничества. 25 млн клиентов СберБанка пользуются этими сервисами.

ПРОТИВ ПОДМЕНЫ НОМЕРА

В штаб-квартире Сбера состоялось выездное заседание Межфракционной рабочей группы Госдумы РФ.

Участники обсудили законопроект, направленный на запрет звонков с подменой номера из-за границы и регламентирование VoIP-операторов.

Каждый день гражданам РФ поступает в среднем 100 тысяч звонков от мошенников. Причины, по мнению специалистов, заключаются в доступности и анонимности услуг для злоумышленников, нахождении VoIP за рамками правил пропуска трафика, недостаточном регулировании отрасли, нечеткой формулировке федерального закона «О связи», отсутствии у операторов связи технической возможности проверить подмену номера и др.

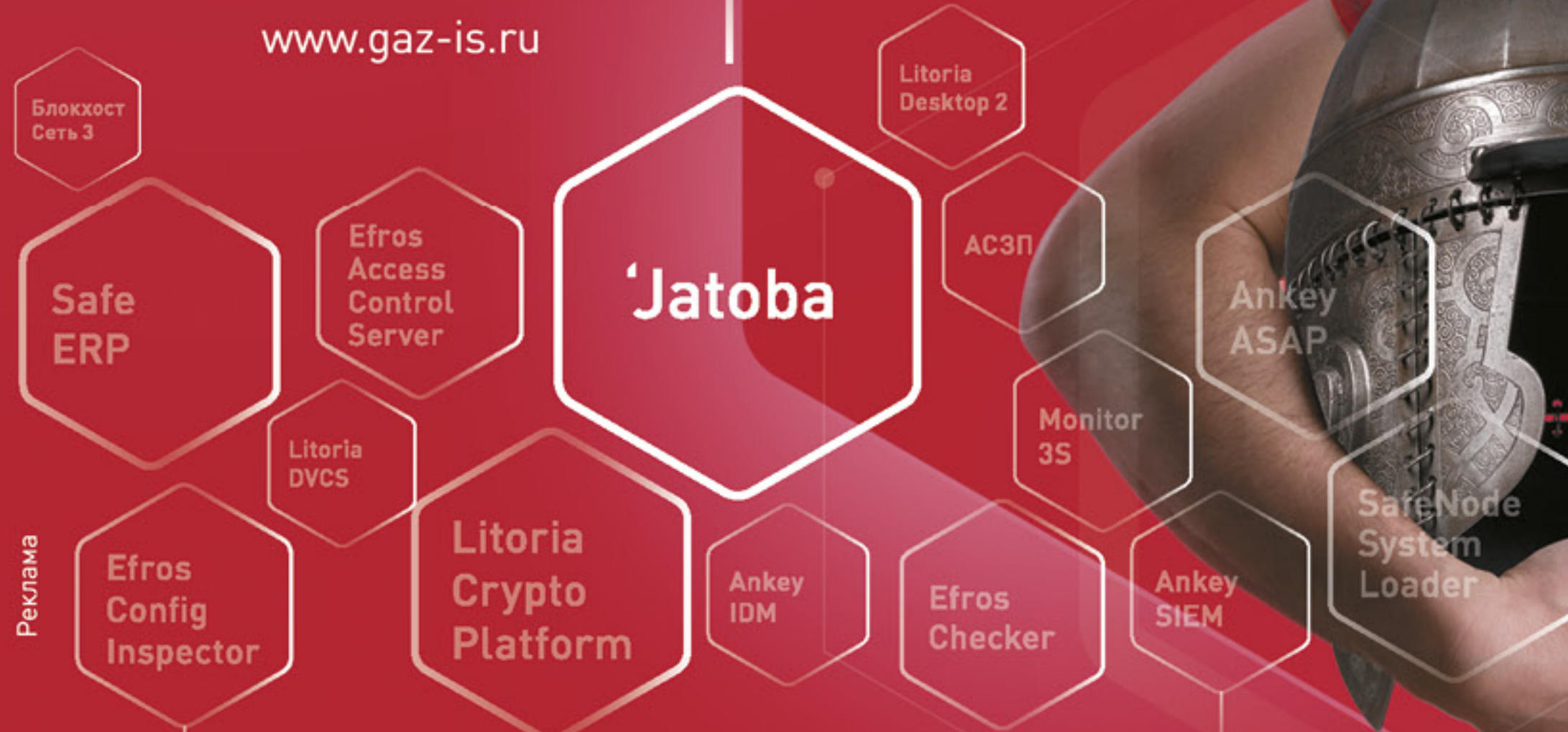
Депутаты и руководители Сбера рассмотрели инициативы регулятора (Минцифры), определили первоочередные меры и внесли свои предложения.

Надежная система управления базами данных

Jatoba

- быстродействие
- отказоустойчивость
- круглосуточная техподдержка
- оперативный выезд специалиста
- представительства в 10 регионах России

www.gaz-is.ru



18+

GIS
ГАЗИНФОРМ
СЕРВИС

КИБЕРДЮЖИНА ЦЕНТРОБАНКА

Банк России составил список из двенадцати банков для тестирования новой формы рубля. Разработку платформы должны завершить в этом декабре, а старт тестирования системы намечен на начало следующего года.

В перечень вошли «Сбер», ВТБ, «Альфа-банк», «Газпромбанк», «Тинькофф», «Промсвязьбанк», «Росбанк», «Ак Барс Банк», «Дом.РФ», «СКБ-банк», «Союз» и «ТКБ банк».

Сначала регулятор протестирует эмиссию кибер-рубля и другие операции, а после — увеличит число участников пилота. По результатам теста будет составлена дорожная карта для внедрения системы. Зампред Банка России Ольга Скоробогатова напомнила, что цифровой рубль отличается от безналичных платежей тем, что клиенты получают одинаковые условия и тарифы на совершение операций по всей стране вне зависимости от кредитной организации.

ГАЗПРОМБАНК ПЕРЕШЕЛ НА МАСТЕРЧЕЙН

В рамках проекта по цифровизации ипотечных сделок Газпромбанк переводит выпуск закладных на блокчейн-платформу Мастерчейн, разработанную Ассоциацией ФинТех.

Использование Мастерчейн позволит отказаться от бумажного документооборота и выпускать закладные в электронном виде. В результате время на выдачу закладной по ипотеке сократится с 9 дней до одного.

Переход на электронные закладные — один из этапов, необходимых для перехода к оформлению ипотеки в полностью цифровом формате. На сегодня к сервису для выпуска электронных закладных на Мастерчейн подключены полтора десятка игроков рынка. Мастерчейн позволяет обеспечить высокую безопасность учета закладных. Платформа прошла сертификацию на применение российских средств криптографической защиты.

«МИР» ВЫХОДИТ НА ANDROID

Подключение карт «Мир» к сервису Google Pay позволит привязать их к гаджетам на Android, что, в свою очередь, даст возможность бесконтактно оплачивать покупки. Новость коснется и российских, и зарубежных банков-эмитентов национальных карт.

Техническую готовность сервиса для банков пропишут на уровне документации в осеннем релизе, после чего те смогут заняться реализацией этой связки. Сроки внедрения — индивидуальные.

Промсвязьбанк, Почта-банк, Росбанк, ВТБ и «Дом.РФ» планируют

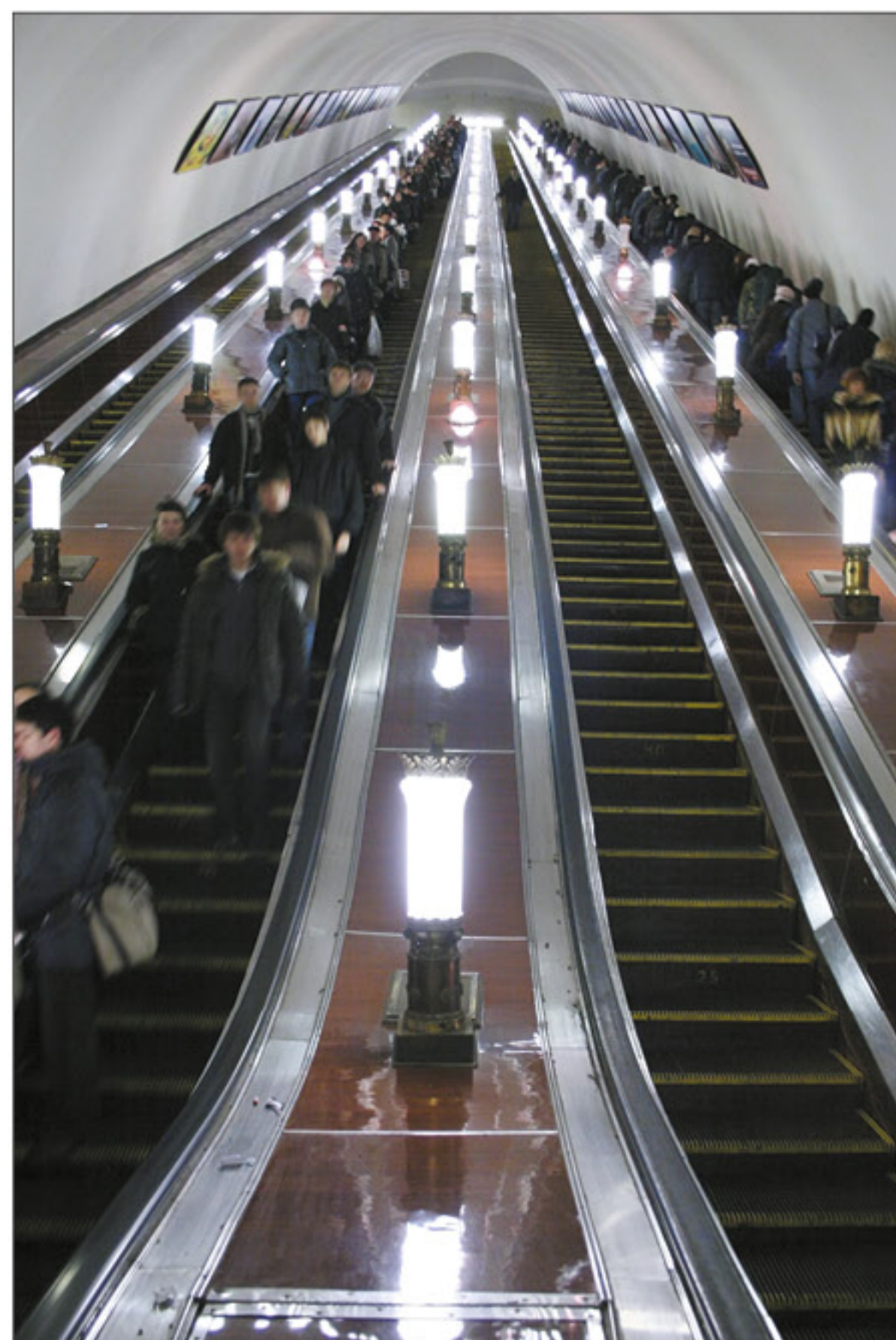
первыми предоставить клиентам эту возможность. МКБ и Россельхозбанк намерены подружить «Мир» и Google Pay до конца года, а «Ренессанс Кредит» — в 2022 году. Допускают такой союз Ак Барс банк, Газпромбанк и УБРиР, но сроки ими не называются.

Сейчас оплата «Миром» при помощи смартфона возможна через Mir Pay и Samsung Pay. В апреле банкам разрешили подключить их и к Apple Pay, но пока ни одна кредитная организация этой возможностью не заинтересовалась.



ВТБ, FACE PAY, МЕТРО

Уже осенью в столичную подземку можно будет пройти по лицевой биометрии, заявил председатель правления ВТБ Андрей Костин на Moscow Urban Forum 2021.



«Разрабатываем оплату проезда по биометрии лица. Этот сервис сократит время оплаты проезда и в час пик значительно разгрузит входную группу в метро, что сделает проезд комфортным и безопасным. Планируем запуск лицевой биометрии в московском метро осенью этого года», — сказал он.

По словам Костина, аналогичные проекты запущены в Китае и Южной Корее, однако кейс ВТБ с полным охватом всех станций метро будет первым в мире.

Развитие и масштабирование технологии Face Pay в метрополитене базируются на платформе транспортного процессинга, которая включает собственные разработки ВТБ. Она построена с применением компонентов российского ПО и софта с открытым исходным кодом.

В последствии технология Face Pay имеет шансы стать основным платёжным инструментом на других объектах городской инфраструктуры: театры, музеи, выставки и другие места массового скопления людей.



СРОК НЕМАЛЫЙ — 15 ЛЕТ!

Присяжные заседатели в суде штата Коннектикут признали гражданина РФ Олега Кошкина виновным в управлении криптографическим сервисом.

По версии обвинения, с 2013 по 2017 год фигурант, проживавший тогда в Эстонии, занимался с двумя подельниками разработкой зловредного Сруфт4U. «Сруфт4U — это сервис, который шифрует вредоносное ПО, чтобы избежать обнаружения антивирусами, популярными среди американских пользователей. Целью обвиняемых и их сообщников было позволить распространителям и кодировщикам

вредоносного ПО снизить шансы, что их вредоносное ПО будет обнаружено антивирусами на атакуемых компьютерах».

Также было заявлено, что Кошкин сотрудничал с Петром Левашовым — оператором крупного ботнета Kelihos: «К тому моменту, когда сеть была закрыта ФБР, Kelihos насчитывал по меньшей мере 50 тыс. заражённых компьютеров по всему миру».

Левашов уже признал вину — приговор будет вынесен 20 июля. Приговор Кошкину должен быть оглашён 20 сентября. Ему грозит до 15 лет тюрьмы.

СЛЕДСТВИЕ ВЕДЁТСЯ...

Следком завёл уголовное дело в отношении айтишника Павла Ситникова по подозрению в утечке данных коронавирусных больных в Москве.

Известно, что Ситников опубликовал в своём Telegram-канале файл с персональными данными 300 тыс. москвичей, переболевших COVID-19. Ему предъявлено обвинение по статье 273, ч. 2 «Создание, использование и распространение вредоносных компьютерных программ». Фигуранту грозит до пяти лет тюрьмы.

По данным следствия, обвиняемый создал вредонос, с помощью которого похитил информацию из столичного департамента информационных технологий (ранее глава департамента Э. Лысенко признавал, что утечка произошла по вине сотрудников).

Техника Ситникова была изъята, сам он помещён под домашний арест. Однако айтишник и его близкие считают дело сфабрикованным — они предполагают, что таким образом чиновников хотят избавить от ответственности за халатность.



МИЛЛИОНЕР «ПОНЕВОЛЕ»

Советский районный суд Тулы признал местного жителя виновным в особо крупной краже. Фигурант воспользовался ошибкой в банковском мобильном приложении и перевёл на свой счёт более девяноста пяти миллионов рублей.

В прошлом году мужчина заметил ошибку при обновлении приложения и вывел деньги со счёта через букмекерские конторы, после чего позвонил в банк. Там подтвердили, что клиент может распоряжаться средствами.

Средствами «миллионер» распорядился около двух месяцев — успел совершить двести двадцать операций. На суде обвиняемый свою вину не признал, что, однако, не освободило его от возмещения банку ущерба в 40 млн рублей.

В результате суд приговорил «миллионера» к шести годам лишения свободы. По статье об отмывании денег он был оправдан.

ДЖЕК-ПОТ НА СКАМЕРЕ

В прошлом году скамеры поставили рекорд — похитили у одной жертвы 400 млн рублей, рассказал начальник управления противодействия кибермошенничеству «Сбера» Сергей Велигодский.

Злоумышленники позвонили 54-летней женщине и представились сотрудниками службы безопасности банка. Они сообщили, что кто-то пытается провести «несанкционированную операцию» с её счётом и убедили, что денежные средства нужно срочно «спасти».

Жертва в свою очередь рассказала им, что у неё на счету было 14 млн рублей, на что скамеры ответили: «Отлично. Берём, снимаем и несём». После этого женщина призналась, что у неё имеется ещё 380 млн рублей в другом банке. Преступники заверили, что спасти необходимо и эти средства тоже.

«И вот она в течение месяца снимала эти деньги и отправляла их «спасателям», — заключил Велигодский.



МЕЖДУ ЭНТУЗИАЗМОМ БИЗНЕСА И ФОБИЯМИ ОБЫВАТЕЛЕЙ



**Елена
ПОКАТАЕВА**
специальный
корреспондент
BIS Journal

КАК «ЦИФРА» МЕНЯЕТ ПРЕДСТАВЛЕНИЯ ЛЮДЕЙ О ПРИВАТНОСТИ И ПРАВОВУЮ БАЗУ ГОСУДАРСТВА

Цифровизация продолжает менять наш привычный мир. Сегодня одновременно действуют несколько разнонаправленных тенденций:

- ◆ Государство стремится повысить за счёт цифровизации управляемость страной, сделав одновременно жизнь населения удобнее и безопаснее. Для этого оно собирает данные обо всех и каждом, агрегирует их и применяет в управленческих решениях на всех уровнях власти: от муниципальной до федеральной.

- ◆ Граждане, с одной стороны, с удовольствием пользуются благами цифровой цивилизации: совершают покупки и оплачивают услуги ЖКХ онлайн, покупают билеты на интернет-сайтах, частенько заглядывают на сайт госуслуг. С другой стороны, беспокоятся о том, в чьи руки попадают их паспортные данные, снимки с уличных видеокамер и параметры банковских карт.

- ◆ Бизнес стремится собирать детальные сведения о людях, чтобы лучше знать своих клиентов и предлагать им персонализированные услуги.

- ◆ Персональные данные утекают через бреши в системе защиты клиентских баз данных прямоком в теневой Интернет. Одним из драйверов роста DarkNet являются именно личные данные граждан.

Эти тенденции переплетаются, подпитывая друг друга, а развитие технологий больших данных только подстегивает процесс. Так, государство собирает и консолидирует данные

разных ведомств, составляя из них цифровые профили граждан. Бизнес использует в своих целях не только сведения о клиентах, полученные собственноручно, но и те, что собирает государство и разные коммерческие организации. Формируется легальный рынок больших данных, а параллельно живёт своей жизнью нелегальный: мошенники, комбинируя украденную и открытую информацию, плодят фальшивых цифровых двойников.

Какие тренды усиливают сегодня вышеуказанные тенденции? Каким образом они меняют риски безопасности персональных данных?

ПРЕСТУПНОСТЬ НАГУЛИВАЕТ ЖИРОК

Статистика МВД свидетельствует, что за пандемийный 2020 год количество киберпреступлений в России выросло на 73,4%. По данным ОНФ, за этот год мошенники похитили 2,8 млрд руб., что на 70% больше, чем годом ранее. Подобная цифра и в отчёте Банка России: хищения через системы ДБО выросли в 2020 г. на 70,1% по сравнению с 2019 г. А доля социальной инженерии в общем числе операций в данном случае составила около 80%.

«Поскольку ИТ-инфраструктуры компаний, особенно крупных, более или менее защищены, основной удар пришёлся на слабое звено — их сотрудников и мелких контрагентов: число разнородных фишинговых атак выросло в разы. Поддельные сайты, рассылки и подставные телефонные звонки стали очень правдоподобно имитировать официальные источники, из-за

чего на удочку мошенников попало рекордное количество человек. Получила развитие и технология подделки голоса и видео — deepfake», — рассказал С. Шерстобитов, гендиректор ГК Angara в интервью CNews.

По данным аналитиков Group-IB, продажи доступов в скомпрометированные сети компаний выросли в этот период в 4 раза — до 6,2 млн долл., а объём рынка продаж краденых данных банковских карт вырос на 116% и приблизился к 2 млрд долл. Высокие темпы роста характерны как для текстовых данных (номер, дата истечения, имя держателя, адрес, CVV), так и для дампов (содержимое магнитных полос карт). Количество предлагаемых к продаже текстовых данных выросло на 133% — до 28,3 млн карт, а дампов — на 55% (до 63,7 млн). При этом, по данным Банка России, лидируют по количеству мошеннических операций CNP-транзакции (покупки через Интернет без физического предъявления карты), из них 61,5% являются результатом применения социальной инженерии.

В компании Positive Technologies отмечают, что популярным товаром в DarkNet стали скан-копии личных и конфиденциальных документов: паспорта, водительские удостоверения, ИНН, СНИЛС и т.п., а также финансовые документы, в том числе отчёты о кредитной истории граждан и скан-копии внутренних документов коммерческих компаний (рис. 1).

Паспортные данные злоумышленники используют для регистрации в различных интернет-сервисах. Например, чтобы переводить денежные средства другим пользователям в системе «Яндекс.Деньги», злоумышленнику достаточно иметь реальные паспортные данные любого человека, а остальную информацию

он сможет получить из открытых источников (социальных сетей, ресурсов государственных органов). Такой кошелек не связан с личностью злоумышленника, что развязывает ему руки.

По оценкам Андрея Некрасова, начальника Главного организационно-аналитического управления Генпрокуратуры РФ, ещё пять лет назад доля компьютерных преступлений в общем объёме составляла менее 2%, а в 2020 г. она достигла 25%. Раскрываемость же таких преступлений составила лишь 20%.

Одна из причин такого положения дел — непрозрачная структура Интернета. Аналитики Positive Technologies утверждают, что только 4% страниц в Сети сегодня проиндексировано поисковыми системами. За пределами их возможностей остается так называемый глубокий Интернет (Deep Web), состоящий из частных форумов, закрытых баз данных (медицинские, исследовательские, финансовые) и т.п., и главное — DarkNet.

Эксперты предсказывают, что быстрорастущий «чёрный рынок» персональных данных будет активно расти и дальше. По оценкам учёных Р. Алигулиева и Р. Махмудова из Национальной академии наук Азербайджана, приведённых в их исследовании «Особенности «чёрного рынка» персональных данных и создаваемые им проблемы» (журнал «Информационное общество», № 1/2021), самый крупный «чёрный рынок» персональных данных в мире находится в США — он занимает около 60% мирового рынка и составляет 15,2 млрд долл. Вторым по величине является китайский рынок ПД — 2,4 млрд долл. Следующие — Великобритания, Канада и Франция соответственно.

Питательной почвой для роста этого рынка являются утечки данных, как внешние, так и внутренние. Сложность борьбы с ними заключается в том, что, **во-первых**, источников утечек — великое множество: личные данные могут быть украдены не только из базы данных кредитной организации, но и из торговых или обслуживающих предприятий.

Во-вторых, компании непросто определить, действительно ли доступ к клиентским данным необходим тому или иному сотруднику по работе или его поведение следует считать подозрительным и пресекать?

В-третьих, ситуация с утечками в нынешнем виде сложилась благодаря пробелам в законодательстве. По оценке Р. Алигулиева и Р. Махмудова, до сих пор законодательство ни одной страны не признаёт какую-либо информацию, в том числе и персональные данные, предметом продажи.



Рисунок 1. Типы продаваемых в DarkNet конфиденциальных документов.
Источник: «Рынок преступных киберуслуг 2018», Positive Technologies

На данный момент только закон «О защите персональных данных потребителей», принятый штатом Калифорния в США (вступил в силу 1 января 2020 г.), предусматривает куплю-продажу персональных данных. Согласно этому закону, продажа персональных данных — это предоставление компанией ПД потребителя в коммерческих целях третьей стороне в устной, письменной, электронной или других формах за плату. В данном случае речь идёт о продаже персональных данных, собранных компанией от потребителей, которых она обслуживает, третьему лицу, желающему использовать эту информацию в коммерческих целях. То есть этот закон не регулирует прямые отношения между владельцами персональных данных и их получателями. Эксперты прогнозируют, что такой правовой механизм в будущем будет применяться на всей территории США, а также в других странах.

Термин «кража персональных данных» как юридическое понятие в настоящее время отражён только в законодательстве США и Великобритании. В законодательствах многих стран такие действия описываются через другие понятия, например «нарушение неприкосновенности личной жизни», «несанкционированный доступ к компьютерной информации» и т.д. В результате, несмотря на то что технологии больших данных сегодня относятся к числу ключевых технологических и экономических тенденций в мире, законодательные конструкции в этой области ещё только предстоит создать.

Законодатели пытаются приспособить к новым условиям старую законодательную базу. Так, 11 июня Владимир Путин подписал закон, который вводит новые штрафы за разглашение информации ограниченного доступа (до 10 тыс. руб. для граждан и до 50 тыс. руб. для должностных лиц) — на порядок больше, чем раньше. Под это зонтичное понятие попадает множество различных типов данных, например коммерческая

или банковская тайна, тайна усыновления, адвокатская тайна, тайна связи и т.п. Также ужесточена уголовная ответственность за незаконное распространение и использование информации, составляющей коммерческую, налоговую и банковскую тайну, а также за разглашение информации для должностных лиц, которые по служебной необходимости имеют доступ к сведениям о мерах безопасности, применяемых к сотрудникам правоохранительных органов.

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ В ГОССТРУКТУРАХ

В госсекторе РФ сейчас популярна идея клиентоориентированности. Речь о том, что вложения в цифровизацию российского госсектора помогли в результате создать инфраструктурный базис. Настало время цифровых сервисов для клиентов государства: граждан и бизнеса. При этом соответствующие государственные информационные системы (ГИС) создаются как многоуровневые конструкции, в рамках которых данные граждан собираются на нижнем уровне, затем консолидируются и обрабатываются на следующих уровнях: региональном, ведомственном, федеральном. Собственно, создание таких информационных конструкций и составляет суть цифровой трансформации, происходящей в госструктурах.

Например, в рамках создаваемой ГИС Минздрава вся система здравоохранения превращается в единый цифровой контур. В нём выделяется федеральный и региональный уровень, а также уровень ВИМИС (вертикально-интегрированные МИС) по каждому профилю заболеваний (рис. 2, 3). Это более глубокий уровень цифровизации, чем, например, внедрение медкарты пациента.

На 2021 г. запланирована реализация регионального уровня единого цифрового контура здравоохранения, а также новых сегментов вертикально-интегрированных медицинских



Рисунки 2, 3. В рамках создаваемой ГИС Минздрава вся система здравоохранения превращается в единый цифровой контур. В нём выделяется федеральный и региональный уровни

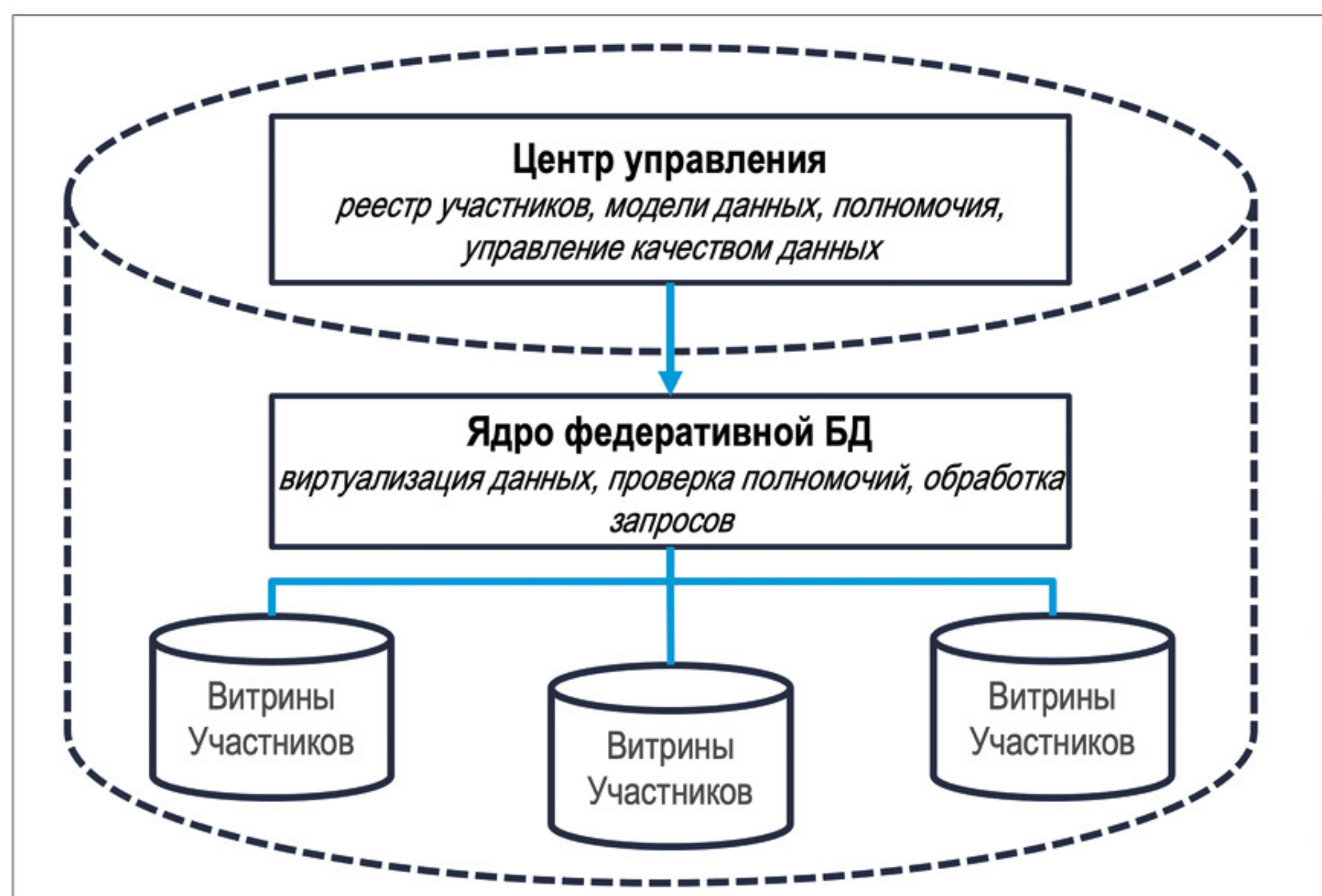


Рисунок 4. СМЭВ 4 как федеративная база госданных. Источник: Минцифры, май, 2021 г.



Рисунок 5. Архитектура НСУД. Источник: Минцифры, апрель 2021 г.

систем — по сердечно-сосудистым заболеваниям, направлениям акушерства, гинекологии и неонатологии и профилактической медицины. Иными словами, речь идёт об увеличении доли услуг, которые человек может получить удалённо, не посещая медицинское учреждение.

Похожие процессы идут в сфере образования: создаётся единая цифровая образовательная среда (ЦОС). Её идея, по словам чиновников, в усилении возможностей классической очной школы за счёт электронных образовательных ресурсов. Эти ресурсы предоставят школьнику сервисы, реализованные на современных образовательных платформах. Другой тип сервисов направлен на организацию образовательных процессов: оценка успеваемости, цифровые дневники, родительские собрания, биография ребёнка и т.д.

Минспорта РФ также занято созданием ГИС. По словам замминистра А. Сельского, эта ГИС не стремится подменить собой всю отраслевую информатизацию. Её предназначение — выполнять функции проводника для сквозных отраслевых сервисов и агрегатора/поставщика данных для других информационных систем отрасли и региональных систем.

На федеральном уровне все данные из разных ГИС консолидируются в виде НСУД (Национальная система управления данными), которая создается как федеративная база данных. А между разными структурами данные передаются с помощью новой версии системы межведомственных электронных взаимодействий СМЭВ 4. Главное отличие новой версии СМЭВ от предыдущих заключается в том, что данные становятся доступны не только в режиме межведомственных запросов со сроком обработки 5 дней, но и в формате витрин данных, например ведомственных витрин (рис. 4).

По сути, НСУД — это единая платформа управления большими госданными, которая содержит, в частности, описания моделей данных. С точки зрения фронтальной системы, например портала госуслуг или коммерческих front-систем, получение данных из единой федеративной государственной базы данных будет подобно обычному обращению к обычной СУБД. При этом потребители запрашивают данные в терминах единой модели, а поставщики данных (ведомства) управляют своими данными самостоятельно (рис. 5).

В период 2021–2023 гг. запланировано создание 41 витрины ФОИВ, включающих свыше 300 видов сведений. Пилотные проекты витрин уже идут в ФНС (ФИАС, ЕГРЮЛ, ЕГРИП), ГУОБДД МВД России (реестр транспортных средств), ПФР (база учёта пенсионных прав граждан), Росреестр (сведения из ЕГРН). Подключение Роскомнадзора, кстати, запланировано на 2023 г.

Вопрос использования госданных различными государственными системами для анализа решается за счёт создания озера деперсонализированных данных, оформленных в виде тематических наборов данных. К настоящему времени в НСУД описано 250 наборов данных. «Созданных наборов уже достаточно, чтобы понимать текущую ситуацию на разных рынках внутри страны», — подчёркивает Олег Качанов, замминистра цифрового развития, связи и массовых коммуникаций РФ.

Следующий шаг — доступность наборов данных НСУД для внешних пользователей. К ним Минцифры относит разработчиков систем

искусственного интеллекта (в целях обучения своих ИТ-систем на обезличенных наборах реальных данных) и иных бизнес-пользователей. Предполагается, что в течение 2021–2022 гг. будет создано 25 паспортов наборов данных для ИИ, и уже в сентябре начнётся их размещение в НСУД, как в формате аналитического хранилища, так и в формате витрин данных.

Минцифры заявляет, что платформа НСУД должна заработать до конца года.

Таким образом, сегодня выделяется три уровня доступности госданных для внешних потребителей:

- ◆ данные госуправления, доступные только ФОИВ;
- ◆ данные госуправления, доступные для исследовательских задач;
- ◆ данные госуправления, доступные для бизнеса и граждан.

Для поддержки этого направления предусмотрен ряд законодательных инициатив, направленных на внесение поправок в 152-ФЗ «О персональных данных». Так, законопроект № 992331–7 предусматривает обезличивание персональных данных без согласия субъекта при условии, что обезличенные данные получены на законных основаниях. «Это ключевое изменение, согласованное с регулятором в сфере информационной безопасности», — отмечает Олег Качанов, замминистра цифрового развития, связи и массовых коммуникаций РФ. Кроме того, не допускается создание условий для деобезличивания

ранее обезличенных ПД. А также в ряде случаев, строго определяемых Правительством РФ, бизнес должен безвозмездно предоставлять в определённые Правительством госорганы обезличенные ПД, которые могут быть использованы для госуправления, а также для развития решений ИИ в госсекторе.

БД СПЛОТИЛИ ГОСУДАРСТВО И БИЗНЕС

По мнению А. Серебряниковой, президента Ассоциации больших данных, в области совместного использования больших данных у бизнеса и государства сложилось полное взаимопонимание, достичь которого обычно не просто. Так она характеризует появление законодательства об экспериментальных правовых режимах (ЭПР) и регуляторных песочниц, которые предназначены для исследования механизмов бизнеса на персональных данных.

В конце января 2021 г. вступил в силу Федеральный закон № 258 «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации», за ним следует законопроект-спутник № 1129501–7 «О внесении изменений в отдельные законодательные акты РФ в связи с принятием Федерального закона № 258-ФЗ». Он призван исключить законодательные препятствия для тестирования новых технологий в рыночной среде (рис. 6).

Для экспериментов в формате регуляторных песочниц выбрано семь направлений (ЭПР):



Рисунок 6. Законопроект-спутник. Источник: Минэкономразвития России, март, 2021 г.

1. Оценка эффективности лекарств (исследование повседневной клинической практики применения лекарств у пациентов);
2. Беспилотные авто (эксплуатация высокоавтоматизированного транспорта без водителя за рулем для коммерческих такси-перевозок);
3. Телемедицина;
4. ИИ в медицине (медицинские услуги с применением инновационных технологий);
5. Дистанционное заключение договоров (применение биометрии для удалённого заключения договоров связи);
6. Беспилотные летательные аппараты (использование дронов для доставки грузов на труднодоступные территории);
7. Сервис «Моё дело» (подбор оптимальных сфер для старта предпринимательской деятельности на основе анализа больших данных).

«Это, действительно, большое достижение и серьёзная смелость со стороны государства, потому что речь идёт об установлении новых правил для проведения согласованных экспериментов, — заявила А. Серебряникова в марте на круглом столе «Перспективы развития отрасли больших данных с учетом появления экспериментально-правовых режимов». — Это очень понятно бизнесу и сложно для понимания государства. Но сложилась политическая воля, и закон был принят».

Действительно, государственная воля для поддержки экспериментов с большими данными и решениями ИИ на их базе потребовалась, ведь только в части направления здравоохранения речь идёт фактически о перезагрузке телемедицины. В марте Минздрав выдал рекомендации для онлайн-приёмов больных. Госдума работает над телемедицинским законопроектом, который позволит работникам предприятий проходить медосмотры с помощью цифровых технологий. Эксперты говорят, что государство повернулось лицом к телемедицине.

ЭПР «Моё дело» — рекомендательный сервис для предпринимателей, собирающихся начать бизнес, — будет запущен уже в этом году. Предполагается, что будет создана платформа для использования обезличенных данных операторов персональных данных. И для её поддержки понадобится ввести упрощённый порядок обработки персональных данных.

По большому счёту, бизнес заинтересован в том, чтобы добавлять в свои экосистемы государственные услуги и таким образом реализовывать бесшовный переход из экосистем коммерческих компаний в госсистемы для получения государственных услуг. Проекты ЭПР позволяют бизнесу снять нынешние регуляторные

проблемы, связанные с использованием данных из государственных систем, ресурсов и реестров, обеспечить недискриминационный доступ бизнеса к государственным данным с использованием открытых протоколов.

Д. Тер-Степанов, заместитель гендиректора АНО «Цифровая экономика», сетует, что подобная активность воспринимается российскими регуляторами как поле для рисков, и отмечает: «У нас есть три года, чтобы в ограниченных условиях изучить возможные риски, в том числе для государства. И выявить обоснованные, чтобы не допустить в дальнейшем внедрения технологий, которые могут такие риски создавать». Эта организация помогает правительству отбирать следующие ЭПР для реализации, заботясь при этом о создании конкурентной среды для бизнес-участников.

РЕГУЛИРОВАНИЕ БОЛЬШИХ ДАННЫХ В РФ

Функции регулятора персональных данных граждан в нашей стране возложены на Роскомнадзор. Он ведёт реестр операторов персональных данных — по состоянию на начало 2020 г. в нём числилось 402 642 организации, в том числе:

- ♦ государственные органы — 6829;
- ♦ муниципальные органы — 33 862;
- ♦ юридические лица — 334 110;
- ♦ физические лица (в том числе ИП) — 27 841.

При этом сведения о месте нахождения баз данных с персональными данными граждан РФ, что требуется по закону, предоставили 86,75 % операторов, внесённых в реестр.

Как отмечает А. Липов, глава Роскомнадзора, регулятору сложно справляться с растущим потоком жалоб, поступающих от граждан. Так, в 2019 г. их количество выросло на 20 % и достигло 43 тысяч (официальные итоги 2020 г. ещё не оглашены). По каждому обращению Роскомнадзор как уполномоченный орган, занимающийся защитой прав субъектов персональных данных в сети Интернет, обращается в суд с соответствующим иском заявлением. Но ещё более усложняет ситуацию, что активность регулятора оказывается не очень эффективной: компании, нарушающие закон о персональных данных, не пугают штрафы — их «потолок» составляет всего 75 тыс. руб. Кроме того, обработчики персональных данных передают сведения друг другу, а проверить всю цепочку ведомство не может.

Неслучайно несколько лет назад ведомство задумалось о внедрении практик по типу саморегулируемых организаций в сфере обработки

ПД. Кодекс добросовестных практик в сети Интернет, разработанный Роскомнадзором, стал инструментом повышения «сознательности» компаний, обрабатывающих ПД граждан. На данный момент Кодекс поддерживают более 7 тыс. операторов персональных данных по всей России.

Свой Кодекс этики использования данных разработали два года назад Ассоциация Больших данных и Институт развития Интернета (ИРИ). Он представляет собой свод отраслевых стандартов профессионального и этического поведения, которые участники признают и обязуются исполнять. Положения Кодекса распространяются на оборот всех типов данных: от пользовательских до промышленных — и содержат принципы профессиональной этики при их сборе, обработке, использовании и хранении. За 2019–2020 гг. в соответствующем реестре разместились 24 компании.

А ГДЕ ИНТЕРЕСЫ ЧЕЛОВЕКА?

Весной этого года в Совете по правам человека при Президенте РФ стартовала разработка «Цифрового кодекса». Была создана рабочая группа по защите цифровых прав граждан, в которую вошли представители ИТ-индустрии, Роскомнадзора, других профильных ведомств и эксперты. Со стороны СПЧ эту тему курирует И. Ашманов, президент ИТ-компаний «Крибрум» и «Ашманов и партнёры».

Глава СПЧ В. Фадеев считает, что российское законодательство не справляется с защитой граждан в цифровой среде. С ним согласен И. Ашманов: «Везде, где обсуждаются вопросы цифровизации, например, образовательной сферы или здравоохранения, чиновники разговаривают с бизнесом. Иногда говорят, что привлекают к своим задачам академическое сообщество. Диалога с общественностью нет». По мнению эксперта, утечки персональных данных — это не самая большая проблема, гораздо серьёзнее риск манипуляций с помощью этих данных.

Действительно, утечки данных создают основу нелегального бизнеса и приводят главным образом к финансовым потерям граждан, что теоретически поддаётся регулированию с помощью Уголовного кодекса. Манипулирование данными — это вариант «причинения добра», под который практически невозможно подвести ни УК, ни КОАП РФ. Более того, прямой ущерб для человека может не просматриваться. Он возникает персонализировано, когда конкретный человек усматривает в использовании его ПД чей-то злой умысел.

Игорь Ашманов приводит пример: в концепции цифровизации средней школы есть понятие образовательной траектории учащегося. Но что под ней скрывается: мониторинг учебного процесса ребёнка в интересах статистики или попытка влиять на его выбор предметов для усиленного изучения?

Кто-то видит злой умысел в муниципальных программах безопасных городов с множеством видеокамер на городских улицах, а кто-то — в телемедицине. Кому-то не нравится настойчивость коммерческих компаний в навязывании услуг, которая явно связана с появлением у этих компаний некоторых сведений о гражданах. А кто-то недоволен тем, что силовые структуры умеют «вычислять» участников протестных мероприятий.

Получается, что новые понятия «цифровой суверенитет человека» и «цифровой суверенитет государства» нередко вступают в противоречия? Да, это так, подтверждает председатель Конституционного суда РФ В. Зорькин в своей статье «Право в цифровом мире» («Российская газета», 29.05.2018): «Как всегда, сложным будет отыскание баланса между регулятивными и охранительными нормами. С одной стороны, государство не должно оставлять человека в сети Интернет один на один с преступными посягательствами на его права, законные интересы и имущество. Но, с другой стороны, применяемые меры (технологии) противодействия преступности не должны превращаться в чрезмерные ограничения, посягая на саму суть (основное содержание) конституционного права на информацию и находящейся под его защитой свободы поведения человека в интернете».

НОВЫЙ ОБЩЕСТВЕННЫЙ ДОГОВОР?

Похоже, что, по большому счёту, речь идёт о формировании нового общественного договора между гражданами, бизнесом и государством. Договора, призванного гармонизировать цифровые «интересы» в обществе. На каких весах нужно взвешивать «добро» от повышения безопасности для человека и «зло» от потери privacy? Можно ли обеспечить такой механизм обработки ПД на стороне госструктур и бизнеса, который сделает эту обработку прозрачной и контролируемой со стороны граждан?

Редакция BIS Journal собрала мнения российских экспертов по этому кругу вопросов.

«СИТУАЦИЯ ГОРАЗДО ПРОЩЕ, ЧЕМ ДУМАЕТСЯ»



**Надежда
ЩЕГОЛЕВА**

руководитель
Департамента
развития
технологий
больших данных
Института развития
информационного
общества, доктор
технических наук,
профессор

Выскажу не только мою личную точку зрения, но и консолидированное мнение всей дирекции развития цифровых технологий Института развития информационного общества, которую возглавляет д.ф.-м.н., проф. Александр Богданов: в фундаментальной информатике вопрос больших данных хорошо проработан, и большинство данных, которые сегодня считаются большими, таковыми не являются.

Естественно, для областей, близких к большим данным, вопрос анонимизации является ключевым, у него есть несколько решений. Но областей, где эти проблемы встают во весь рост, на самом деле не так много. И надо понимать, что если данные не являются большими (в смысле определения фундаментальной информатики), то решения для них существуют, и они хорошо разработаны.

Например, большие данные часто упоминаются, когда речь заходит о цифровом промышленном предприятии, где работают системы IoT. Но IoT в настоящее время — это технология, далёкая от больших данных (слишком слабые процессоры и малые транзакции), поэтому для неё применяются стандартные решения как для централизованных систем. При этом, конечно, имеет смысл не скупиться и поставить приличную защиту на гейт во внешний мир.

Сегодня много говорят о проблемах безопасности данных, в частности, в системах видеоаналитики, используемых в рамках проектов безопасных городов или региональных МИС в здравоохранении. На самом деле описать характер киберугроз в подобных случаях — относительно простая задача: необходимо чётко разделять типы больших данных и связанные с ними угрозы. Для централизованных систем этот вопрос решён, и надо просто применять правильные подходы. Для систем типа частных облаков существуют подходы к решению проблемы, и надо заниматься разработкой соответствующих платформ применительно к рассматриваемым задачам. Для публичных облаков общего решения даже в теории пока нет, и надо разрабатывать системы безопасности для каждого конкретного случая.

При этом надо отделять чисто технические решения от организационных сценариев работы. Например, традиционным аспектом безопасности данных, и больших данных в том числе, является незаконное проникновение в инфор-

мационные базы компаний и организаций с целью получения личных данных. На наш взгляд, при правильном подходе современные системы защиты позволяют полностью перекрыть периферию и блокировать попытки проникновения. Однако инсайдер может свести на нет все возможности такой системы. Думаю, что это задача скорее для психологов — чисто техническими средствами её не решить.

Стоит отметить, что самые продвинутые системы защиты персональных данных от утечек фактически работают по принципу «виртуализации» данных, когда все организации работают не с реальными данными клиентов, а с некоторыми их виртуальными образами. Для применения такого подхода есть только два существенных вопроса — цена и скорость обработки данных. С точки зрения самих технологий обработки — это применение статистических методов, которые себя очень хорошо зарекомендовали в политической психологии.

Однако всё существенно сложнее, если мы говорим о реальных больших данных, там пока работают только статистические методы. Они гарантируют анонимизацию, но пригодны не для всех приложений. Правда, в основных запросах, связанных с рекламой, эти методы самые эффективные.

Сегодня самые жаркие дискуссии в обществе по поводу сбора и обработки больших данных граждан идут в основном не вокруг академических подходов и определений, а вокруг эмоционально наполненных понятий типа «цифровой суверенитет человека». Полагаю, что это вопрос консенсуса между обществом и властью. Он требует обсуждения и определяется тремя факторами: адекватностью власти, информированностью населения и внешними угрозами. Причём последними ни в коем случае нельзя манипулировать. У нас пока ни власть, ни общество к такому консенсусу не готовы.

Если в целом говорить о главных направлениях развития регулирования больших данных в современном обществе, то сначала надо констатировать: по большому счёту, регулирования больших данных пока вообще нет. Для наведения порядка в этой сфере необходимо провести аудит и понять, кому, для каких целей и в каком виде такие данные нужны. И если отделить потребности от рекламы, то окажется, что ситуация гораздо проще, чем думалось, и она вполне регулируема.

«У РЫНКА БОЛЬШИХ ДАННЫХ БОЛЬШОЕ БУДУЩЕЕ»

Один из главных рисков, связанных с большими данными в государстве, — риск утечки персональных данных граждан. Хотя юридические меры защиты ПД и ответственности за их незаконное распространение прописаны достаточно подробно, организационные и технические меры, реализуемые операторами данных, зачастую недостаточны.

Центр мониторинга и реагирования на кибератаки Solar JSOC компании «Ростелеком-Солар» за январь-ноябрь 2020 г. зафиксировал больше 200 профессиональных хакерских атак на российские компании. Многие из объектов атак — это объекты критической информационной инфраструктуры (КИИ). Поэтому, на мой взгляд, главная опасность заключается в том, что из-за больших данных и Интернета вещей офлайн и онлайн срачиваются, и кибератаки могут выводить из строя объекты реального мира, обеспечивающие деятельность целых предприятий и городов.

Одной из лучших защит от кибернападений является осознание каждого сотрудника компаний, оперирующих большими данными, своей личной ответственности за их сохранность. Например, по данным Infowatch, почти 80% утечек ПД происходит из-за внутренних нарушений. Однако стремление к тотальному контролю за действиями сотрудников способно превратить их в объекты постоянной цифровой слежки.

Действительно, DLP-системы представляют достаточно эффективными инструментами контроля, но важно мотивировать работников не только слежкой и наказаниями, но и поощрениями. Чем больше у работника предпочтений и карьерных возможностей, тем меньше вероятность, что он станет передавать инсайдерскую информацию конкурентам. При этом не надо забывать, что права сотрудников также должны быть защищены, а их ПД должны находиться под защитой.

Кроме того, необходимо строго соблюдать существующие принципы обработки персональных данных, в частности, принцип целевого сбора данных (данные должны быть собраны с конкретной, чётко обозначенной целью) и принцип минимизации их сбора (данные должны быть собраны только в том объёме, который необходим для достижения целей обработки).

Цифровые предприятия сегодня объединяются в цифровые цепочки компьютерного обмена данными между поставщиками, партнёрами, ведомственными ГИС и т.д. Разумеется, консолидация инфраструктур увеличивает риск кибератак, а наличие больших данных добавляет риски, связанные с утечками. В случае данных промышленного Интернета вещей речь идёт скорее о данных, связанных с работой устройств. Но если мы говорим, например, о технологиях «умного города» и обработке данных, полученных от устройств учёта, установленных в частных домохозяйствах, то здесь вполне может возникнуть угроза для ПД.

В любом случае лучшая защита — это предупреждение возникновения атак. Разработка стратегии сбора, обработки и хранения данных с учётом обеспечения их безопасности, внедрение передовых практик, связанных с защитой данных и обеспечением конфиденциальности, постоянный пересмотр подходов к обеспечению безопасности с точки зрения появления новых угроз должны присутствовать в каждом промышленном предприятии, использующем большие данные.

Какой метод хранения данных наиболее соответствует задаче их сохранности и конфиденциальности? Полагаю, что централизованные базы данных не самое лучшее решение с точки зрения обеспечения безопасности. Сосредоточение данных в одном месте повышает риск утечек, в том числе риск перехвата данных при их передаче в централизованную базу. Кроме того, если утечка всё-таки произошла, последствия будут катастрофическими. Вспомним, например, случай с утечкой персональных данных всех пациентов с диагнозом COVID-19 (а это более 16 миллионов человек), которая произошла в конце прошлого года в Бразилии. Тогда были скомпрометированы две правительственные базы данных, которые использовались для регистрации жителей страны с соответствующими симптомами. Опасения относительно централизованных баз данных, особенно тех, что содержат биометрические данные, высказываются в Евросоюзе, Австралии, Китае, Индии. Неслучайно, например, для построения модели цифровой идентификации сегодня часто рассматриваются технологии распределённого реестра и блокчейн — такая модель предложена, например, GSMA в рамках программы M4D



Сергей ПЛУГОТАРЕНКО
директор РАЭК

(mobile for development). На базе блокчейна построена политика обработки биометрических данных Международной организации «Красный Крест», а также программа по созданию виртуальных аккаунтов для беженцев ООН в рамках проекта United Nations World Food Programme.

Сегодня также популярна идея анонимизации конкретных персональных данных. Разработано много методов обезличивания (анонимизации). В этой связи необходимо отметить, что в нашем законодательстве отсутствует разграничение между обезличенными (лишёнными связи с субъектом) и псевдонимизированными (сохраняющими связь с физическим лицом) данными. В зарубежной практике такое разграничение есть, и, как правило, обезличенные данные выводятся из-под требований законодательства по защите персональных данных.

Требования, предъявляемые к обезличиванию, различаются в отдельных юрисдикциях. Например, GDPR требует необратимости данной процедуры, то есть персональные данные не должны восстанавливаться из обезличенных никаким способом. Таким образом, например, шифрование, хеширование или токенизация не являются методами обезличивания, а относятся к методам псевдоанонимизации. К современным методам обезличивания относят такие методы, как k-анонимность, l-разнообразие или t-близость, а также наложение шума или дифференцированная конфиденциальность.

Однако общая позиция зарубежных регуляторов заключается в том, что ни один из этих методов сам по себе не может рассматриваться в качестве абсолютно надёжного. Необходимо сочетание методов в зависимости от конкретной ситуации, имеющихся данных и существующих рисков. При этом очень важно, чтобы в процессе обезличивания данные сохранили свою ценность, то есть были способны обеспечить достижение той цели, ради которой они собирались и обрабатывались.

Отмечу ещё один существенный риск для граждан — профайлинг и автоматизированное принятие решений на основании собранных данных. В настоящий момент принятие на основании исключительно автоматизированной обработки персональных данных таких решений, которые порождают существенные последствия для субъекта, запрещено. Но даже частичное делегирование процесса принятия решений алгоритмам, в том числе алгоритмам искусственного интеллекта, в таких процессах, как, например, оценка кредитоспособности, может повлечь за собой существенные риски. В числе таких рисков, которые сейчас широко обсуждаются на

международном уровне, — риски дискриминации различных социальных групп, риски принятия необъективных или ошибочных решений.

Сегодня многие страны озабочены поиском баланса между соблюдением прав субъекта и общества. В поиске баланса основой выступает риск-ориентированный подход, при котором преимущества использования того или иного технологического решения оцениваются относительно возможных рисков, связанных с его использованием. Если риски существенны, то для таких решений требуется жёсткий контроль, особое регулирование, а в отдельных случаях использование технологии может быть запрещено.

Например, в ряде штатов США запрещено массовое видеонаблюдение с использованием технологии распознавания лиц, поскольку в случае ошибки системы последствия для субъекта могут быть крайне негативными. Запрет данной технологии обсуждается и в ЕС. Совсем недавно Еврокомиссией был представлен комплекс правил регулирования систем искусственного интеллекта, который рассматривает четыре уровня рисков, связанных с использованием таких систем. Согласно этим правилам, системы четвёртого (неприемлемого) уровня риска, которые представляют угрозу безопасности гражданам и их правам, должны быть запрещены. В их число попадают, например, разработки, позволяющие манипулировать поведением пользователей.

Обычная практика контроля за принятием решений — прозрачность операций, в том числе операций с персональными данными граждан. Как это выглядит сегодня?

В соответствии с положениями 152-ФЗ, механизм обработки ПД на территории РФ предусматривает разработку политики оператора в отношении обработки персональных данных, обязательное уведомление уполномоченного органа по защите прав субъектов персональных данных (Роскомнадзор) о намерении осуществить обработку. Это уведомление содержит, в частности, информацию о целях обработки, категории персональных данных, которые планируется обрабатывать, правовое обоснование обработки и т.д. Кроме того, операторы персональных данных должны назначить отдельное лицо, ответственное за разработку. На повышение прозрачности обработки и более существенный контроль граждан за своими данными направлен также механизм получения согласия.

Вместе с тем более чёткому контролю за соблюдением законодательства в сфере ПД могло бы способствовать создание отдельного органа, отвечающего исключительно за данную



сферу (примером такого органа в ЕС является European Data Protection Board — Европейский совет по защите данных), в состав которого вошли бы представители государства, бизнеса и научного сообщества.

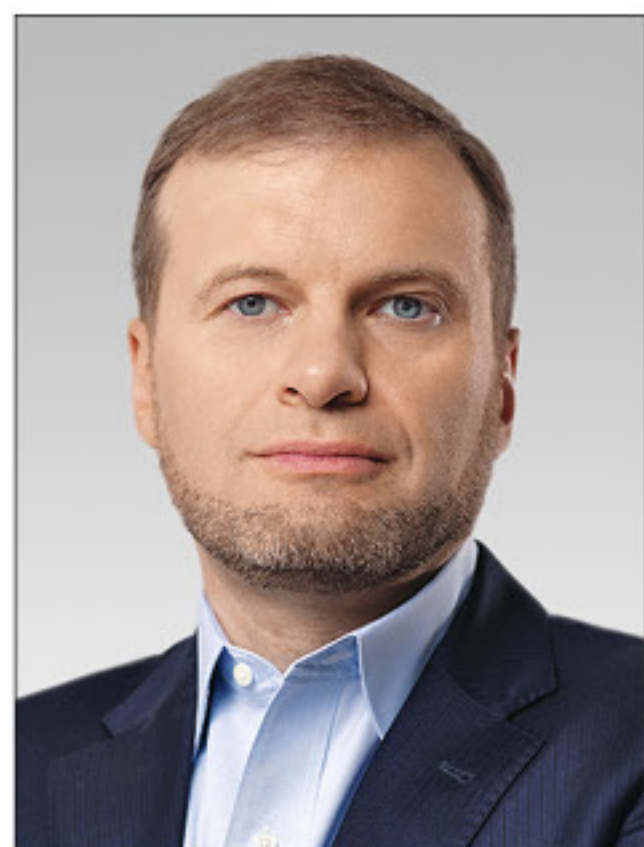
В целом на регулирование больших данных, как, впрочем, и на любое регулирование развивающейся технологии, нужно смотреть с точки зрения баланса. Необходимо, с одной стороны, обеспечить соблюдение прав владельцев данных, прежде всего пользователей, а с другой — не препятствовать, а наоборот, стимулировать развитие инноваций. В прошлом году Ассоциация больших данных выпустила исследование, согласно которому при благоприятном регулировании развитие рынка больших данных к 2024 г. должно привести к существенному экономическому эффекту — прирост составит

0,3 % ВВП, или около 3 трлн руб. В качестве направлений модернизации регулирования указываются упрощение доступа бизнеса к сбору и обработке данных, обеспечение возможности обмена данными и их обогащения, создание R&D-песочниц для исследования больших данных, финансирование инноваций и т.д.

* * *

Таким образом, модернизация должна затронуть нормативные акты, связанные с обработкой данных, в первую очередь Федеральный закон 152-ФЗ «О персональных данных». Однако при модернизации необходимо не забывать об интересах граждан. Права субъектов на безопасность и конфиденциальность должны быть, безусловно, соблюдены.

«ОТ БУМАЖНОЙ ОТЧЁТНОСТИ К ЛАТАНИЮ ДЫР, ЧЕРЕЗ КОТОРЫЕ ТЕЧЁТ»



**Алексей
РАЕВСКИЙ**
генеральный
директор компании
Zecurion

Проблема больших данных не только в том, что это данные о людях или организациях, но и в том, что на их основе можно генерировать новые данные и знания, наличие которых изначально не предполагалось. Два примера. Первый — как американская торговая сеть сделала специальное предложение старшекласснице — в виде набора для беременных. Получился скандал, руководство магазина извинялось перед родителями девочки, мол, искусственный интеллект, анализируя данные, сделал ошибку. А потом оказалось, что система всё верно спрогнозировала, только семья была не в курсе насчёт юной особы.

Другой пример — когда частная британская компания Cambridge Analytica использовала Facebook для глубоко таргетированной рекламы. Около 300 тыс. пользователей получили от Cambridge Analytica денежное вознаграждение за прохождение психологического теста. Затем компания использовала результаты этого теста вместе с лайками и личными данными этих пользователей, а также их друзей, для генерации и запуска высокоперсонализированной политической рекламы. И во многом благодаря именно ей Дональд Трамп победил на президентских выборах.

При этом данные собирались в соответствии с политикой Facebook, с помощью API Facebook, без какого-либо несанкционированного доступа или взлома. Но оказалось, что век ИИ принёс с собой новый вызов: набор данных, которые не считаются конфиденциальными, может генерировать чувствительные, а порой и вредные новые знания. И к такому не готово ни общество, ни индустрия информационной безопасности.

Ведь индустрия ИБ привыкла иметь дело с классическими угрозами, а в описанных случаях речь идёт о другом — о том, как используются большие данные.

Когда мы говорим, что интернет-поисковики собирают большие данные, чтобы показывать нам таргетированную рекламу товаров, это приемлемо и зачастую даже удобно: экономит силы, время и т.д. Настоящей проблемой это становится, когда большие данные используются для целей, идущих вразрез, скажем, с

нашими ожиданиями, общепринятой моралью и т.п. Отсюда вопрос: кто и как будет контролировать варианты и способы применения персональных данных? И этот вопрос до сих пор открыт.

Идеи, что, мол, персональные данные граждан страны должны храниться внутри этой страны, не дают ответа на поставленный вопрос. Необходимо выработать кодекс, помогающий различать, что такое хорошо и что такое плохо.

Первый шаг в этом направлении сделали наш российский закон 152-ФЗ и европейский GDPR: в них заявляется, что персональные данные должны обрабатываться только для тех целей, ради которых они собирались. Легко видеть, что в случае Cambridge Analytica это требование не соблюдалось, но Цукербергу повезло — на момент скандала сегодняшние нормы GDPR ещё не действовали. А они гораздо более жёсткие, чем российские. Так, если у нас всё сводится к «галочке» — явному разрешению самого человека передавать персональные данные третьим лицам, то в GDPR прописана концепция Data Privacy Officer. Она подразумевает, что в каждой организации должен быть менеджер, ответственный за приватность пользовательских данных.

По сути, этот человек представляет в компании интересы регулятора и несёт личную ответственность, в том числе и материальную, за нарушения в сфере персональных данных. Например, если в компании происходит утечка данных, он обязан отчитаться о случившемся перед регулятором и, возможно, после расследования, на него будет наложен штраф.

GDPR, на мой взгляд, — это самое прогрессивное регулирование. Правда, оно затрагивает только те организации, которые обрабатывают личную информацию жителей ЕС. Можно ожидать, что законодатели других стран скоро пройдут тот же путь в своём законотворчестве. Почему?

Анонимность не пройдёт — это уже понятно. Вспомните, насколько популярна во всём мире концепция Know Your Customers («Знай своего клиента»). Для российских банков, кстати, с точки зрения управления киберрисками решения KYC входят в состав обязательных. Да и другие компании постоянно проводят Due Diligence, изучая своих клиентов.

Запретить компаниям собирать и обрабатывать ПД клиентов тоже вряд ли получится. Заставить компании размещать клиентскую базу на сторонней площадке и получать к ней удалённый доступ? Тоже нет: кто откажется от хранения очень ценных данных — о клиентах — под своим контролем?

Пожалуй, более реально запретить компаниям передавать данные клиентов. Вернее, делать это не напрямую, а через доверенного посредника. Скажем, человек регистрируется на некотором ресурсе, типа портала госуслуг, и там получает идентификатор, который затем использует в различных операциях. С одной стороны, есть взаимно однозначное соответствие между идентификатором и физлицом. С другой — сторонним компаниям реальные сведения будут недоступны.

Для банковских задач класса KYC это может оказаться хорошим решением, ведь они затрачивают много сил и средств на реализацию процедур Know Your Customers. Правда, есть существенный минус: ответственность размазана. Скажем, открыли счёт новому клиенту, а позже выяснилось, что этого не стоило делать. С кого спрашивать? С сервиса обработки персональных данных? С него взятки гладки, да и сама кредитная организация, тоже вроде бы не имеет отношения к исходным клиентским данным... Кроме того, такой метод «сокрытия» данных всё равно не позволит полностью решить поставленную проблему. Ведь всё равно компании будет известен профиль клиента, и этого вполне достаточно для многих задач. Более того, на основании профиля нетрудно вычислить и недостающие данные.

Остаётся только снижать риски неправомерного использования персональных данных. С точки зрения концепции защиты ПД, это означает, что к традиционным аспектам защиты информации — конфиденциальность, целостность, доступность — нужно добавить ещё один — целеполагание. В этом случае модель защиты персональных данных будет охватывать риск злоупотребления данными, который появился благодаря развитию технологий искусственного интеллекта и обработки больших данных.

На практическом уровне появляется много вопросов, и все они весьма сложные. Поэтому движение в эту сторону будет постепенным, мелкими шажочками и, конечно, гораздо более медленным, чем скорость развития самих технологий обработки больших данных.

Пример такого актуального шажочка — история с массовыми утечками ПД из банков

Век ИИ принёс с собой новый вызов: набор данных, которые не считаются конфиденциальными, может генерировать чувствительные, а порой и вредные новые знания. И к такому не готово ни общество, ни индустрия информационной безопасности

и компаний связи. Сформировалась целая индустрия мошеннических кол-центров. Их коммерческий успех основан на халатном отношении организаций к защите своей информации. А подвигает их на такое отношение смешное наказание за нарушение закона о персональных данных: кого смотивирует штраф в 150 тыс. руб. на создание команды специалистов по защите? В англоязычных новостях то и дело выскакивают заголовки: очередной банк оштрафован за утечку персональных данных на десятки (а порой сотни) миллионов долларов. Наше непозволительно мягкое законодательство в этой области — болевая точка № 1.

Отсутствие ответственности самой организации за утечки — проблема № 2. У нас тоже бывают утечки, и большие, и даже в самых крупных банках. Однако наказание несут обычно рядовые сотрудники, и масштаб наказания — соответствующий. У банков просто нет стимулов превентивно заниматься этой задачей. И это проблема № 3. Нужно от методических рекомендаций и тесно связанной с ними «бумажной безопасности» переходить к практическому залатыванию дыр, через которые утекают данные.

По большому счёту, понятие утечек данных должно стать понятием законодательства. Согласно западному законодательству, штрафуют именно за утечки данных. Эта практика напоминает надзорную работу с экологическими нарушениями: если компания загрязнила окружающую среду, она должна заплатить штраф, а размер штрафа должен быть соразмерен и с нанесённым ущербом, и с тем, какие усилия компания предпринимала для защиты от инцидентов такого рода.

* * *

Список проблем-«шажков» можно продолжить. И вряд ли он в обозримом будущем будет исчерпан. Это новая реальность — новая промышленная революция, и в ней надо учиться жить.

«ПРЕДСТОИТ НАУЧИТЬСЯ УПРАВЛЯТЬ БД КАК ОБОЮДООСТРЫМ ОРУЖИЕМ»



Сергей НАЗАРЕНКО
руководитель
центра
компетенций Big
Data компании
«Рексофт»

Когда мы говорим об опасности утечек персональных данных людей или сведений, составляющих коммерческую тайну компании, мы имеем в виду неконтролируемый обмен данными. Например, при приобретении телефонного номера или автомобиля мы подписываем договор, где есть такой пункт: «гражданин, получивший товар или услугу, разрешает передачу информации о себе третьим лицам». Формулировка часто неконкретная. И это важный аспект безопасности: только потому, что вы поставили «галочку» в договоре, ваши данные могут стать предметом купли или продажи.

Нередко такие галочки мы ставим при регистрации на различных сайтах или для получения бесплатных услуг. Тогда «продукт» для продажи — это вы сами: ваше поведение, ваш профиль. Именно поэтому персональные данные очень острый аспект безопасности, ведь средств контроля за этим обменом, по сути, нет. Правда, сейчас люди сами открыто публикуют много разной информации о себе в соцсетях: где находятся в данный момент, с кем, что делают. Журналисты уже научились с помощью инструментов соцсетей и публично доступных данных проводить настоящие расследования. Это говорит о том, что ситуация на практике гораздо сложнее, чем может показаться на первый взгляд.

С одной стороны, персональные данные, действительно, нужно защищать. С другой стороны, те из них, которые мы легко раскрываем в соцсетях, уже не являются тайной. Поэтому сложно определить, что на самом деле означает понятие «защищаемые персональные данные». Пока что это серая зона.

Как выйти из этой «серой зоны»? Возможно, стоит приглядеться к концепции «обмен privacy на безопасность». Например, на улицах города за нами следит огромное количество видеокамер. По ним при желании можно проследить весь наш путь от двери до двери, со всеми подробностями типа скорости перемещения и остановок по дороге. Кто-то громко возмущается: «Тут нарушается право на тайну частной жизни!» Вряд ли кто-то хочет, чтобы «Большой брат» следил за ним, но можно рассмотреть сделку: что я приобретаю взамен утраты privacy? Может

быть, человек будет готов поставить видеокамеры в свой дом, если оператор гарантирует, что к нему не придёт преступник. Безопасность гораздо выше, чем потеря приватности. Но чтобы это сработало, такого типа услуга должна быть глобально доступна и однозначно принята максимальным количеством людей.

Отличный пример — работа интернет-поисковиков. Поведение пользователей — важные персональные данные. Но поисковики и рекомендательные сервисы на базе знаний о цифровом профиле предоставляют пользователям более качественную услугу. Например, если кто-то ищет белые кроссовки, с высокой степенью вероятности современный маркетплейс подкинет ему похожую модель или информацию о распродаже.

Так что вопрос, что мы приобретаем в обмен за частичную утрату privacy, — далеко не простой. Главная сложность заключается в том, чтобы не начать без оглядки регулировать доступность персональных данных, потому что тогда легко потерять уже привычное нам качество сервисов.

Возьмём в качестве примера GDPR — европейское законодательство о персональных данных. Оно предполагает жёсткое регулирование, которое потенциально может привести к многомиллионным убыткам для любой компании, неправильно обрабатывающей данные граждан Евросоюза. С одной стороны, этот закон стимулировал рост ИТ-рынка, потому что породил огромное количество услуг по адаптации корпоративных систем к GDPR. А с другой стороны, он закрыл Европу для многих сервисов нового поколения, чаще всего стартапов, базирующихся на сборе и анализе данных о пользователях. Например, сервис Unroll.me, который помогает пользователям отказаться от подписки на спам по электронной почте, получая доступ к содержимому их почтовых ящиков, приостановил обслуживание жителей ЕС. Компания Uber Entertainment, производящая онлайн-игры, закрыла свою игру Super Monday Night Combat в мае этого года из-за GDPR. Американская компания Brent Ozar Unlimited, занимающаяся обучением и консультированием, отказалась от доходов, поступающих из Европы, объяснив своё решение в блоге, озаглавив материал: «GDPR: почему мы перестали продавать в Европу».

В России тоже порой звучат предложения пойти по простому пути — запретить консолидировать персональные данные или жёстко зарегулировать доступ к ним. Например, разрешить хранить только анонимизированные данные. Но это вряд ли поможет. Просто те люди, которые строят услуги на купле/продаже данных, понесут дополнительные издержки, ведь стоимость данных увеличится. А мошенники также продолжат свою деятельность. Вывод один: запретами проблему не решить. Нужно думать, как помешать тем, кто использует персональные данные людей в мошеннических целях. И здесь возникает важнейший вопрос: кто должен разрабатывать технологии анонимизации и деанонимизации, обмена обезличенными данными?

Вряд ли это задача регулятора. Скорее всего, это поле для совместной работы профессионального сообщества. Если стоит задача усложнить жизнь мошенникам, которые хотят воспользоваться личной информацией, нужен общий «мозговой штурм». Инструменты должны разрабатываться по модели Open Source, учитывая опыт, например, Linux Foundation. То есть любой человек или организация, которая интересуется этими вопросами, может внести свой вклад в общее дело. На первом уровне — разработка механизмов, открытая для сообщества, а на втором должны подключаться механизмы сертификации.

Тогда получится сбалансированная конструкция: стандарт разрабатывает профессиональное сообщество, а регулятор выполняет технические процедуры: связывает конкретные стандарты безопасности с процессами. Это будет, во-первых, гарантировать прозрачность разработки стандартов анонимизации и обмена персональными данными и, во-вторых, уменьшит риск внедрения «бумажной безопасности».

Иногда высказывается радикальная идея: поместить все реальные данные в суперзащищённое хранилище. Все организации будут работать с некоторыми виртуальными образцами этих данных. Тогда, кажется, разрешаются все проблемы: украсть данные из корпоративных систем будет невозможно, объём предложения на чёрном рынке резко снизится, будет подорвана сама основа теневого бизнеса. Но здесь появляется вопрос: кто будет обеспечивать безопасность этого суперзащищённого хранилища оригиналов данных? Его ведь даже хранилищу золотого запаса страны не уподобить, ведь в те кладовые не ходят толпами самые разные люди и компании.

Единое место для хранения оригиналов всех персональных данных граждан, с одной стороны, должно быть на 100 % безопасным, а с другой стороны, взаимодействие с ним должно быть максимально доступным, простым и удобным. Отдельный вопрос — защита от хакеров. Получается, что сверхсекретное хранилище персональных данных придётся очень хорошо защищать, постоянно контролировать и при этом не лишать доступа к сервису всех желающих. Это очень сложная технологическая и не менее сложная административная задача. И то, и другое требует гигантских затрат.

Кроме того, нужно обеспечивать, с одной стороны, платный, а с другой — не очень дорогой доступ к этим данным. По сути, единственный, кто может осилить такой проект, — это государство. Точнее, государство должно создать инфраструктуру и делегировать полномочия по администрированию данных некоторому оператору. И снова мы возвращаемся к вопросу коллегиального прозрачного администрирования оборота персональных данных и к тому, что эффективнее всего это может сделать только профессиональное сообщество.

Подводя итог, скажу, что, прежде всего, надо думать не над тем, как ограничить доступ, а над тем, чтобы у мошенников не было возможности использовать эти данные. Ведь проблема главным образом не в том, что мошенник получил номер телефона, а в том, что он может связаться с человеком и причинить ему вред. Нужно уметь ограничивать использование персональных данных. И в этом, как ни парадоксально, могут помочь те же самые большие данные. Сегодня в Интернете есть немало ресурсов, где собирается и публикуется информация по телефонным номерам мошенников. Есть соответствующие мобильные приложения. На самом деле большие данные содержат много полезной информации, и её нужно использовать для того, чтобы помогать тем, кто находится под угрозой.

* * *

Эпоха больших данных, в начале которой мы находимся, требует серьёзных изменений в ментальных представлениях всех участников: разработчиков и пользователей технологий, регуляторов. Дело не в создании очередной ассоциации разработчиков и клиентов, а в том, что в эпоху больших данных принятие решений может быть только абсолютно прозрачным общим делом. Никто объективно не может найти решение этой проблемы в одиночку, нужно искать его совместно.

«КОНЦЕПЦИЯ СУВЕРЕННОЙ ИДЕНТИЧНОСТИ ВСЕЛЯЕТ НАДЕЖДУ»



Алексей КУБАРЕВ
руководитель
группы развития
бизнеса центра
продуктов Solar
Dozor компании
«Ростелеком-Солар»

Безусловно, данные граждан представляют ценность как с точки зрения широких возможностей их использования в мошеннических целях, так и для различных рекламно-маркетинговых компаний для навязывания различного рода коммерческих услуг. Поэтому им должна быть обеспечена надёжная защита. Пожалуй, не менее важными, чем утечки, являются такие задачи, как обеспечение целостности и доступности данных. Например, если хранящиеся в государственных информационных системах данные гражданина окажутся на какое-то время недоступными или и вовсе повреждёнными, то этот гражданин потом замучается бегать и доказывать, что он — это он. Он просто не сможет получить необходимые госуслуги. И тут многое зависит от того, насколько надёжную защиту этим данным обеспечат госорганы — операторы этих данных.

Что касается утечек конфиденциальных данных с промышленных предприятий, подобные инциденты несут серьёзную угрозу сразу большому числу граждан. Как минимум упрощают реализацию хакерской атаки на промышленный объект, от которой могут пострадать жители близлежащих населённых пунктов. А если речь об оборонном предприятии, то возникает угроза и для всей страны, вплоть до снижения её обороноспособности.

Мы уже живём в цифровом мире, наполненном разнообразными техническими средствами контроля. Системы защиты от утечек данных, контроля доступа, видеонаблюдения и т.п. используются повсеместно. Но обрабатывать весь объём информации, которая снимается с приборов, с помощью человеческих ресурсов невозможно, для этого применимы лишь технические средства контроля. Стоит подчеркнуть, что этический момент здесь присутствует незначительно — он касается тех немногих специалистов, которые настраивают систему контроля и с ней работают, то есть потенциально имеют доступ к личной информации сотрудников. Однако в крупных организациях осуществлять тотальное наблюдение

за каждым сотрудником в режиме 24/7 никто не будет, поскольку это слишком ресурсоёмкая задача. Поэтому я считаю, что технических средств вполне достаточно для решения задачи защиты от утечек данных.

Другой вопрос — какая технология наилучшим образом сможет решить задачу защиты ПД в информационных системах. Относительно идеи выделить суперзащищённое хранилище персональных данных и предоставлять всем заинтересованным структурам доступ к ним через некий виртуальный идентификатор — я считаю, что пока такая схема нереализуема. По крайней мере, на данном этапе развития технологий.

Приведу пример. Допустим, в организации есть хранилище, с которого снимается некий отпечаток, и с ним работают сотрудники. Но если этот отпечаток доступен сотруднику, значит, теоретически он может эти данные слить. Конечно, данные могут быть обезличены, тогда их утечка не страшна, но в таком случае большинство операций, связанных с идентификацией граждан, например банковские операции, с такими данными производить будет уже нельзя. Анонимизация данных применима лишь для узкого спектра задач, например проведения маркетинговых исследований, рекламных кампаний и т.п.

* * *

Правда, недавно возникла новая концепция суверенной идентичности (Self-sovereign identity, SSI), которая развивается в рамках блокчейн-технологий. Её смысл заключается в том, что пользователь сам владеет своими данными и сам предоставляет их тому, кому считает нужным, а также подтверждает их подлинность для верификации третьей стороной. В такой концепции пользователь лично отвечает за безопасность данных и может, например, продать свои данные рекламному агентству. Теоретически в результате реализации данной концепции или чего-то похожего можно будет минимизировать утечки баз, содержащих персональные данные.

«ИБ СУЩЕСТВУЕТ В ПАРАЛЛЕЛЬНОМ С ИТ-ТЕХНОЛОГИЯМИ МИРЕ»

Вопрос о безопасности больших данных — многоаспектная тема. По-крупному можно выделить две ключевые сферы. Во-первых, это большие массивы данных, которые накапливаются в различных транзакционных системах: государственные регистры, госуслуги, финансовые транзакции, коммерческие услуги в разных сферах. По существу, это структурированное электронное досье на человека — его цифровой профиль. Независимо от того, хранится такое досье в одной системе или во множестве, принадлежащих различным государственным или коммерческим операторам, сути дела это не меняет. Во-вторых, в связи с галопирующим развитием социальных сетей человек в течение своей жизни добровольно оставляет множество информационных следов. Если безопасность первого типа данных ещё как-то можно регламентировать законодательно и обеспечить приемлемый уровень их защиты, то предоставление человеком информации во втором случае — это свобода его воли. Здесь какие бы то ни было ограничения воспринимаются обществом весьма враждебно. Поэтому имеет смысл рассматривать вопросы безопасности в каждой из этих сфер отдельно.

В первом случае государственное регулирование защиты информации в России и в Европейских странах вполне адекватно. Основная проблема здесь заключается в стойком нежелании российских операторов данных выполнять предъявляемые требования в полном объёме и в ничтожном уровне ответственности за инциденты, связанные с неправомерным доступом или использованием больших данных. Второй проблемой является размывание ответственности за обеспечение безопасности таких данных между разными операторами. Третьей — недостаточная унификация технологий и продуктов для защиты данных.

Продукты защиты информации в российских реалиях живут в параллельном с ИТ-технологиями мире: ИТ-компании стремятся быстрее выпустить на рынок свои продукты, при этом значимая часть вопросов ИБ для них остаётся незакрытой. Необходимо сделать так,

чтобы выход «сырых», с точки зрения ИБ, продуктов на регулируемый рынок (государственные системы, базовая телеком-инфраструктура, финансы, торговля, медицина, энергетика и иные отрасли) был невозможен. А чтобы такой подход не отбросил ИТ-отрасль на годы назад, решения ИБ должны стать платформенными, компонентными — легко имплементируемыми в современный технологический стек. К сожалению, сегодня таких решений на рынке нет. Вместо этого мы видим всё более обособляющиеся экосистемы ИБ ведущих российских производителей средств защиты.

Безопасность информации в социальных сетях — это вопрос, который не может быть решён только в пределах национальных границ (в России это пытается делать Роскомнадзор, и часто успешно). Требуется широкий международный консенсус и наднациональное регулирование вопросов безопасности и использования данных в мировых агрегаторах информации — таких гигантах, как Google, Apple, Telegram, Amazon и т.п. В текущих реалиях эти операторы существенно злоупотребляют доминирующим положением и при попытках регулирования стремятся выйти из подчинения. Кроме того, отказ инфраструктуры таких операторов несёт глобальный риск для всего интернет-пространства. Недавним примером такого инцидента стал отказ CDN-провайдера Fastly, затронувший множество коммерческих и государственных ресурсов. Также недавно стало известно про утечку RockYou2021 — миллиардов паролей от учётных записей пользователей в различных публичных ресурсах. Оценить степень достоверности этой базы данных и масштаб ущерба не представляется возможным. Всё это представляет собой угрозу мирового масштаба.

Интересен вопрос выбора подходов к хранению БД. Задача безопасности транзакционных БД в подрегуляторных сферах вполне выполняема и даже не является сверхзадачей. При этом важно иметь в виду, что концентрация данных всегда консолидирует риски, связанные с их использованием. Так что стратегически распределённая система центров обработки данных с множеством центров ответственности (при условии должного, сопоставимого и



Дмитрий РОМАНЧЕНКО
директор
Департамента
информационной
безопасности
компании Rubytech

контролируемого уровня защиты) является гораздо более безопасной, чем создание единого мегахранилища (или мегаплатформы). К слову, идея мегаплатформы сейчас активно продвигается отдельными участниками рынка.

Уровень защиты всегда предполагает оценку потенциала злоумышленника, ценности защищаемых данных и стоимости самой защиты. Чем выше концентрация данных, тем больше их потенциальная ценность для злоумышленника, а значит, риск ущерба резко возрастает. Концентрация данных в одном месте приведёт к необоснованным затратам на их защиту, при этом атака на такой объект будет заветной целью для высокопрофессиональных нарушителей. В случае успешной атаки ущерб будет катастрофическим.

Отдельная серьёзная проблема — это подконтрольность субъекту его собственных персональных данных. Здесь также надо разделять транзакционные подрегуляторные истории и обычное использование социальных сетей, сервисов и экосистем глобальных игроков digital-рынка.

В первом случае цель обеспечения контроля вполне достижима. Необходимо на уровне регуляторов обязать операторов персональных данных обеспечить людям возможность контроля над использованием провайдерами их персональных данных. Неслучайно сегодня наметилась тенденция перехода от разобщённых и несогласованных множественных государственных ИС к централизованным ГИС по отраслям (ведомствам). Это поможет сократить число государственных операторов персональных данных и позволит отслеживать все обращения к персональным данным субъектов.

В банковской (финансовой) сфере и у телеком-операторов проблема решается ещё проще. Не секрет, что данные клиентов просто «продаются» или «сливаются» операторами на коммерческой основе. Аналогичная история — в страховом бизнесе и в коммерческой рознице. Здесь имеет смысл использовать европейский опыт и установить колоссальные штрафы за несогласованное с владельцем использование его персональных данных (по аналогии с санкциями за нарушение GDPR). Так, чтобы штрафкратно превышал потенциальную прибыль от продажи данных, причём по каждому субъекту.

Что касается вопросов защиты персональных данных в социальных сетях, то здесь на текущий момент может помочь только грамотная просветительская деятельность. Это долгий, планомерный и многоступенчатый процесс. Но начинать прививать цифровую гигиену нужно уже со школьной скамьи.

Рассматривается также подход, связанный с использованием анонимизации персональных данных, он вынашивается уже долгие годы. Технически вполне возможно ввести специальный ID для каждого человека и далее на основании этого ID связывать все данные человека в различных системах в единый профиль. Есть, однако, и некоторые возражения против такого подхода. Во-первых, таких идентификаторов у человека в России уже слишком много: номер паспорта, СНИЛС, ИНН, идентификатор в Единой биометрической системе (ЕБС) и другие. Во-вторых, это не меняет сути проблемы: неважно, хранятся в системе Ф. И. О. или иной идентификатор пользователя, за ним стоит конкретное физическое лицо. Поскольку при получении услуг и выполнении различных транзакций человек всё равно будет себя идентифицировать, важно обеспечить высокую степень безопасности каждой конечной точки транзакции, исключить неправомерное использование данных. При этом важно понимать, что задачу введения единого ID невозможно решить до тех пор, пока все данные в государственных и коммерческих системах не будут взаимоувязаны, а ошибки и дублирование — исключены. В России сейчас этот процесс идёт активно, но всё же пока не завершён.

* * *

Ещё одним риском такой «виртуализации» человека является возможность похищения всего его цифрового профиля и выполнение произвольных действий от его имени. Да и любая база ключей, связывающая ID с конкретным лицом, рано или поздно может быть скомпрометирована внешним или внутренним нарушителем. Чтобы этого не произошло, важно поддерживать требуемый уровень информационной безопасности контролируемого множества информационных систем, достоверно увязанных между собой по идентификаторам лица. Создание таких защищённых информационных систем должно стать утилитарной задачей, решить которую позволит переход на компоненты обеспечения ИБ, стандартизованные по интерфейсам, технологиям и протоколам. Сегодня, однако, заметными препятствиями к такому переходу становятся: технологический монополизм производителей средств защиты информации в России, а также разобщённость рынков ИТ и ИБ. Устранить данное препятствие по силам только государству при активном участии независимых коммерческих игроков рынка.

«ПРОБЛЕМА БД — ЭТО В ПЕРВУЮ ОЧЕРЕДЬ МОРАЛЬНЫЙ ВЫЗОВ»

Большие данные сегодня собираются на разных уровнях и в интересах различных структур. Думаю, в первую очередь необходимо защищать всё то, что связано с персональными данными граждан. Ведь именно они в современной России позволяют криминальным элементам разного толка осуществлять мошеннические действия: красть деньги со счетов граждан, представляясь сотрудниками банка, брать на них кредиты, подделывать документы для сделок и многое другое. К сожалению, в этой сфере очень силен человеческий фактор — сами сотрудники оператора персональных данных продают данные, и этот теневой рынок в России развит.

О параметрах его развития можно судить, например, по данным исследования мирового рынка преступных киберуслуг, которое провела компания Positive Technologies в 2018 г. Например, стоимость целевой атаки на организацию в зависимости от сложности может составлять от 4500 долл., включая наём специалиста по взлому, аренду инфраструктуры и покупку соответствующих инструментов. Взлом сайта с получением полного контроля над веб-приложением обойдётся всего в 150 долл. Если войти в TOR и сделать запрос «Купить персональные данные», можно увидеть обилие предложений и сайтов, на которых эти данные продают. Купить фото документов человека — от 300 руб., а полное досье на персону стоит около 70–100 тыс. руб. Но технологии между тем двигаются дальше. Множество ботов в Telegram могут предоставить доступ к данным по украденным базам и утечкам (это и персональные данные в виде телефонов, паспортов, номеров машин, и слитые в сеть пароли, и многое другое) — и это уже отдельные не подконтрольные государству сервисы. Вопрос только в актуальности и достоверности этих данных.

ЧТО ДЕЛАТЬ?

Тут нужно и усиление мер защиты этих данных в самом операторе, и внедрение разных средств контроля, например систем класса DLP. В целом значимость таких систем в свете сегодняшней ситуации будет только повышаться. Однако сама по себе DLP-система обеспечить полную безопасность не сможет, это лишь один из «кирпичей» в вашей защите («стене») от утечек. Тут надо понимать специфику того, что защищаем,

где защищаем, и тогда становится понятно, как надо защищать. По крайней мере, компании «ВС Лаб» удаётся подобрать и способы, и средства для защиты своих клиентов.

Например, связка DLP + OSINT (Open source intelligence — глубокий интеллектуальный поиск в Интернете) может показывать очень интересные результаты: выявлять потенциально неблагонадёжных сотрудников, обнаруживать и перехватывать каналы продаж персданных, выявлять способы хищения и взлома.

Кроме того, оператору необходимо отслеживать факт утечек данных в Dark Web. Здесь также могут помочь наработки, связанные с технологиями OSINT. Приведу пример работы OSINT: система автоматически вытягивает с разных специфических форумов информацию о появившихся новых уязвимостях в распространённом ПО или популярном аппаратном обеспечении. Эта информация видна подразделениям заказчика, обеспечивающим защиту, и они тут же начинают придумывать способы устранения этих уязвимостей.

Второй пример с OSINT. Компания берёт на работу нового специалиста, получающего доступ к важной информации, и система сама проверяет его на наличие связей с различными сообществами и предоставляет данные в службу безопасности. Третий пример: DLP-система выявила круг общения некоторого специалиста, и если у него корпоративный телефонный номер, то по нему получаем списки людей, с кем этот человек активно созванивается сам и кто ему звонит. На основе этих данных OSINT может предоставить данные по коммуникациям человека, а также понять, от каких организаций поступают звонки. Например, если сотрудника беспокоят коллекторы, значит, у него финансовые проблемы, а стало быть, есть риски. Это очень простой кейс, но тем не менее весьма показательный.

Ещё один пример: DLP + система видеоаналитики. DLP не даст скопировать данные, а видеоаналитика покажет, когда сотрудник попытается сфотографировать эти данные с экрана компьютера или когда сотрудник будет совершать звонок кому-то по личному телефону с открытым окошком персданных в программе оператора.

Сегодня нередко поднимается вопрос о соотношении моральных и технических аспектов в



**Дмитрий
ВАСИЛЬЕВ**
президент
компании «ВС Лаб»

сфере применения DLP-систем. Здесь, на мой взгляд, работают два основных тезиса. Первый: у злоумышленников нет морали. Второй: DLP-система — это «кибер-/автоматизированная мораль» сотрудника организации. По-моему, это намного надёжнее, чем просто вера в человека.

DLP и другие умные системы — это правильный и достаточно надёжный способ контролировать мораль сотрудника. Даже если для этого сотрудникам, например, современного банка, придётся работать весь день под прицелом видеокамер и всяких умных систем, которые фиксируют и анализируют движение его глаз, рук, произнесённые слова и сопутствующие интонации и т.д. И только потому, что у преступников нет морали, офис или подразделения крупного банка или иной организации, работающей с персональными данными, должен быть под усиленным контролем. Ибо утечка данных может нанести слишком большой вред.

Конечно, можно попробовать посмотреть на проблему с другой стороны — это борьба с незаконным бизнесом на персональных данных в DarkNet. В самом деле, есть же возможности снизить степень воздействия криминала на общество в офлайне! По аналогии можно предположить, что подобные действия могут привести к снижению воздействия киберпреступности на общество. Правда, «серебряной пули» в этой части пока не существует. Сегодня мы можем только взять в качестве аксиомы тезис: чем меньше у злоумышленников товара для продажи, тем лучше. Значит, чем будут лучше защищены данные, тем меньше будет утечек, а значит, меньше товара на чёрном рынке. Если же мы понимаем каналы распространения утечек или каналы взлома, то нам проще это пресечь или взять под контроль.

Другой вариант снизить порог утечек — это проводить обезличивание данных, но тут, как говорится, дьявол кроется в деталях: стандарты обезличивания у всех свои.

С общих позиций, разработка универсального решения не является чем-то невозможным, это всего лишь вопрос затраты определённых сил и средств и определённых компромиссов. Кроме того, нужно понимать, что даже при появлении такого универсального подхода всё равно придётся защищать каждый узел передачи данных, а это вновь — деньги и люди. К тому же нужно вовремя остановиться: если довести ситуацию до того, что обмен данными между системой анонимизации/обезличивания и базами данных будет осуществляться в каком-то закрытом контуре, это наложит ограничения на скорость обработки данных, а значит, на скорость и

качество оказания услуги потребителю, то есть принесёт вред бизнесу. А это уже явный перегиб. Надо искать компромиссы. Причём не только в технической части.

Надо отдавать себе отчёт в том, что все серьёзные подвижки в этом плане будут «оплачиваться» редуцированием того, что сегодня называется цифровым суверенитетом человека. Дело в том, что в современном мире нет никакой приватности: она иллюзорна. Как только в ваших руках появился смартфон и вы начали активно с ним работать, забудьте о приватности — ваши данные видят все (банки, сотовые операторы, государство и т.д.). Моё мнение: если из-за потери приватности я буду в безопасности (во всех смыслах) и мои данные будет обрабатывать только государство и с помощью тех компаний, которым я разрешу это делать, то я не вижу в этом ничего страшного. «Цифровая слежка», кстати, может быть полезна и для самого гражданина, как, например, в случае подтверждения алиби человека на основе геоданных его мобильного телефона. Примеров, когда «цифровая слежка» работает в интересах общества и конкретного человека, множество.

В государстве должен быть найден баланс между безопасностью и анонимностью. Насколько я понимаю, в правительстве и правоохранительных органах всегда обсуждается нахождение именно этого баланса. С одной стороны, никто не будет требовать отмены видеонаблюдения на улицах, ведь это вопросы безопасности нас самих и наших близких. С другой стороны, правоохранительные органы всегда хотят ужесточить свои требования, увеличить своё влияние и возможности. Но предъявлять на каждой интернет-сессии свой паспорт — это уже нелепо. Если система определяет, что у человека недобрые намерения, — это хорошо. А если по моему лицу можно узнать мои паспортные данные и привязку к банковской карте — это плохо.

* * *

Мы живём в интересное время: бурное развитие технологий обуславливает появление множества моральных вызовов. И именно нам с этими вызовами нужно внимательно разбираться. Простых решений здесь нет, а с течением времени указанные проблемы будут лишь усугубляться. Нужно работать над формулировкой некоторого общественного договора — достигать консенсуса между государством и человеком.



«ГРАЖДАНИН ДОЛЖЕН ЗНАТЬ, КТО И ЗАЧЕМ ЗАПРОСИЛ ЕГО ДАННЫЕ»

Большие данные собираются в разных информационных системах. Думаю, в первую очередь нужно уделять внимание тем, что являются критическими для управления технологическими циклами. Например, данным для управления домами. Если в ходе кибератаки их подменить, это может обернуться катастрофой. Таких примеров много, хотя, конечно, непросто найти общий подход, в рамках которого можно говорить, что одни данные нужно защищать, а другие могут «постоять в очереди».

Основной риск, связанный с большими данными, — их потеря, например, в результате действия шифровальщика, порчи носителей или ИТ-инфраструктуры. Конечно, БД, представляющие собой огромный массив, целиком украсть сложно, однако их можно украсть частично.

И именно из-за того, что их нельзя украсть в полном объеме, необходимо иметь такие технологии, которые позволят выявлять факты того, что передаваемая наружу информация содержит данные из «озера локальных данных». Иными словами, необходимы системы, детектирующие выгрузки из баз.

При этом к числу основных рисков, связанных с обработкой больших данных, следует отнести отсутствие бэкапов. Создание резервных копий БД, равно как и их сбор, — это бесконечно дорогое удовольствие. Поэтому, как правило, отсутствует возможность их восстановления. Если говорят, что в результате инцидента выгружены все данные, это означает, что кто-то целенаправленно вынес все дисковые массивы.

Фокус при выборе средств защиты информации нужно делать на предотвращение атак за



Андрей АРЕФЬЕВ
директор
по инновационным
проектам
ГК InfoWatch

счёт создания замкнутых экосистем и использования специфических средств, например систем детектирования шифровальщиков. На рынке существуют, к сожалению, недовостребованные в России технологии DSML-платформы (Data Scientist Machine Learning Platform). Они представляют собой замкнутые экосистемы, позволяющие, с одной стороны, организовывать сбор данных, а с другой — их использование. За счёт изоляции от внешнего мира такой подход обеспечивает защиту периметра в среде виртуализации, что значительно усложняет злоумышленникам возможность шифрования. Одной из базовых функций таких платформ является управление и контроль доступа к большим данным.

Если перейти от общих вопросов защиты БД к наиболее актуальным, например утечкам данных банковских клиентов, что обычно происходит с помощью пособников-инсайдеров, то здесь принципиальных проблем нет: компании, занимающиеся сбором и хранением БД, должны отвечать за их безопасность, защищать от несанкционированного доступа к ним. Использование этих данных на стороне — это непосредственная ответственность компании. Конечно, для этого нужно уделять должное внимание средствам защиты от утечек. Ежегодно мы фиксируем преобладающее число утечек из внутренней изолированной среды по вине внутренних нарушителей. Это говорит о том, что необходимо использовать технологии, позволяющие выявлять факты передачи хранимой информации. Однако как производитель ИБ-решений я должен заявить: мы испытываем существенные сложности от отсутствия ярко выраженных санкций регуляторов в таких ситуациях.

Ещё одна остро дискуссионная тема — о соотношении цифрового суверенитета конкретного человека и цифрового суверенитета государства. В целом на этот вопрос сегодня нет чёткого ответа. Только зрелое общество в состоянии найти справедливый ответ на вопрос, где кончается цифровой суверенитет гражданина и начинается зона интересов государства.

Пожалуй, стоит начать с того, чтобы чётко отделить персональные данные, с которыми работают государственные структуры, от деталей частной жизни человека. Тогда, говоря о регулировании взаимоотношений человека и государства в области персональных данных, было бы справедливо иметь такой механизм, в рамках которого гражданин знает, когда его персональные данные начинают обрабатываться той или иной организацией и для какой цели.

Сегодня же, не имея централизованной системы сбора данных, мы вновь и вновь оставляем

свои данные, создавая бесконечные дубли в каждой новой организации. Иными словами, совершенно потеряв контроль над сбором и обработкой персональных данных, отсутствует понимание, зачем происходит этот бесконечный сбор. Возможно, при наличии единого реестра персональных данных в рамках государства и при условии, что любое обращение любой организации к такому реестру контролируется конкретным гражданином, мы могли бы получить более-менее уравновешенную ситуацию.

На уровне государства этот подход должен подразумевать контроль действий любых организаций и предоставлять только ту информацию, которую разрешил гражданин. Стоит отдельно отметить, что такая система будет представлять лакомый кусок для злоумышленников, и прежде чем её создавать, нужно тщательно продумать, как её защищать.

Вопрос анонимизации персональных данных в виде, например, уникального идентификатора для каждого гражданина имеет много аспектов, не всегда однозначных. Скажем, персональный идентификатор практически не отличается от номера паспорта: в какой-то момент такой идентификатор станет фактически ID, то есть ещё одним числом, присваиваемым человеку. Ситуацию это не особенно изменит. Качественные сдвиги могут произойти, если гражданин будет знать, кто и зачем запросил доступ к данным о нём, и будет иметь возможность этот доступ контролировать.

Технологически можно сделать так, что никто технически не сможет получить или предоставить доступ к персональным данным, кроме владельца. Такой подход может строиться на технологиях шифрования, распределённых реестров шифрования, где только обладатель уникального ключа может обеспечить доступ к своим данным. Однако нельзя исключить, что предоставленный доступ будет агрегирован и мы получим очередной дубликат. Тут необходимо продумать ответственность тех, кто запрашивает доступ к данным.

* * *

Считаю, что приоритетом в области регулирования БД в данный момент должно стать ужесточение мер за агрегацию больших данных. Если доказано, что компания собирает большие данные и не принимает мер по обеспечению их защиты, что утечка или изменение данных имело последствия, такая компания должна привлекаться к серьёзной ответственности.

«ЦИФРОВОЙ СУВЕРЕНИТЕТ ЧЕЛОВЕКА — ЭТО МИФ»

Необходимо понимать: абсолютной защиты не бывает. Даже если установить лучшую DLP-систему, отключить порты на компьютерах сотрудников, запретить пользоваться флешками, закрыть Интернет, включить видеонаблюдение, анализировать поведение... всё равно серьёзно замотивированный на кражу данных сотрудник найдёт способ обойти защиту. И это печально. Мы настолько привыкли к постоянным кражам и утечкам информации, что уже смирились: пусть уж лучше будет корпоративный «цифровой концлагерь», лишь бы это хоть немного исправило ситуацию.

Простых решений здесь нет. Скажем, невозможно забрать у компаний саму возможность собирать данные, чтобы пресечь их нелегальные утечки. Данные — это новая нефть, необходимая для работы «двигателя» бизнеса. Более того, люди сами предоставляют свои данные компаниям, когда пользуются их сервисами. Цифровой суверенитет человека — это миф, его не существует. В современном мире мы не можем не оставлять цифровых следов. Можно лишь пытаться избегать «цифровой слежки» или «цифрового мониторинга», отказываясь от цифровых услуг. Но вряд ли городской житель сможет отказаться от сотовой связи, услуг банков или скрыть своё лицо от видеокамер.

Ещё важно отметить, что украденные данные используются в том числе и для обогащения баз данных киберпреступников. Сама по себе одна небольшая утечка может и не угрожать человеку, но если добавить к ней информацию из прошлых и новых утечек, то со временем накопится критичный объём информации, ущерб от использования которой будет существенным для большого количества людей.

Ещё один важный аспект. Уровень анонимности профессиональных преступников в DarkNet максимальный. Они могут работать из любой точки мира и применяют такие техники и инструменты, которые практически не позволяют их идентифицировать, что делает их поимку невозможной. А взаимодействие между странами в области борьбы с киберпреступностью не всегда эффективно. Получается, что мы можем воздействовать в основном на то, что можем сами контролировать. В первую очередь я имею в виду системы защиты внутри компаний и вовлечение в них сотрудников.

Люди традиционно являются одним из самых слабых звеньев в системе защиты. Задача компании, в частности службы ИБ и кадровых подразделений, заключается в том, чтобы обучить их правилам защиты и, что крайне важно, мотивировать их защищать корпоративные данные и данные клиентов. Мотивация здесь является ключевым элементом: сотрудник должен не только бояться совершить ошибку, но и хорошо относиться к своей компании, быть лояльным, чтобы точно соблюдать все внутренние правила безопасности.

Какую поддержку этим процессам могут оказать технологии? Например, определённая анонимизация персональных данных, которая сократит возможность получения интегрированных данных. Это можно сделать с помощью технологии блокчейн. На рынке уже есть решения, которые дают возможность пользователям самостоятельно хранить свои данные и полностью контролировать их предоставление тем или иным компаниям или организациям. Думаю, этот подход получит широкое распространение.

Также самим компаниям стоит придерживаться правил «техники безопасности» при работе с корпоративными данными. Например, сокращать наборы собираемых данных. Скажем, компаниям розничной торговли не нужны паспортные данные клиентов для совершения коммуникаций, но они их нередко собирают. Это называется избыточной обработкой данных по отношению к целям обработки.

Ещё пример: компания занимается разработкой своих внутренних ERP- и CRM-систем и использует для их тестирования реальные, а не обезличенные данные. Мы знаем много громких примеров утечек, связанных именно с такой ситуацией, хотя существуют инструменты и технологии, позволяющие маскировать и обезличивать информацию, используемую для тестирования.

Указанные аспекты — только часть проблемы. Конечно, нужно развивать технологии — они должны исправлять ошибки людей, нужно вводить правила и ограничения, повышать штрафы за утечки, повышать культуру кибербезопасности.

Ещё, на мой взгляд, очень важно, чтобы государство своим примером показывало, как нужно управлять данными граждан и защищать их. Если государство будет задавать тренд и высокие стандарты безопасности данных граждан, то все остальные будут вынуждены соответствовать этому уровню.



Андрей ТИМОШЕНКО
руководитель
практики
информационной
безопасности
Accenture в России

«ИНТЕРНЕТ — ЭТО НОВОЕ ПРОСТРАНСТВО, И ЕМУ ТРЕБУЕТСЯ СВОЙ КОДЕКС»¹



Игорь АШМАНОВ
президент ИТ-компаний «Крибрум» и «Ашманов и партнёры»

Необходимо требовать участия общества во всех вопросах цифровизации общества, обсуждается ли проблема утечек больших данных или внедрение искусственного интеллекта в школе. Скажем, для целей безопасности граждан не нужно распознавать лица всех людей, проходящих мимо видеокамеры, как будто все они потенциальные преступники. Для целей безопасности нужно распознавать злодеев.

Дело в том, что цифровая среда, конечно, полезна, с её помощью можно многое сделать. Но её нужно привести в соответствующее рациональное русло. Приведу аналогию: Интернет стал транспортом для передачи информации и теперь занимает определённое место в нашей жизни — наряду с другими транспортными системами, занимающимися в наших домах водоснабжением, электроснабжением и т.д. В этих традиционных коммунальных системах есть встроенная базовая безопасность: кто-то, формируя схему забора и доставки воды потребителям, уже обеспечил эту безопасность. Интернет стал таким же транспортом, но его базовую безопасность никто не обеспечивает. Только Роскомнадзор пытается что-то делать в этом направлении.

Но нужно гораздо больше. Нужно довести до завершения серию законов про западные платформы, чтобы они начали выполнять требования наших законов и удалять контент. Надо окончательно зачистить экстремистский и прочий нежелательный контент. Нужно создать бригады, которые занимаются конкретными видами цифровых преступлений типа школьных расстрелов, закладок наркотиков и т.д.

Интернет — это ведь новое пространство, которому требуется свой кодекс, подобно тому как Морской кодекс регулирует отношения, возникающие в мореплавании, а Воздушный кодекс РФ регулирует использование воздушного пространства страны и деятельность в области авиации. В Интернете правил «дорожного движения» сейчас нет, но они должны появиться, потому что нужно разрешить проблемы, возникшие из-за отсутствия правил.

Роскомнадзор должен получить гораздо больше полномочий. Ведь сегодня, по сути, если он хочет проверить, не ущемляются ли права граждан, он проверяет бумажные документы. Компании показывают проверяющим регламенты обработки персональных данных, которые могут хорошо выглядеть, но при этом понять, куда на самом деле деваются данные граждан, Роскомнадзор не может.

Работа над новыми задачами только-только началась. В частности, есть поручение Президента РФ создать концепцию защиты прав граждан в цифровом пространстве. Она должна быть представлена 1 августа. Но это только концепция. Далее должны пойти целенаправленные процессы реализации этой концепции на административном уровне — в Государственной думе, правительстве и т.д.

Но возможно, что наши «цифровизаторы» во власти не захотят много думать и удовлетворятся небольшими поправками к нынешним законам. Поэтому поддержать идею реализации Цифрового кодекса может общественность. Нужно привлекать внимание государства к тому, что у общественности есть негативное отношение к «ковровой» цифровизации.

¹ На основе контента «Главное с Анной Шафран» на телеканале СПАС

ПОСЛЕСЛОВИЕ ОТ РЕДАКЦИИ

Очевидно, что privacy (конфиденциальность) частных лиц сегодня нарушается не только откровенными злоумышленниками из DarkNet. Однако содержательное определение понятия «цифровой суверенитет личности» ещё только предстоит сформулировать. Дальше всё будет зависеть от того, примет ли общество ту грань, которая отделит «цифровую слежку» от «цифрового мониторинга безопасности граждан и государства». Понятно,

что полного единства мнений в масштабах всей страны тут быть не может. Однако для государства важно, чтобы представления о цифровых правах граждан консолидировали общество. А для этого одних технологий ИТ и ИБ недостаточно. Кто-то или что-то должно стать гарантом правильного использования Больших данных в обществе. И именно это, похоже, и станет ключевым вопросом безопасности Больших данных в ближайшей перспективе.



АССОЦИАЦИЯ
БАНКОВ
РОССИИ



ХVIII Международный банковский форум «Банки России - XXI век»

Организуемый Ассоциацией банков России форум является одним из самых крупных и представительных мероприятий в стране, пользуется заслуженным вниманием банковского сообщества, регуляторов финансового рынка, органов исполнительной, законодательной власти и средств массовой информации.

На форуме традиционно выступают руководители Банка России, федеральных министерств и ведомств, члены Совета Федерации и депутаты Госдумы, топ-менеджеры банков, представители международных финансовых организаций.

Панельные дискуссии и круглые столы в этом году посвящены ключевым вызовам и направлениям развития финансового рынка в России и в мире, цифровой трансформации, ESG-банкингу, маркетплейсам и экосистемам, развитию и регулированию региональных кредитных организаций и банков с базовой лицензией, вопросам снижения регуляторной нагрузки, применения искусственного интеллекта, обеспечения информационной безопасности, регулирования персональных данных и банковской тайны физических лиц.

15 - 18 сентября 2021 года

Сочи, отель Radisson Collection Paradise Resort & Spa

Генеральный спонсор



Оргкомитет:
тел./факс: (495) 785-29-93, 785-29-88
e-mail: event@asros.ru
www.asros.ru





Василий ПИСКАРЕВ
председатель Комитета
Государственной
Думы по безопасности
и противодействию коррупции

НЕ ДАТЬ ПОГАСИТЬ «ЗАРНИЦЫ ДОВЕРИЯ»

КИБЕРБЕЗОПАСНОСТЬ ТРЕБУЕТ ОТВЕТСТВЕННОГО ПОВЕДЕНИЯ

Недавняя встреча Владимира Путина и Джоозефа Байдена в Женеве заронила надежду, что между Россией и США возобновится полноценный диалог по широкому кругу вопросов — и в том числе о стратегической стабильности и кибербезопасности. Опыт последних лет, когда уровень отношений между нашими странами снизился до рекордно низких значений, показывает, что в интересах каждой из сторон контакты нужно налаживать, как бы трудно это ни было. Нельзя допустить, чтобы противники диалога погасили те «зарницы доверия», проблески которых заметил в ходе встречи Президент В. В. Путин.

ОТВЕТСТВЕННОСТЬ И СОТРУДНИЧЕСТВО

В то время как наши заокеанские партнёры составляют списки кибердержав, рождают всё новые и новые воинственные термины, — «киберкомандование», «киберразведка», «кибервойна», — и меряются силой в виртуальном пространстве, Россия последовательно на протяжении уже многих лет настаивает на формировании глобальной системы международной информационной безопасности. В её основе должно быть не планирование кибервойн и спецопераций в Интернете, а мирное сосуществование и сотрудничество, предотвращение конфликтов в информационном пространстве.

Последовательная позиция Российской Федерации находит поддержку на уровне ООН. Совсем недавно, 1 июня 2021 года, в Нью-Йорке состоялась первая (организационная) сессия Рабочей группы открытого состава, которая в период до 2025 года должна выработать систему правил и принципов ответственного поведения государств в информационном пространстве. О серьёзности формата говорит участие в нём 193 государств. И безусловной победой нашей страны стало создание Специального

межправительственного комитета экспертов открытого состава, которому предстоит разработать и представить на Генеральной ассамблее ООН конвенцию о противодействии использованию информационно-коммуникационных технологий в преступных целях.

Прогресс в консультациях между Россией и США по вопросам кибербезопасности помог бы серьёзно продвинуться в этом направлении, но пока мы видим со стороны администрации Байдена скорее декларации о намерениях и расставление флажков, чем реальные шаги навстречу. Как отметил на пресс-конференции в Женеве В. В. Путин, на все десять американских запросов в сфере кибербезопасности в прошлом году Россией были даны «исчерпывающие ответы», а вот десятки российских запросов остались без ответа. Замглавы МИД России Сергей Рябков сообщил, что наша страна более 40 раз обращалась к Соединённым Штатам по конкретным ситуациям использования сетевого пространства для осуществления атак на российские госструктуры и различные юридические лица. Но американская сторона отвечает на обращения России, по меткому выражению дипломата, «крайне редко» — «практически никогда». По-видимому, для Вашингтона важнее информационный шум о кибератаках «русских хакеров», чем сотрудничество в противодействии таким угрозам. А между тем, киберкриминал, который не знает границ, в период пандемии COVID-19 заметно нарастил свою активность и стал серьёзной проблемой не только для наших двух стран, но и для всего мира.

По данным МВД России, только в январе этого года в нашей стране количество преступлений в сфере информационно-коммуникационных технологий выросло на треть, причём нередко совершаются они из-за рубежа, и даже установленных преступников поэтому трудно наказать. Действенное международное сотрудничество в этой сфере давно уже назрело.



В дискуссии с Германом Грефом о том, как пресечь телефонное мошенничество

ОСТАНОВИТЬ «РЫБАКОВ» И «ПСИХОЛОГОВ»

Развитие технологий в сочетании с доверчивостью людей открывает широкий простор для совершения мошеннических преступлений. Одним из самых распространённых в последние десятилетия остаётся так называемый «фишинг» — выманивание персональных данных у пользователей сети с помощью фейковых рассылок и мошеннических сайтов, чтобы получить доступ к их сбережениям.

Как показывает практика, современные мошенники используют для достижения своих целей самые последние достижения науки и техники, но нередко им бывает достаточно самого простого кнопочного мобильного телефона и владения нехитрыми психологическими приёмами, чтобы выудить у человека все его сбережения. Их жертвами становятся не только пожилые люди, которые с доверием относятся к звонкам якобы представителей службы безопасности банка или правоохранительных органов, но даже сами сотрудники финансовых учреждений, казалось бы, знающие все тонкости банковского дела.

Во многих случаях такие звонки осуществляются из мест лишения свободы или следственных изоляторов. Одной из мер противодействия мошенникам стал разработанный мной совместно с коллегами закон, который позволит ликвидировать тюремные «колл-центры». В марте этого года он подписан Президентом России. Операторы мобильной связи по представлению руководителей федеральных и

территориальных органов уголовно-исполнительной системы теперь обязаны прекращать оказание услуг по тем абонентским номерам, с которых осуждённые, находящиеся в исправительных учреждениях, или лица, содержащиеся в следственных изоляторах, осуществляют противоправную деятельность.

Другой проблемой, которая требует законодательного решения, стало так называемое «ложное минирование». Из-за сообщений о якобы готовящемся акте терроризма эвакуируются сотни людей, закрываются на проверку больницы, школы, магазины, предприниматели терпят убытки. Несколько лет назад нам удалось сбить вал таких звонков, усилив ответственность по ст. 207 УК РФ за это опасное преступление.

Однако, сейчас мы видим, что подобные случаи повторяются вновь, и мы имеем дело уже не с обычными телефонными хулиганами. Большинство таких сообщений сегодня приходит с зарубежных электронных почтовых сервисов. Ложные сообщения о терактах поступают из Германии, Франции, США, Бельгии, Голландии, Японии и Украины. Всего за несколько лет в России было зафиксировано свыше 16 тыс. таких ложных сообщений, «заминированы» были 50 тыс. учреждений в России, эвакуировано порядка 1,5 млн человек.

Мы работаем сегодня над поправкой в действующее законодательство об оперативном ограничении доступа к информации, содержащей заведомо ложное сообщение об акте терроризма. В соответствии с ней Генеральный прокурор и



Заседание Комиссии Государственной думы по расследованию фактов вмешательства иностранных государств во внутренние дела России

его заместители смогут во внесудебном порядке ограничить доступ к ресурсу, распространяющему фейковую информацию. Все поступающие сообщения по-прежнему будут проверяться, но дезорганизовать работу социальных и образовательных учреждений, объектов транспорта, сеять панику среди людей мы не позволим.

ПРИЗЕМЛЕНИЕ СОСТОИТСЯ В ЛЮБУЮ ПОГОДУ

В июне, в последний день итоговой сессии Государственной Думы 7 созыва был принят федеральный закон, который журналисты окрестили «законом о «приземлении» IT-гигантов». Он обязывает владельцев крупных информационных ресурсов открывать в России филиалы, представительства или учредить российские уполномоченные юрлица своих фирм. На прошедшей недавно прямой линии Президент России В. В. Путин подчеркнул, что если зарубежные соцсети работают и «деньги зарабатывают» в России, то должны выполнять российские законы. Важно, что он открыто заявил, что «на первом этапе мы настаиваем, чтобы эти платформы открывали у нас полноценные представительства».

«Приземлиться» в России новый закон заставит социальные сети, различные поисковые и рекламные системы, аудиовизуальные сервисы, мессенджеры, интернет-магазины, а также хостинговых провайдеров, игровых дистрибьюторов и онлайн-игры. Речь идёт об иностранных IT-гигантах с суточной аудиторией более полумиллиона пользователей в России. Им предстоит зарегистрировать личный кабинет на сайте Роскомнадзора и разместить у себя электронную форму для обратной связи с российскими гражданами или организациями.

Ранее другим принятым Госдумой законом их обязали самостоятельно модерировать и удалять противоправный контент. Теперь необходимо тщательно проконтролировать, чтобы это требование выполнялось. Опыт прежних лет показал, что без нажима со стороны регулятора они делают это, мягко говоря, неспешно и неохотно. Так, по данным Роскомнадзора,

с 2015 года Google и Youtube не удалили более 5,2 тыс. запрещённых материалов, а Facebook и Instagram — около 3,7 тысяч. Такая медлительность, конечно, недопустима.

Считаю принятие этих двух законов принципиально важным решением. Комиссия Государственной Думы по расследованию фактов вмешательства иностранных государств во внутренние дела России, которую я возглавляю, ведёт мониторинг публикаций в Интернет-пространстве и давно обратила внимание на весьма вольные действия IT-гигантов, которые расходятся с российским законодательством.

В январе-феврале этого года мы были свидетелями того, как наших детей пытались активно вовлечь через соцсети и мессенджеры в противоправные действия. Ежедневно появлялись сотни таких публикаций, и зарубежные площадки, на которых они размещались, скажем прямо, не торопились удалить такие сообщения ни по требованию Роскомнадзора ни самостоятельно. Мы решили с этим досконально разобраться. Комиссия инициировала и провела прямые переговоры с руководством соцсетей и видеохостингов для разъяснения требований российского законодательства в информационном пространстве и представления методических рекомендаций.

СОЦСЕТИ И ВИДЕОХОСТИНГИ ДОЛЖНЫ СТАТЬ МАКСИМАЛЬНО БЕЗОПАСНЫМИ ДЛЯ ДЕТЕЙ

9 апреля состоялась видеоконференция Москва — Сингапур — Дублин с участием депутатов-членов нашей Комиссии и представителей руководства компании «ТикТок» во главе с Хелен Лерш, директором по связям с органами власти и корпоративным вопросам. Разговор шёл о нарушениях, допущенных компанией. Мы привели руководству «ТикТок» примеры, когда пользователи видеосервиса могли знакомиться с информацией, доступ к которой подлежит ограничению в соответствии с российским законодательством.

«ТикТок», наряду с другими зарубежными интернет-ресурсами, в течение довольно длительного времени распространял в нашей стране запрещённую информацию — призывы к несовершеннолетним участвовать в несанкционированных митингах, призывы к насилию и нападению на сотрудников правоохранительных органов (мы насчитали свыше 1000 таких публикаций). При этом, по сравнению с другими аналогичными сервисами, «ТикТок» отличился «наибольшей активностью» в распространении деструктивных призывов к детям. И что особенно вызвало возмущение наших граждан — распространялись призывы к детским самоубийствам (зафиксировано более 250 опубликованных материалов).

Фокус-группой данного видеосервиса преимущественно является молодёжь, поэтому характер и качество распространяемых им на российскую аудиторию видеоматериалов привлекли особое внимание депутатов. По данным, которые есть в распоряжении Комиссии, рекомендательные сервисы ТикТока целенаправленно использовались для адресной рассылки противоправного контента, ориентированного на молодёжь, которая политикой ранее не интересовалась, что, конечно же, недопустимо.

Мы получили от Роскомнадзора подтверждение, что «ТикТок» в целом удалил противоправный контент по незаконным протестным акциям, а также публиковавшиеся призывы к детям совершать 3 марта самоубийства. Но большинство материалов удалялось в течение длительного времени, что позволило организаторам манипулирующего контента достигать запланированного массового эффекта и своих незаконных целей. Более того, российскими компетентными органами фиксировались факты восстановления ранее удалённых материалов (известно более 70 таких случаев).

Мы обсудили с руководством компании технологические особенности их работы по модерации размещаемых пользователями материалов, высказали свои рекомендации и предложили методическую помощь.

В целом руководство видеосервиса проявило готовность к сотрудничеству, нас проинформировали об уже удалённом противоправном контенте. Такая работа, по словам представителей компании, продолжается персоналом «ТикТок»



Телемост Москва – Сингапур – Дублин связал членов Комиссии по расследованию фактов вмешательства иностранных государств во внутренние дела России с руководством компании «ТикТок»



На связи с Госдумой Хелен Лерш, директор по связям с органами власти и корпоративным вопросам компании «ТикТок»

в офисах компании, расположенных в Сингапуре, Лос-Анджелесе и некоторых других городах мира. В ходе обмена мнениями представители «ТикТок» высказали намерение продолжать контакты с Комиссией Госдумы.

GOOGLE: ПОЛИТИЧЕСКАЯ ЦЕНЗУРА ЕСТЬ, И ОНА ВЕСЬМА ИЗБИРАТЕЛЬНА

16 апреля такой же видеомост Москва — Брюссель — Москва мы провели с представителями руководства компании Google — Марко Панчини, директором по взаимодействию с органами государственной власти в странах Европы,



На связь с депутатами Госдумы вышел Марко Панчини, директор компании Google по взаимодействию с органами государственной власти в странах Европы, Ближнего Востока и Африки

Ближнего Востока и Африки, YouTube, и Мариной Жунич, директором по взаимодействию с органами государственной власти «Google Россия». Причиной для видеовстречи стали аналогичные нарушения. Длительное время YouTube распространял в нашей стране запрещённую информацию — призывы к несовершеннолетним участвовать в несанкционированных митингах. А кроме того, к компании у нас накопилось немало вопросов и по другим поводам. В частности, по политической цензуре. В последнее время участились случаи блокирования ресурсами компании информации российских СМИ, в том числе заявлений официальных лиц о развитии ситуации с коронавирусом и предпринимаемых государством мерах по противодействию пандемии. Установлены многочисленные факты цензуры на видеохостинге YouTube в отношении материалов таких российских СМИ, как НТВ, «Россия 24», ТВЦ, RT, «Спутник», «Царьград», РИА «Федеральное агентство новостей» и многих других.

Не могли мы не привлечь внимания Марко Панчини и к странной аномалии в электронных картах на сервисах Google. На них, к примеру, чётко указана принадлежность острова Сардиния Италии, но при этом острова Итуруп, Кунашир, Хабомаи и Шикотан почему-то не обозначены как часть Сахалинской области России. Так же ошибочно оказался отображён Крым. Наша позиция однозначная: Крым должен быть обозначен на российской версии сервиса «Карты Google» не под нейтральным названием «Полуостров Крым», а под наименованием, соответствующим Конституции и законодательству Российской Федерации, — Республика Крым.

В ходе видеоконференции была продемонстрирована подборка материалов, размещённых на видеохостинге YouTube, которые вызвали возмущение российской общественности и серьёзно обеспокоили родителей. Так, уже за четыре дня до незаконной акции, намеченной на 23 января, детям внушали, что силы правопорядка будут не защищать граждан, а расстреливать мирных протестующих. За два дня до акции детей инструктировали, как противодействовать правоохранительным органам. При этом накануне незаконных акций YouTube прекратил распространение лишь 30% выявленных Роскомнадзором призывов к подросткам принять в них участие.

Кроме того, мы наглядно показали представителям компании, что при введении в поисковую строку жаргонного названия наркотиков, Google сам предлагает варианты запросов с применением специфической лексики наркоманов, и даже подсказывает выход на теневую площадку продажи наркотиков в Интернете. Представителям Google были заданы вопросы: знают ли модераторы компании русский язык, знакомы ли с нашим законодательством и способны ли они качественно модерировать запрещённый контент, не дожидаясь напоминания контролирующих органов. Марко Панчини пообещал серьёзно отнестись к данной информации, разобраться в том, почему так получается, и устранить нарушения.

Нашим визави мы разъяснили, что добиваемся лишь одного — исполнения и уважения наших законов. И я рассматриваю состоявшиеся телемосты как шаг к диалогу. Например,

с Google мы договорились продолжить общение в таком же режиме ориентировочно через полгода.

Что же касается принятого недавно закона «о приземлении» «IT-гигантов», то я уверен — в сочетании с жёсткой политикой Роскомнадзора, чередующего методы убеждения с многомиллионными штрафами для тех, кто не торопится привести свою деятельность в соответствие с российским законодательством, он даст хорошие результаты.

ЧТОБЫ НЕ УВЯЗНУТЬ В «МИРОВОЙ ПАУТИНЕ»

Несколько лет назад мы столкнулись с таким явлением в соцсетях, как «группы смерти», «Колумбайн-сообщества», игры «Синий кит», «Беги и умри» и другие. Рост числа самоубийств среди детей вынудил нас к поиску законодательных мер по блокировке такого опасного контента. Ряд поправок, внесённых в действующее в законодательство, позволил оперативно пресекать распространение информации о способах совершения самоубийства, призывов к суициду и иных форм вовлечения и принуждения детей к противоправным действиям. Введён ускоренный порядок ограничения доступа к любого вида запрещённой информации в случае её повторного размещения, то есть незамедлительно.

Меры по ограничению доступа к противоправному контенту в Интернете были приняты и в отношении рекламы наркотиков. Разработанный Комитетом по безопасности и противодействию коррупции и принятый Госдумой закон запрещает публиковать в СМИ и Интернете сведения о способах изготовления и местах приобретения новых потенциально опасных психоактивных веществ, например, спайсов. Кроме того, запрещена «пропаганда каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов или прекурсоров, новых потенциально опасных психоактивных веществ, растений, содержащих наркотические средства или психотропные вещества либо их прекурсоры».

Крайне важна, по нашему мнению, профилактика проявлений экстремизма и терроризма среди молодёжи, и в том числе в Интернете. При этом периодически встречаются случаи обеления и оправдания преступлений нацистов и коллаборационистов, которые происходят под личиной якобы реализации права на свободу выражения мнения. Такие действия вместе с глумлением над памятью погибших в Великой Отечественной войне вылились в какую-то необъяснимую ярость к движению «Бессмертный полк». Если честно, я не могу этого понять, в какой стране родились и где воспитывались люди, козыряющие портретами Гитлера и Власова, бравирующие своим хамским отношением к ветеранам. Что это, если не экстремизм? Нужны эффективные меры по предупреждению, пресечению и локализации проникновения таких идей в нашу страну. И одна из них предложена в нашем законопроекте, который предусматривает оперативную блокировку информации с оправданием экстремизма и терроризма. В марте он принят в первом чтении, работа над ним будет продолжена уже новым составом Государственной Думы.

В своём законопроекте мы предлагаем ограничивать доступ к такой информации по решению Генерального прокурора Российской Федерации или его заместителей. Сегодня уже действует механизм, по которому Генеральная прокуратура в случае выявления фактов призыва к осуществлению экстремистской или террористической деятельности обращается в Роскомнадзор с требованием принять меры по ограничению доступа к таким публикациям, а в случае переноса указанных материалов на другие интернет-ресурсы также ограничить к ним доступ. Это уже предусмотрено статьёй 15.3 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Этот же алгоритм действий предлагается и для блокировки так называемого «оправдательного» контента.

Глубоко убеждён: подобные публикации должны блокироваться как можно быстрее, так как они представляют прямую угрозу для подрастающего поколения, для безопасности наших детей. Подростки в силу возрастных особенностей наиболее подвержены негативному влиянию, поэтому наш законопроект направлен не только на повышение безопасности информационного пространства, но и на предотвращение радикализации несовершеннолетних. К сожалению, статистика свидетельствует о всё большей распространённости экстремистских идей среди населения, в основном, у молодёжи. Так, по данным Генпрокуратуры, количество выявленных в 2020 г. преступлений экстремистской направленности возросло на 42,4% и составило 833. Большинство преступлений указанной категории совершены с использованием сети «Интернет»: 396 (в 2019 г. — 261, рост на 34%).

Интернет даёт людям уникальные возможности для обмена информацией, получения образования, да и просто общения. И охватившая мир пандемия коронавируса лишь ускорила проникновение современных информационных технологий во все сферы нашей жизни. Но давайте признаемся, Интернет обладает и огромной разрушительной силой, если его использовать в преступных целях. Скорость распространения информации и широта охвата аудитории здесь ограничены лишь наличием у людей компьютеров и других гаджетов, подключённых к «мировой паутине».

* * *

Именно поэтому, выступая за свободу обмена информацией, мы являемся сторонниками идеи закрепить в международном праве нормы ответственного поведения в информационном пространстве. Предложения России о сотрудничестве в сфере информационной безопасности, обмене информацией о киберугрозах, сближении законодательных норм, принятых в различных государствах, ранее нашли поддержку на уровне стран-участниц БРИКС, ШОС и ОДКБ, поддерживаются многими государствами на уровне ООН. Развивая такое сотрудничество, важно последовательно совершенствовать наше национальное законодательство, делая информационное пространство максимально безопасным для российских пользователей. Это мы видим своей ближайшей задачей.

ИБ ФИНАНСОВОЙ СФЕРЫ: ЧТО ИМЕННО ХОЧЕТ ДОНЕСТИ ЦБ ДО УЧАСТНИКОВ РЫНКА

ПРАКТИЧЕСКИЕ ВЫВОДЫ ИЗ СТАТИСТИКИ
И АНАЛИТИКИ ПО ОПЕРАЦИЯМ БЕЗ
СОГЛАСИЯ КЛИЕНТОВ



Вадим УВАРОВ
директор
Департамента
информационной
безопасности Банка
России

«**О**бзор операций, совершённых без согласия клиентов финансовых организаций за 2020 год» опубликован Департаментом информационной безопасности Банком России в апреле 2021 года. В отчёте, предназначенном и профессионалам, и широкой аудитории, рассматриваются главные отраслевые тренды, анализируются самые важные и актуальные вопросы.

МАКСИМАЛЬНАЯ ПУБЛИЧНОСТЬ

Документ ориентирован как на профессионалов, так и на широкую массовую аудиторию, которой интересны и важны вопросы информационной безопасности финансового сектора. В этом его отличие от ранее опубликованного обзора «Основные типы компьютерных атак в кредитно-финансовой сфере в 2019–2020 годах», предназначенного главным образом для профессионалов информационной безопасности финансового рынка.

Основной посыл обзора операций, совершённых без согласия клиентов, таков: социальная инженерия остаётся главной угрозой деньгам клиентов финансовых организаций, хотя доля её снижается. Дается сигнал рынку, в первую очередь банкам, уделять ещё больше внимания информированию клиентов о рисках мошенничества. Говорится, каким инструментам и схемам атак, механизмам и каналам вывода денег нужно уделить приоритетное внимание.

Обзор широко презентуется. Раньше это делалось на Уральском форуме «Информационная безопасность финансовой сферы», на этот раз — из-за пандемии — на пресс-конференции в Москве. Конечно, далеко не все клиенты финансовых организаций подробно изучат обзор, но основные положения узнают из прессы, которая многое о нём сообщает. Через популярную подачу журналистами граждане, пользующиеся дистанционными финансовыми сервисами, узнают основные угрозы, вооружаются пониманием и знаниями, как не быть обманутым злоумышленниками.

Документ полезен всем группам клиентов финансовых организаций: сотрудникам бухгалтерий, индивидуальным предпринимателям и физическим лицам. Есть некоторая разница инструментария социальной инженерии, нацеленного

на каждую из этих групп. Специалисты могут понять общую картину и главные тенденции отрасли, руководители финансовых организаций — делать обоснованные выводы и принимать правильные решения.

Одна из свежих тенденций — переориентация атак мошенников с банковских карт на депозиты, текущие счета клиентов. Ноу-хау — схемы, при которых людей убеждают оформить кредит и перевести деньги на мошеннический счёт. Социальные инженеры заменяют тактику «от многих по чуть-чуть» принципом «от одного, но много».

Среди самых изощрённых, массовых и прибыльных инструментов «социальных инженеров» — телефонный звонок якобы из «службы безопасности банка». С конца 2020 года участились звонки злоумышленников от имени «правоохранительных органов».

АКТУАЛЬНЫЕ АТАКИ

К гражданам злоумышленники чаще всего обращаются посредством звонков по телефону. На юридических лиц они обычно ориентируют рассылки писем по электронной почте, в том числе содержащие вредоносное программное обеспечение, компьютерные вирусы.

Для юридических и физических лиц придумываются разные легенды. Гражданам сообщают о несуществующих проблемах с деньгами на их личных счетах, заведением дела в полицию... К юридическим лицам злоумышленники обращаются якобы от имени контрагентов и должностных лиц — налоговой службы, арбитражных судов.

Требуют под вымышленными предложениями срочно перечислить деньги по указанным реквизитам: оплатить счёт и т.п. Применяются как массовые, так и адресные рассылки с хорошо продуманной легендой, индивидуально ориентированным содержанием письма, оформленного бланками, логотипами, печатями.

Из клиентов финансовых организаций более уязвимы для социальной инженерии граждане, которые гораздо чаще попадают на уловки мошенников. Граждане, как правило, самостоятельно распоряжаются своими деньгами, но менее грамотны в вопросах информационной безопасности, чем сотрудники юридических лиц.

Вынудить сотрудников юридических лиц совершить перевод денежных средств злоумышленникам труднее. Как правило, в организации решение о финансовых транзакциях принимается не единолично. Если мошенническое предложение получил секретарь, для подтверждения транзакции нужно «добро» ещё от генерального директора и бухгалтера.

Кроме того, процедуры вывода денег со счетов юридических лиц сложнее, они состоят из большего количества операций. Например, неосторожный сотрудник открыл опасное электронное письмо и допустил заражение вирусом и своего компьютера, и корпоративной сети. Но в такой ситуации всё же остаётся время выявить и купировать эту атаку, предотвратить хищение.

У граждан, напротив, деньги очень быстро перечисляются на счета сообщников злоумышленников и обналичиваются. Поэтому физическим лицам, особенно пожилым гражданам, рекомендуется не спешить при сомнительных предложениях от якобы сотрудников банка или полиции. Лучше перед принятием решения выждать время, посоветоваться с родственниками, друзьями, самому перезвонить в банк или полицию,

ПРИОСТАНОВИТЬ И ВЕРНУТЬ

Часть ответственности за сохранность денег клиентов и противодействие злоумышленникам лежит, конечно, на финансовых организациях, в первую очередь на банках. Однако ст. 9 Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платёжной системе» позволяет банку не возмещать клиенту похищенные таким образом средства: если тот нарушил условия договора обслуживания. Например, когда клиент сообщил третьим лицам информацию, которая способствовала хищению денег.

Главный смысл методов социальной инженерии как раз в том и заключается, чтобы добиться от клиента сообщения таких данных, например номера банковской карты. Или в том, чтобы спровоцировать человека самого перевести деньги сообщникам злоумышленников.

Статистика показывает, что в 2020 году банки вернули клиентам только 11 % денежных средств по операциям без согласия клиентов. Возврат удавалось осуществить там, где хищения были вовремя приостановлены благодаря антифрод-процедурам или информационному обмену с ФинЦЕРТ. Деньги, которые злоумышленники успевали вывести со счёта клиента и обналичить, вернуть практически невозможно.

Случаи возврата денег клиентам по оспоренным транзакциям связаны, в частности, с нежеланием банков нести риски своей деловой репутации. Клиент, обманутый злоумышленниками, сообщивший данные своей банковской карты, может винить в случившемся банк, который не предотвратил и не приостановил хищение.

Одним из средств усиления банками защиты клиентов от социальной инженерии являются антифрод-системы, автоматизация выявления и приостановка подозрительных финансовых операций. Банки могут создавать и развивать

собственные системы или пользоваться услугами специализированных организаций. Антифрод-системы — одно из конкурентных преимуществ финансовых организаций в поддержании доверия клиентов.

ДОСТИЖЕНИЯ И НОВЫЕ РУБЕЖИ

Можно отметить улучшение защищённости информационных инфраструктур и клиентских сервисов финансовых организаций. Таковы результаты совершенствования систем управления информационной безопасностью, расширения перечня используемых средств защиты информации.

Растёт профессиональный уровень сотрудников подразделений информационной безопасности и информационных технологий. Важную роль играет успешное обезвреживание многих злоумышленников правоохранными органами разных стран.

Эффективность массовых рассылок злоумышленников значительно снизилась благодаря функционированию системы информационного обмена ФинЦЕРТ Банка России. Информация о любой новой рассылке включается в оперативный бюллетень и быстро становится известной всем финансовым организациям.

Если атакующим удаётся проникнуть в информационную инфраструктуру финансовой организации, то закрепиться до принятия защитных мер они не успевают. Их затраты на рассылку и подготовку атак оказываются напрасными.

Сократилась до минимума доля таргетированных, тщательно подготовленных атак «социальных инженеров» на банки. То же самое можно отметить в отношении целевых атак на клиентов, хотя юридические лица атакуются таким образом чаще, чем физические.

Осведомлённость клиентов финансовых организаций и умение применять правила кибербезопасности увеличиваются. Доля социальной инженерии в общем объёме несанкционированных операций снизилась с 68,6 % в 2019 году до 61,8 % по итогам 2020 года.

Стало нелегко найти клиента банка, который бы ничего не слышал про мошенников, использующих обзвоны по телефону и интернет. Однако психология человека такова, что учиться на чужих ошибках могут далеко не все. Даже зная о рисках мошенничества, люди часто не думают, что сами могут оказаться мишенью. Многим свойственно строить иллюзии, мол, обмануть могут кого угодно, но только не меня.

Зачастую злоумышленники застают жертву врасплох и требуют действовать незамедлительно — под влиянием эмоций, не думая. Поэтому крайне важно, чтобы работа по информированию граждан об актуальных угрозах мошенничества велась системно и постоянно.

* * *

Повышение защищённости от социальной инженерии — во многом результат информирования граждан со стороны правоохранительных органов, финансовых организаций и Банка России. Эта совместная работа должна продолжаться.

СЧАСТЬЕ ДЛЯ ВСЕХ!

КАК УНИФИЦИРОВАТЬ И СВЕСТИ К МИНИМУМУ МНОЖЕСТВО НОРМАТИВНЫХ ТРЕБОВАНИЙ К ИБ?



Василий ОКУЛЕССКИЙ
заместитель
начальника
службы ИБ банка
«Возрождение»,
кандидат
технических наук

Недавно коллеги из АРБ организовали и провели при поддержке уважаемой компании «ДиалогНаука» вебинар по ознакомлению с очередными требованиями Банка России по обеспечению информационной безопасности. Получилось хорошее мероприятие, но не буду его пересказывать, а поделюсь своими мыслями, которые зародились после его завершения.

Друзья мои, мы живём в интересное время. Не многим повезло так, как нам с вами. Мы не изучаем информационную безопасность, а создаём её, сами пишем эту увлекательную историю.

На наших глазах и нашими с вами руками создавались фундаментальные для финансовой отрасли основы защиты информации в форме сначала стандартов Банка России, а затем несколькими итерациями Положений БР мы перешли к российским стандартам — ГОСТам. Только перечисление СТОБРОВ, ГОСТов, МРок, Указаний и Положений заняло бы целую страницу. Не одно поколение авторов прошло эту школу писательства нормативки. Вдогонку

много прилетает к нам от наших партнёров из-за рубежа — ещё одна гора стандартов карточных платёжных систем со всего света, включая наши собственные, да ещё всякие SWIFTы и пр., а ведь мы не только реализуем эти требования, но ещё и сами принимаем активное участие в их разработке на основе нашего собственного опыта.

Но всё-таки основная проблема — в реализации требований, а гора их растёт.

За что это нам? Неужели нельзя было сделать что-то «одно на всех» и соответствовать «ему», а все остальные пусть доверяют! Давайте посмотрим картинку (рис. 1).

В банке, как правило, обрабатываются различные виды информации, к которым предъявляются различные требования по защите этих видов информации. Их пересечения очень условно можно поделить как на рис. 1.

Очевидно, что невозможно совсем разделить все эти виды информации на изолированные контуры. И невозможно строить несколько систем защиты информации. Естественно, что идеологически самый простой способ — объявить всю информации равнозащищённой, строить безопасность по самому высокому уровню защиты, какой найдётся в организации, и тогда вся информация будет защищена. Технически это очень дорогостоящая утопия, потому что надо будет научиться делить все системы по уровню защиты, научиться гарантированно разделять те сегменты сети, где обрабатываются данные одного уровня, и в каждом сегменте строить свою защиту. Но тогда, возможно, окажется, что принципы построения защиты в каждом сегменте могут значительно отличаться.

Проблема эта не новая, и её решение на каждом этапе развития ИБ было своё. Например, в начале 2010-х годов остро встал вопрос соответствия требованиям по защите персональных данных. Благодаря усилиям Банка России родилось знаменитое письмо четырёх, в результате банки, имеющие определённую оценку соответствия требованиям ЦБ, автоматически считались соответствующими требованиям по защите ПДн. Как это решилось? Были обозначены «кирпичи» из фундамента безопасности, которые надо было взять и вложить в свой «фундамент» (рис. 1).

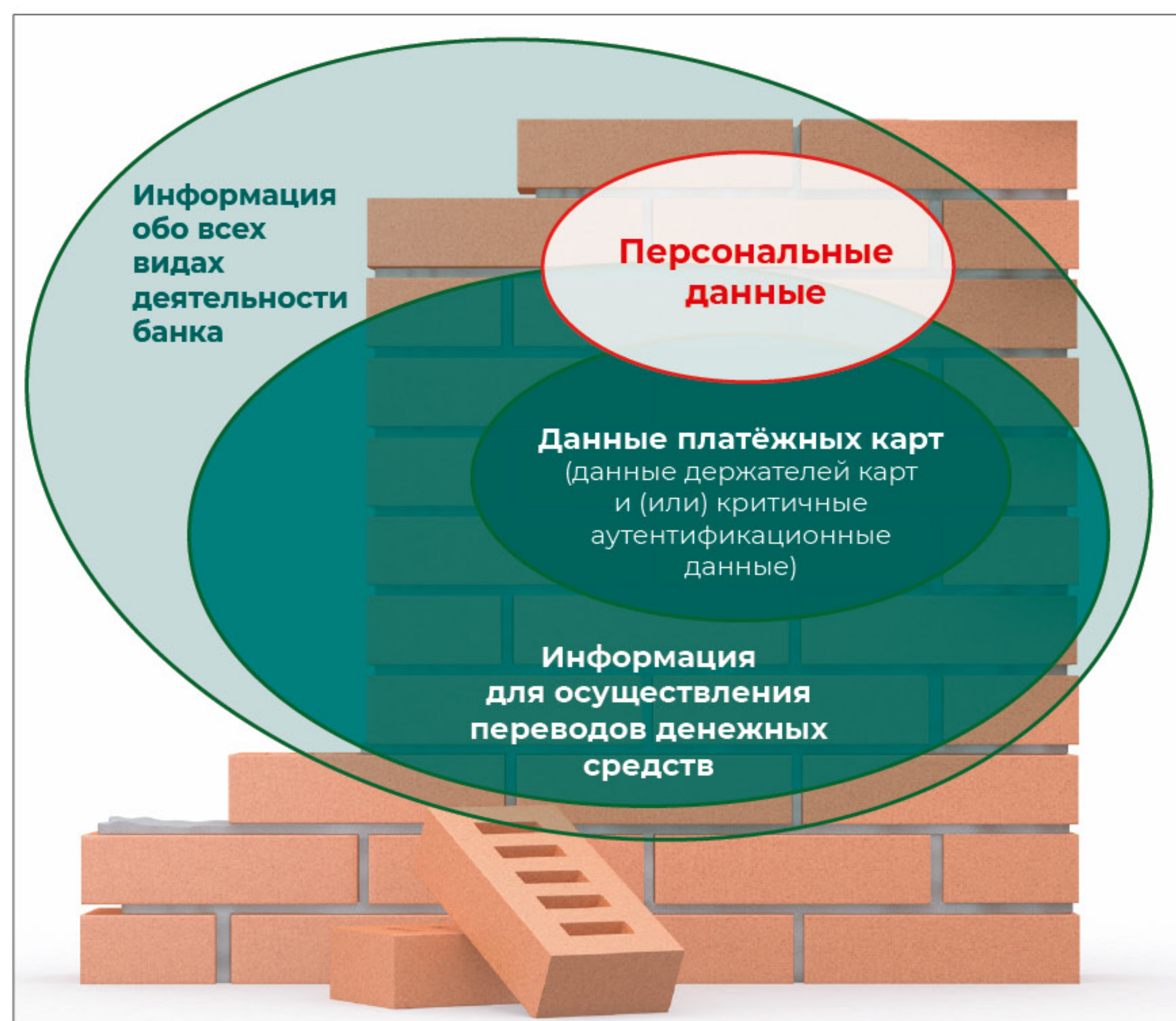


Рисунок 1. Области требований к защите информации

Сейчас, когда требований стало больше и они стали разнообразней, появилось новое видение, как строить безопасность: нам предложили набор «кирпичей» для строительства системы обеспечения ИБ — наборы организационных и технических мер в форме стандарта ГОСТ-Р 57580.1–2017 и правил оценки правильности «сбора этих кирпичей» ГОСТ-Р 57580.2–2018. Очень кратко это выглядит так: группы процессов объединены направлениями, внутри каждого из которых сгруппированы наборы организационных и технических мер:

- ◆ обеспечение защиты информации при управлении доступом;
- ◆ обеспечение защиты вычислительных сетей;
- ◆ контроль целостности и защищённости информационной инфраструктуры;
- ◆ антивирусная защита;
- ◆ предотвращение утечек информации, защиты машинных носителей информации (МНИ);
- ◆ управление инцидентами защиты информации;
- ◆ защита среды виртуализации;
- ◆ защита информации при осуществлении удалённого логического доступа с использованием мобильных (переносных) устройств.

Внутри каждого буллита есть свои 2–10–20–30–40 «подбуллитов», которые, собственно, и создают ту самую основу — «кирпичи» и правила обращения с ними, благодаря чему мы можем строить любую систему защиты информации. Всего набирается около 340 мер, каждая из которых может иметь организационную или техническую составляющую, либо не иметь её вовсе, в зависимости от целевого уровня защиты. **Для того чтобы разобраться с обилием кирпичей, предлагается использовать процессный подход для управления «стройкой» и последующей «эксплуатацией».**

Более того, если взять обобщённые требования МПС (см. врезку), то даже для их

реализации всегда можно набрать кирпичей из стандарта.

Если рассмотреть требования к типовым информационным системам банка — АБС, СДБО, CRM, процессинговые системы, системы отчётности, технологические системы и т.д., — то в общем случае требования начинают носить всё более унифицированный характер.

Иначе говоря, система защиты информации банка, правильно собранная из этих кирпичей на основе процессного подхода, будет соответствовать требованиям практически любого нормативного документа БР или МПС.

Все Положения БР теперь не формулируют непосредственно требования, а ссылаются на ГОСТ — возьми такой-то набор кирпичей и будет тебе хорошо. То есть в общем случае применение кирпичей необходимо как для платёжных, неплатёжных и просто технологических систем. Такой подход позволит унифицировать применяемые средства защиты для разных элементов банковской КИС и тем самым хоть немного облегчить участь ибэшников.

Совершенно очевиден следующий шаг — гармонизация этой «фабрики кирпичей» с техническими требованиями других стандартов. При таком подходе появление нового документа не будет вызывать очередной шок — не надо начинать всё сначала, а нужно просто проверить все ли кирпичи на месте, уложены ли правильно, либо где-то каких-то кирпичей не хватает и их надо будет «просто» добавить.

Отдельно нужно было бы взглянуть на управление жизненным циклом автоматизированных банковских систем, на ряд требований к выделению технологических участков и обеспечения их безопасности, на требование сертификации ФСТЭК отдельных видов ППО, на профиль защиты ППО.

Но это уже другой разговор.

Построение и обслуживание защищённой сети и систем

1. Установить и обеспечить функционирование межсетевых экранов для защиты данных держателей карт
2. Не использовать пароли и другие системные параметры, заданные производителем по умолчанию

Защита данных держателей карт

3. Обеспечить безопасное хранение данных держателей карт
4. Обеспечить шифрование данных держателей карт при их передаче через сети общего пользования

Программа управления уязвимостями

5. Защищать все системы от вредоносного ПО и регулярно обновлять антивирусное ПО
6. Разрабатывать и поддерживать безопасные системы и приложения

Внедрение строгих мер контроля доступа

7. Ограничить доступ к данным держателей карт в соответствии со служебной необходимостью
8. Определять и подтверждать доступ к системным компонентам
9. Ограничить физический доступ к данным держателей карт

Регулярный мониторинг и тестирование сети

10. Контролировать и отслеживать любой доступ к сетевым ресурсам и данным держателей карт
11. Регулярно выполнять тестирование систем и процессов обеспечения безопасности.

Поддержание политики информационной безопасности

12. Разработать и поддерживать политику информационной безопасности для всего персонала организации

НЕ ДАЙ НАМ БОГ ЖИТЬ В ЭПОХУ ПЕРЕМЕН

РАЗМЫШЛЕНИЯ ПОД СУРДИНКУ НА ТЕМЫ СТАТЬИ
В. А. ОКУЛЕССКОГО «СЧАСТЬЕ ДЛЯ ВСЕХ!»



Сергей ВИХОРЕВ
советник
Генерального
директора
ООО «ИТ-Экспертиза»

Проблема большого количества нормативных документов, поднятая автором, безусловно приводит многих к состоянию когнитивного диссонанса. Да, разобраться в этом сонме бумаготворчества наших регуляторов непросто. Но зачастую это вызвано не их количеством, а тем, что, к великому сожалению, сейчас в институтах не учат правильно читать нормативные акты, правильно их увязывать. И это беда не только тех иб-шников, кто сидит «на земле», но и проверяющих от регуляторов, которые вываливают список «на сорок листов» с нормативкой и, не вникая в их суть, требуют безоговорочного выполнения всех требований. Но вернёмся к статье. Один профессор, оценивая научную работу соискателя на учёную степень, как-то сказал: «Работа содержит много актуального и нового. К сожалению, всё актуальное — не ново, а всё новое — не актуально». Почему? Попробую объяснить.

ЭФФЕКТ ГАЗОКОСИЛКИ

Давайте подумаем, почему сейчас так много разных требований? Можно ли создать единые универсальные требования по безопасности информации, которые подходили бы каждому? Задача благородная, но невыполнимая. Нет, конечно, если всех подстричь под одну гребёнку, как траву на газоне, то, наверное, задача будет разрешима. Однако так не получится. Так же как нельзя найти два одинаковых дактилоскопических узора, принадлежащих разным людям, так нельзя найти и две одинаковые информационные системы. С одной стороны, они все разные и находятся в разных условиях, обрабатывают информацию разного рода, имеют разные угрозы безопасности информации, а значит, и требования к ним должны быть разные. С другой стороны, все эти системы используют одну и ту же инфраструктуру и, как оказывается, разделить их не так-то просто, даже на уровне приложений, так как информация между ними мигрирует.

Мы все прекрасно понимаем, что предметом защиты является информация (вернее, даже её

полезные свойства). Однако, как я уже однажды писал, в силу особенностей самой информации (её идеальной составляющей), точкой приложения усилий по обеспечению безопасности информации является окружение (среда), в котором она обращается, то есть инфраструктура и информационные технологии. При этом элементы инфраструктуры должны рассматриваться именно как факторы, влияющие на реализацию угрозы, а не как объект защиты¹. А из этого следует важнейший вывод: требования должны применяться именно к инфраструктуре и информационным технологиям, они должны быть безопасны и надёжны для объекта защиты.

Обратимся к классике. Что такое информационная система? Это совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств². Почему-то сейчас превалирует очень узкое трактование этого определения. Одна информация — одна информационная система. Вот и получается, что в организации появляется несколько информационных систем, обрабатывающих, например, защищаемые персональные данные: кадровая, бухгалтерия и ещё какая-нибудь, хотя на самом деле все они используют одну и ту же информационную технологию (например, платформу 1С), используют одни и те же базы данных, то есть, по своей сути, это всего лишь одна информационная система, решающая разные задачи. Ведь, наверное, нет идиотов, которые разворачивают две платформы 1С отдельно для бухгалтерии и кадров. А теперь, памятуя уже сделанный вывод, можно сказать, что требования должны предъявляться именно ко всей системе, использующей одну и ту же информационную технологию, а не к её отдельным элементам.

Регулятор выдвигает разные требования, предполагая, что у потребителя есть только

¹ С. Вихорев, А. Сычев, «Диалоги о безопасности информации или введение в основы построения систем безопасности информации», М., изд. «Медиа Группа „Авангард“», 2015.

² Федеральный Закон № 149-ФЗ, ст. 2, п. 3

одна специализированная система, так проще сформулировать требования. Именно этим и объясняется такое обилие различных требований. Но применять их надо с умом, с учётом того, какая информация обрабатывается, откидывая те нормы, которые покрывают друг друга, а не стараться выполнить и те и другие (как говорят: и нашим и вашим за рупь спляшем). Думать надо, правильно читать для чего нужны требования, анализировать, а этому, к сожалению, сейчас не учат.

Здесь на память приходит аналогичная ситуация с требованиями для ГИС³ и ИСПДн⁴. Какие требования применять, если ГИС ещё и обрабатывает персональные данные? «Земские» иб-шники мучались-мучались, терзаясь в когнитивном диссонансе, пока не вышло письмо от ФСТЭК России⁵, которое разъяснило, что меры по обеспечению безопасности персональных, установленные приказом ФСТЭК России от 18.02.2013 г. № 21, аналогичны мерам приказа ФСТЭК России от 11.02.2013 г. № 17 и поэтому достаточно руководствоваться только требованиями приказа № 17. И проблема была решена. Хотя, на мой взгляд, даже этих скромных усилий регулятора по разъяснению для особо непонятливых, что масло масляное не требовалось (посмотрите внимательно п. 21 приказа № 17: этап дополнения уточнённого адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в том числе в области защиты персональных данных). Просто исполнители не захотели читать положения приказа так, как они написаны и побоялись брать на себя ответственность. Но, в целом, опыт регулятора можно считать положительным и полезным. И, в принципе, такие разъяснения, сопоставляющие разные требования из уст регулятора позволили бы снизить градус проблемы большого количества разных требований.

³ ГИС — государственные информационные системы

⁴ Информационные системы персональных данных

⁵ Информационное сообщение от 15.07.2013 г. № 240/22/2637 по вопросам защиты информации и обеспечения безопасности персональных данных при их обработке в информационных системах в связи с изданием приказа ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и приказа ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

ЭПОХА БОЛЬШИХ ПЕРЕМЕН

Не могу не согласиться с тезисом автора о том, что мы живём в интересное время, что мы не изучаем информационную безопасность, а создаём её. Да, сейчас идёт очередной этап смены нормативных документов, переход на новый виток с учётом сложившихся обстоятельств. С одной стороны, это хорошо, с другой — трудно. Одновременно в ходу и уже устаревшая нормативка, например, СТО БР и ещё только разрабатываемая.

ИБ-шникам на земле трудно: неясно, чем руководствоваться, какова преемственность документов новой генерации, какова практика их применения. Да, к сожалению, это трудности переходного периода, трудности роста. Но они скоро уйдут! По крайней мере, я на это надеюсь.

Тенденция новой генерации нормативки вполне ясна: создать некий каталог «кирпичиков», как говорит автор статьи, из мер защиты и дать рекомендации как эти «кирпичики» складывать в той или иной ситуации. И этому есть объективные причины. Любая мера защиты направлена на устранение или ослабление угрозы безопасности информации. А сама угроза информационной безопасности не зависит от категории (значимости) информации и определяется объективными факторами и уровнем развития науки и технологий, то есть угроза, если она есть, для любой категории защищаемой информации будет идентична. А вот эффективность принятых мер защиты будет разной для разных категорий информации. Поясню, как всегда, «на яблоках». Пусть имеется Нечто (купюра в 100 рублей, завещание, бриллиантовое кольцо — неважно). Имярек хочет это Нечто украсть. Нечто можно спрятать: в коробочку из под конфет, закрыв на ключ в ящике стола, поместив в сейф. В данном случае мера защиты — это спрятать. А эффективность — коробочка, стол, сейф. И в зависимости от значимости предмета (кстати, это сущность весьма субъективна и зависит от владельца) прятать мы будем с разной эффективностью (надёжностью).

Именно по этому пути идёт и мегарегулятор кредитно-финансовой сферы — Банк России. Каталог мер защиты выпущен и застандартизирован⁶. А затем выпускаются ряд Положений для различных типов организаций, устанавливающих требуемый уровень защиты (читай: эффективность принимаемых мер) с отсылкой к действующему стандарту и определяющих

⁶ ГОСТ Р 57580.1–2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утв. приказом Федерального агентства по техническому регулированию и метрологии от 08.08.2017 года № 822-ст

общие положения по организации защиты⁷. Обратите внимание: никаких конкретных технических требований в этих документах нет! Правда, объективности ради надо сказать, что вопросы, связанные с защитой критической

⁷ ЦБ РФ Положение от 17.04.2019 г. № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»

⁸ ЦБ РФ Положение от 17.04.2019 г. № 684-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций»

инфраструктуры⁸, к каковой относятся организации кредитно-финансовой сферы, пока полностью не взаимодействуют с этими документами. Но, думаю, это явление временное, тем более что Банк России сейчас активно приводит отдельные документы к утверждённым стандартам.

Ну а что касается других документов типа Положений ЦБ № 382-П, № 379-П, № 381-П, № 607-П, Указаниям ЦБ № 2831-У, № 4793-У, № 4212-У и прочая, так это немного не о том (кстати, сюда можно отнести и серию СТО БР — этот стандарт применяется добровольно, то есть

⁸ Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

ЗАДАЧА ВЫГЛЯДИТ НЕПОСИЛЬНОЙ, НО...

ДОРОГУ ОСИЛИТ ИДУЩИЙ!



Александр ВЕЛИГУРА

председатель комитета по банковской безопасности Ассоциации российских банков, доцент Финансового университета при Правительстве РФ, кандидат физико-математических наук

Требования и рекомендации НПА по ИБ постоянно обсуждаются и совершенствуются. В частности, уже четвёртый год (с 01.01.2018) действует ГОСТ Р 57580.1¹ (далее — Стандарт), представляющий собой в основе своей каталог мер защиты для ссылок на него в нормативных актах Банка России. Этот анонсированный ранее подход направлен на сокращение объёма этих нормативных актов, повышение системности в задании требований к мерам защиты и уменьшение опасности появления ошибок и противоречий в задаваемых требованиях. Наверное, можно считать, что эта задача решается.

В то же время практика общения со специалистами банков показывает, что было бы неплохо уже сейчас кое-что уточнить.

1. Согласен с В.А. Окулесским в отношении гармонизации «кирпичей» с требованиями других документов. Как это сделать, не создавая проблем в общении с авторами этих документов? Опыт показывает («письмо шестерых», а не четверых, хотя регуляторов там действительно четверо), что даже в тех случаях, когда есть формальное согласие засчитывать «чужие» требования

(не своего ведомства), на местах это зачастую игнорируют. Автор своими ушами слышал заявление представителя областной структуры уважаемого ведомства, сделанное не где-нибудь в кулуарах, а с трибуны регионального совещания, что при проверках информация о соответствии требованиям каких-то там стандартов ЦБ во внимание приниматься не будет. Всё будет как всегда, а письмо? — а письмо — это не приказ.

В связи с этим возможно предложить там, где надо, детализировать «кирпичи» — разделить их на такие кусочки, чтобы из них можно было сложить как требования Стандарта, так и требования других НПА так, чтобы это не требовало доказательств.

Это помогло бы решить и другую задачу. Формулировки многих мер защиты в Стандарте допускают варианты их конкретной реализации, имеются ссылки на другие ГОСТы и нормативные документы (например, приказы ФСТЭК, профили защиты), в которых имеется определённый спектр требований. Регламентирование выбора конкретных требований из возможных, как представляется, существенно облегчило бы как работу «безопасников», так и контроль соответствия.

Тут сама собой вырастает следующая задача — а как это регламентировать? На основании анализа угроз, конечно. Заодно появляется ответ, как реализовать «адаптацию (уточнение) при

¹ ГОСТ Р 57580.1–2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер.

не носит обязательного характера, а является только «лучшими практиками»). Да, в этих документах есть вопросы, касающиеся защиты информации, но (!) это не технические требования и они применяются в строго ограниченной сфере своей компетенции. Это, можно сказать, подчёркивает важность решения вопросов обеспечения безопасности информации и контроля за ними в различных сферах деятельности кредитно-финансовых организаций, но не устанавливает каких-либо требований. Эти документы говорят КАК надо делать, а не ЧТО надо делать.

И ещё, контроль и мониторинг информационной безопасности, антифрод, обмен информацией об инцидентах, борьба с мошенническими сайтами и операциями — это, конечно,

очень близко к информационной безопасности, но выходит за рамки предметной области. Так что не надо всё смешивать в одну кучу. И если на службу информационной безопасности банка вешают ещё и антифрод, то это не означает, что антифрод является задачей информационной безопасности, это самостоятельная задача (оценка по определённым критериям правильная или неправильная транзакция — здесь нет защиты информации, здесь защита капиталов клиента от действий, совершённых от его имени) и регулируется она своими правилами.

А ревизия и систематизация всех действующих нормативных документов Банка России и их взаимоувязка действительно назрела. Может, Банк России прислушается...

необходимости выбранного состава и содержания мер защиты информации с учётом модели угроз и нарушителей безопасности информации финансовой организации» (п. 6.3 Стандарта). Один вопрос тянет за собой следующий — а кто и как будет оценивать адекватность модели угроз? Нужны какие-то рекомендации и типовые модели (прототипы). Основа есть².

Как всё это увязать вместе? С точки зрения возможности наиболее полного учёта угроз и индивидуализации подбора требований безопасности перспективным представляется использование подхода, реализованного в «Общих критериях»³, где в соответствующие документы, помимо требований, включаются рассматриваемые угрозы и проводится обоснование включения требований с точки зрения противостояния угрозам. Впрочем, это тема отдельного разговора.

2. Здесь хотелось бы затронуть ещё такой вопрос. Мы молчаливо исходим из того, что представляем себе требования (разных регуляторов)

² Методический документ. Методика оценки угроз безопасности информации. Утверждён ФСТЭК России 5 февраля 2021 г.

³ ГОСТ Р ИСО/МЭК 15408–2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

ГОСТ Р ИСО/МЭК 15408–2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности.

ГОСТ Р ИСО/МЭК 15408–2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности.

ГОСТ Р ИСО/МЭК ТО 19791–2008 Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем.

во всём объёме, и дело только в том, как их экономно, но правильно покрыть мерами защиты.

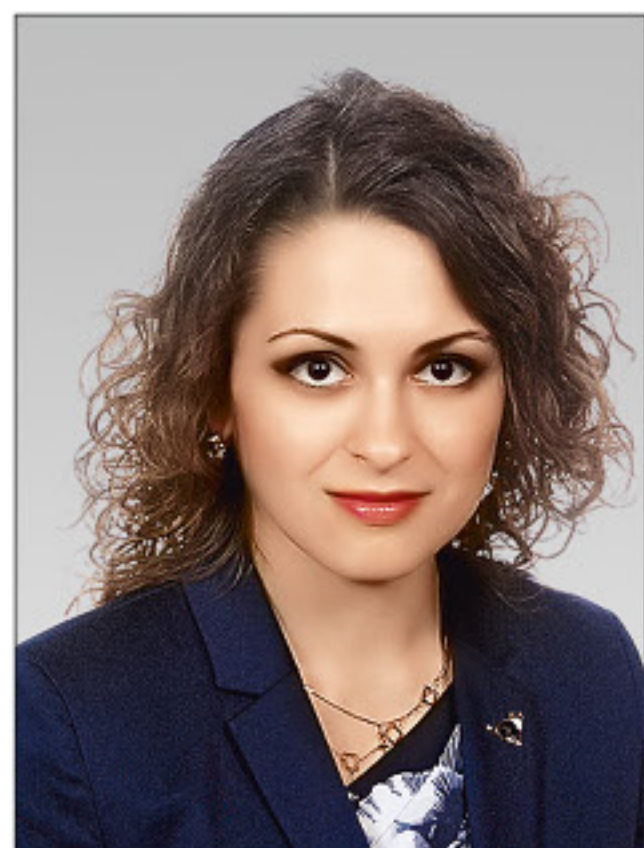
А какие вообще есть требования (по ИБ/защите информации) к финансовым организациям? Вроде бы все (специалисты) о них знают. НО!

Чуть более 5 лет назад по заказу одного крупного российского банка была сделана попытка составить перечень всех обязательных требований, относящихся к ИБ, содержащихся в НПА, распространяющихся на банк. В результате выяснилось, что только содержащих такие требования документов разного уровня — от федеральных конституционных законов до ведомственных актов — около ста двадцати! (на тот момент). Конечно, они имели разный объём и содержание требований, но тем не менее. Плюс ещё полторы-две сотни стандартов, на многие из которых имеются ссылки. Число самих требований вообще привести затруднительно. Перечень органов власти, имеющих те или иные права в отношении защищаемой информации (в банке), тоже оказался больше, чем представлялось вначале. Конечно, далеко не все они имеют право устанавливать требования, но, например, могут запрашивать ту или иную информацию, подлежащую защите по закону. Нужно знать, какие из этих запросов законны, при каких условиях и т.п.

За прошедшие годы число этого всего только увеличилось. Динамика впечатляет.

Если уж пытаться ответить всем требованиям, то есть смысл уточнить, что значит «все», и иметь это хотя бы в качестве ориентира.

Коллеги! Всё это выглядит неподъёмно и, может быть, даже фантастично. Но ведь многого из того, что есть сейчас, тоже ещё недавно не было... Дорогу осилит идущий!



**Екатерина
РАЧКОВА**

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

РУБИТЕ СПЛЕЧА!

ДЕЛАЙ ЧТО ДОЛЖНО, И БУДЬ ЧТО БУДЕТ

«**L**EGO» информационной безопасности (ИБ), безусловно, мощный, гибкий, востребованный, актуальный инструмент, позволяющий оптимально решать задачи управления рисками ИБ при должном уровне зрелости и осознания соответствующих процессов в организации.

Однако в этом «конструкторе» не всё ладно с инструкциями. Иначе говоря, можно строить всё правильно, а на выходе получить гибрид «ежа с ужом» и прийти к неутешительному расхолаживающему выводу: что ни делай, что-нибудь да нарушишь. И в больших данных этих проблем не избежать, поскольку данные-то всё тех же категорий (банковская тайна, персональные данные и др.), только их много, они разрознены и не структурированы.

Чтобы этого избежать и не обесценить «кирпичики», какие-то гордые узлы придётся рубить сплеча.

Необходимо прояснить вопрос о возможности использования облачных технологий по схеме «инфраструктура как услуга» (или сторонних ЦОД аналогичным образом) для обработки информации, относящейся к категории банковской тайны. «Аутсорсинг» вычислительных мощностей критически важен как для системообразующих, так и для малых кредитно-финансовых организаций (для первых — ввиду масштаба деятельности и объёма обрабатываемых данных, для вторых — ввиду высоких издержек на должное обслуживание такой инфраструктуры). На данный момент круг лиц, которые могут легитимно получить доступ к банковской тайне, определён статьёй 26 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности». При этом, если фактически для обработки банковской тайны арендуются вычислительные мощности, никогда нет полной гарантии (иначе говоря, всегда есть ненулевые остаточные риски), что к этой информации не получат доступ третьи лица из числа администрирующего и обслуживающего персонала арендованной инфраструктуры,

хотя бы на физическом уровне семиуровневой модели OSI.

Крайне важно определить, где проходит граница между персональными данными клиента и его банковской тайной. Действующее законодательство не содержит чёткого определения понятия «банковская тайна». Содержание банковской тайны вводится как статьёй 857 Гражданского кодекса РФ, так и статьёй 26 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности». ГК РФ гарантирует тайну банковского счёта, банковского вклада, операций по счёту и сведений о клиенте. Закон «О банках и банковской деятельности» гарантирует тайну об операциях, о счётах и вкладах своих клиентов и корреспондентов, об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону. При этом Центральный банк Российской Федерации в своих разъяснениях¹ указывает на принадлежность банковской тайны к персональным данным. Это влечёт за собой значительное ужесточение требований по защите банковской тайны (которые на самом деле явно ни законом, ни уполномоченными регуляторами не определены), вплоть до необходимости применять сертифицированные средства криптографической защиты при передаче персональных данных по каналам связи общего пользования, к которым относится сеть Интернет. Это коснётся, в частности, иностранной криптографии, применяемой при реализации дистанционного банковского обслуживания (ДБО), и чтобы ДБО через личный кабинет или приложение на мобильном устройстве с передачей данных через защищённый протокол не оказалось вне закона, придётся открывать дискуссию с проверяющим на тему «что есть СКЗИ, а что просто какие-то преобразования», которая ещё неизвестно к каким результатам приведёт.

¹ См. письмо Департамента банковского развития Центрального Банка Российской Федерации от 29.09.2014 № 41-2-2-8/1757 Межрегиональной общественной организации на запрос от 29.07.2014 (<https://cbr.ru/StaticHtml/File/50624/140925.pdf>).

Есть нестыковки в вопросах доступа к банковской тайне, прямо не связанных с информационной безопасностью, но существенно влияющих на эффективность противодействия мошенничеству в отношении целой категории банковских клиентов. Согласно статье 26 ГК РФ, дети 14–18 лет считаются частично дееспособными и могут совершать сделки только с разрешения законных представителей (родителей, опекунов, попечителей и т.д.) за исключением случаев, указанных в части 2 этой статьи (дети 14–18 лет самостоятельно без согласия родителей могут распоряжаться своим заработком, стипендией и иными доходами, осуществлять права автора, вносить вклады и распоряжаться ими). Дебетовые карты по своей сути не вклад, однако к ним регулярно применяется статья 834 ГК РФ, где указано, что к отношениям банка и вкладчика по счёту, на который внесён вклад, применяются правила о договоре банковского счёта (глава 45), если иное не предусмотрено правилами указанной главы или не вытекает из существа договора банковского вклада. Так, требования к защите банковской тайны лишают родителей возможности контролировать использование ребёнком открытой на его имя дебетовой карты, в частности, получать выписки по операциям по ней. Банк России также отмечает², что вопрос заслуживает внимания, и разъясняет, что положения пункта 3 статьи 834 ГК РФ о том, что к отношениям банка и вкладчика по счёту, на который внесён вклад, применяются правила о договоре банковского счёта (глава 45 ГК РФ), не предполагают распространения правил о договоре банковского вклада (глава 44 ГК РФ) на отношения, связанные с заключением договора банковского счёта. Кроме этого, ГК РФ допускается предоставлять информацию, составляющую банковскую тайну, не только клиентам, но и их законным представителям.

В настоящее время Центральный банк РФ запросил в Минпросвещения разъяснения по вопросам определения «объёма дееспособности несовершеннолетних в возрасте от 14 до 18 лет и пределов правомочий их законных представителей». По результатам консультаций регулятор планирует издать рекомендации для банков.

Смежная проблема — неопределённости в вопросе, на основании каких документов (нотариально заверенной доверенности или согласия, заверенного собственноручной под-

В настоящее время Центральный банк РФ запросил в Минпросвещения разъяснения по вопросам определения «объёма дееспособности несовершеннолетних в возрасте от 14 до 18 лет и пределов правомочий их законных представителей». По результатам консультаций регулятор планирует издать рекомендации для банков

писью или её аналогом) можно считать лицо представителем субъекта в контексте возможности передачи ему банковской тайны субъекта. В статье 857 ГК РФ речь идёт о представителях субъекта [банковской тайны], а в уже упомянутых разъяснениях Банка России указывается, что передача информации, составляющей банковскую тайну физического лица, третьим лицам (за исключением лиц, упомянутых в ст. 26 Федерального закона «О банках и банковской деятельности», которые имеют право доступа к указанной информации в случаях и в порядке, предусмотренных этой статьёй) допускается при наличии письменного согласия этого физического лица. Данная позиция также подтверждается судебной практикой³.

А ВРЕДНЫЕ СОВЕТЫ БУДУТ?

И в завершение — самый высокорисковый «вредный совет». Но чтобы бороться с противником его же методами и не быть при этом связанным по рукам и ногам, необходимо законодательно определить границы этичного (белого) хакинга. На данный момент в российском законодательстве нет чётких определений, какие именно действия по работе с сетевыми ресурсами уголовно наказуемы. УК РФ предусматривает наказание за взлом чужой инфраструктуры по трём статьям (ст. 272, 273, 274), которые грозят не только штрафами, но и реальным сроком за неправомерный доступ к компьютерной информации, распространение вредоносного кода и нарушение правил хранения, обработки и передачи информации. Программы поощрения поиска уязвимостей (bug bounty) отдельных компаний решают данную проблему только частично.

² https://arb.ru/b2b/news/tsb_mozhet_vvesti_roditelskiy_kontrol_za_schetami_podrozkov-10471748/

³ См. Постановление Шестого арбитражного апелляционного суда от 14.02.2013 № 06АП-41/2013 по делу № А73-12065/2012.

НОВАЯ ЭПОХА ЭЛЕКТРОННОЙ ПОДПИСИ

СИГНАЛЫ РЫНКА ДОСТИГЛИ ЦЕЛИ



Андрей СТЕПИН
заместитель
генерального директора
Компании «Актив»

Изменения планетарного масштаба, которые коснулись каждого из нас, породили резкий рост мобильности во всех сферах нашей жизни. Только ленивый не говорит сегодня об актуальности тренда удаленной работы и стремительно развивающихся беспроводных технологиях. Ведь в совокупности они помогают бизнесу адаптироваться к новым реалиям — обеспечивают личную безопасность сотрудников при поддержании непрерывности бизнес-процессов. Однако у каждой медали есть обратная сторона. Речь идет о растущем количестве уязвимостей и угроз, которым подвергаются как корпоративные информационные системы, так и персональные данные граждан. Логично, что в такой ситуации в современном мире потребность в обеспечении кибербезопасности уже легла в фундамент пирамиды Маслоу, наряду с безопасностью физической. О том, как в эти интересные времена в Компании «Актив» создают новые продукты для строгой аутентификации и электронной подписи, мы побеседовали с заместителем генерального директора Компании «Актив» Андреем Степиным.

— Насколько быстро происходит сегодня смена ключевых технологий, лежащих в основе развития продуктовых линеек?

— Начнём с того, что технологический цикл существенно зависит от специфики продукта. В сфере ИБ есть корпоративные решения, которые не меняются в течение десятилетий. И это нормально. Однако, продукты для массового использования однозначно

требуют инновационных технологий в основе.

Компания «Актив» создает именно такие продукты — они предназначены для очень широкой аудитории, от школьников с электронным дневником до бухгалтеров преклонного возраста. Технологическая разница поколений сейчас такова, что любое решение, претендующее на массовость, должно быть достаточно простым в использовании, однако постоянно усложняясь внутри. Очевидный пример — путь банковской карты. Десятилетиями использование банковской карты сводилось к снятию оттиска карты и собственноручной подписи клиента. Затем магнитная полоса сделала карту чуть удобнее и технологичнее. И, когда, наконец, в картах появился защищённый чип, весь мир переучился не проводить магнитной полосой, а взаимодействовать с контактным микроконтроллером. Разумеется, эта технология до сих пор востребована, но по-настоящему массовым и удобным способом оплаты стал канал NFC. Причём, обратите внимание, как быстро пользователи прошли путь от прикладывания карты к терминалу до использования смартфонов и умных часов. Именно на технологию беспроводной передачи данных NFC, а также на технологию Bluetooth Low Energy, пал наш выбор при создании новой линейки Рутокен ЭЦП 3.0.

— Какие изменения в запросах клиентов стали катализаторами для появления продуктов линейки Рутокен ЭЦП 3.0?

— В глобальном плане клиенты всегда хотят одного: проще, быстрее, доступнее. Причём в достаточно широком смысле. Как уже было сказано,

очевидный тренд последних лет — повышенный запрос на мобильность. Привычки клиентов меняются: смартфоны и планшеты становятся базовым инструментом практически во всех сферах нашей жизни. Добавьте к этому ставшую привычной удалённую работу на дому или в коворкингах — и вот он, практически идеальный шторм для сферы ИБ.

В то же время повышенная мобильность создает множество новых рисков и угроз. Защищать конкретное рабочее место и инфраструктуру, в которой оно находится, оказалось уже недостаточно. Пришло время учиться защищать свои транзакции в условиях удаленной работы в мобильной среде. Поэтому современный криптографический токен просто обязан соответствовать новым реалиям. Рутокен, например — это самый настоящий ключ к финансам и собственности организации.

С одной стороны, регуляторы рынка в лице Минцифры, ФСБ, ФСТЭК и ЦБ РФ также работают на опережение, предъявляя все новые требования к повышенной защищённости. И неизвлекаемые криптографические ключи, отдельные аппаратные устройства для электронной подписи и шифрования — это лишь верхушка айсберга. Компания «Актив» всегда учитывала в своих разработках требования регуляторов, одновременно понимая и «бизнесовые» чаяния клиентов. И, конечно, сейчас, в процессе эволюции федерального закона «Об электронной подписи», эти вызовы представляются нам довольно серьёзными.

С другой стороны, мы понимаем, что мало кто хочет жертвовать удобством в пользу защищённости. Отсюда и родились решения, позволяющие совершать

криптографические операции по удобному каналу NFC, с построением защищённых ГОСТ TLS каналов связи к государственным сервисам, и продукты для усиленной криптографической защиты ценной информации и работы «на удалёнке», с чем бы она ни была связана.

— **Как вы улавливаете сигналы рынка, чтобы затем преобразовать их в новые продукты для электронной подписи с принципиально новыми характеристиками?**

— Мы постоянно находимся в мощном информационном потоке. Во-первых, это отзывы нескольких миллионов пользователей наших продуктов, которым мы очень благодарны за обратную связь и обращение в техподдержку. Стараемся слышать не только тех, кто платит, но и тех, кто использует продукт. Во-вторых, это мнения и «хотелки» наших технологических партнёров, внедряющих и интегрирующих наши продукты со своими решениями. И, в-третьих, это информация об изменениях законодательства, уязвимости облачных технологий и постоянные новости об утечке баз данных с паролями и персональными данными. Собираем всё воедино, и сразу становится очевидно, что рынок созрел для нового технологического витка. Те тренды, которые сегодня воплощены в линейке Рутокен ЭЦП 3.0, мы в Компании «Актив» частично предвидели еще пять лет назад. Все-таки сложные программно-аппаратные комплексы для криптографической защиты не могут быть созданы за несколько месяцев. А затем — глобальная пандемия и желание нашего государства быть на острие кибербезопасности еще больше катализировали процесс. Сертифицированные решения, работающие с криптографией через бесконтактные интерфейсы, еще несколько лет назад казавшиеся утопией, сегодня стали необходимостью.

— **Известно, что при разработке продуктов зачастую приходится отказываться от определённых характеристик, чтобы получить экономически целесообразный продукт (либо более простой для пользователя). Как вы решали эту задачу?**

— Создавая новое, порой приходится жертвовать старыми проверенными технологиями. В новой линейке

Рутокен ЭЦП 3.0, например, пришлось отказаться от RFID-меток. На смену им пришла технология NFC, открывающая доступ к криптографической аутентификации в системах контроля и управления доступом (СКУД). Теперь это не просто метка с предзаписанной идентификационной информацией. NFC дает полноценный доступ к защищенному смарт-карточному микроконтроллеру и стойкой криптографии. Это принципиально иной уровень защищённости.

Нас не пугало, что пока лишь небольшой процент производителей СКУД поддерживает технологию NFC. Ведь нам пришлось отказаться от существующего решения в пользу аутентификации будущего. Компания «Актив» сейчас сотрудничает и проводит подготовительную работу с партнерами и ключевыми игроками рынка строгой аутентификации и электронной подписи. Мы убеждены, что устаревшие технологии уйдут из мейнстрима буквально за год-два.

Кстати, отдельной и крайне сложной задачей оказалось разместить антенну для бесконтактного питания микроконтроллера внутри небольшого USB-токена. Но у нас получилось добиться практически недостижимой кроссплатформенности — токены работают с любым смартфоном или планшетом, предлагаемым на рынке, поддерживаются все существующие настольные и мобильные платформы. Учитывая, что итоговый продукт должен был стоить недорого, то местами задача казалась невозможной. Вот это стало чрезвычайно сложным вызовом.

— **Ранее обсуждалось, что программные продукты будут вытеснять ПАК. На деле мы видим обратный процесс. Как вы прокомментируете этот тренд?**

— Программные продукты неотделимы от аппаратной части: софт не запускается в вакууме, ему в любом случае нужен кусочек кремния. И сейчас мы имеем весьма уникальную ситуацию на рынке «железа»: с одной стороны, это глобальный дефицит полупроводников, а с другой — потрясающая производительность чип-мейкеров, когда создатели микросхем реально бьют все рекорды. За первые пять месяцев 2021 года в одном только Китае было промышленно

произведено более 140 миллиардов чипов. То есть среднегодовые темпы роста превысили показатели 2020 на 48%. Аппаратная часть нужна всем!

Действительно, в какой-то момент казалось, что даже в сфере ИБ облачные решения и специализированный софт для смартфонов смогут заменить отдельные ПАК. Реальность же рассудила иначе: аппаратное решение априори более защищённое, пользователи привыкли доверять именно физическим артефактам. Учетная запись в облаке может быть скомпрометирована, закрытые криптографические ключи, отданные на хранение третьей стороне, подвергаются слишком большому риску утечки. Персональный ПАК при этом дает одновременно возможность личного контроля, ощущение защиты и реальную высокую защищенность.

Не стоит слепо полагаться на программное обеспечение и облачные технологии, когда речь идёт о безопасности ваших финансов, имущества и в целом цифровой личности.

— **Предвидя тренды ближайшего десятилетия, какими Вы видите продукты Рутокен?**

— Технологии дарят нам небывалую свободу: уже сегодня мы можем удаленно, с помощью смартфона, управлять умным домом, в то время как государственные информационные системы управляют умным городом. Но, чем больше удобства и свободы нам дают технологии, тем больше уязвимостей они несут. Предвижу, что в мире, где можно дистанционно включить плиту в вашем доме, переключить фазу светфора на улице или получить доступ к миллионам камер видеонаблюдения, потребность в строгой аутентификации и криптографической защите будет только расти.

Уже сейчас продукты Рутокен проникают во всевозможные АСУ ТП предприятий, защищая межмашинное взаимодействие от хакерских атак. Крипточипы устанавливаются в приборы учёта электричества и воды, помогая безопасно передавать данные и беречь ценные ресурсы. Решения Рутокен для интернета вещей в ближайшее десятилетие обеспечат защиту даже в невидимых для большинства людей сферах нашей жизни.



Павел МЕЛЬНИЧЕНКО

технический директор SafeTech

РЕАЛЬНОСТЬ, ПОХОЖАЯ НА МИФ

ПРОСТАЯ ЭЛЕКТРОННАЯ ПОДПИСЬ — БОЛЬШЕ, ЧЕМ КОДЫ!

Знали ли вы, что простая электронная подпись (ПЭП) может быть разной и, более того, по уровню безопасности она может быть ничуть не ниже и даже выше, чем усиленная неквалифицированная электронная подпись (УНЭП)? А в вопросе юридической значимости простая ЭП и УНЭП также могут быть эквиваленты? Миф это или реальность?

На сегодняшний день довольно прочно устоялась парадигма, что простая ЭП — это исключительно ОТП-коды, передаваемые на мобильные устройства через SMS и PUSH-каналы, либо постоянные пароли. Действительно, когда только появилось деление на виды электронной подписи, простая ЭП разрабатывалась по принципу простоты и удобства: человек получает код себе на устройство, вводит его и что-то подписывает. А в итоге этот метод подписания создал пространство для бессчётного количества атак на физических и юридических лиц в банковском сегменте.

О технической стороне «безопасности» (именно в кавычках) ОТП-кодов сказано уже много — они подвержены фишингу; не обеспечивают целостность и авторство транзакции; если речь идёт о SMS и PUSH-уведомлениях — элементарно перехватываются почти на всех этапах передачи и непосредственно в устройстве.

Юридическая значимость «кодилов» тоже весьма сомнительна. Хороший

юрист вместе с техническим специалистом легко докажут, что отправленный по SMS или PUSH код не является персонифицированной информацией и доступен неограниченному кругу лиц ещё до получения его адресатом. Судебные прецеденты таких решений общеизвестны.

Отдельной головной болью является уязвимость ОТП-кодов социальной инженерии.

Сегодня мошенники без труда получают всю информацию о клиентах банков — Ф. И. О., номер телефона, данные банковских карт, остатки по счетам, историю операций. И для монетизации всего этого объёма информации им недостаточно только одной составляющей — одноразового кода из SMS или PUSH-уведомления. И, если это не техническая атака, в ход идёт социальная инженерия.

Мошенники, стоит признать, отличные психологи: они разработали большое количество методик, как заставить человека продиктовать нужные цифры. Но все эти методики основаны на простейшей механике — ввести человека в стресс, пообещать помочь избежать губительных последствий и, в качестве промежуточного шага, попросить сообщить код. И человек делает это на автомате, диктуя код прямо из шторки уведомлений смартфона, не вникая в содержимое сообщения.

То есть для того, чтобы кардинально снизить уровень успешности

социальной инженерии, этот шаблон необходимо сломать. И для начала необходимо избавиться от одноразовых кодов, чтобы у пользователя не было возможности что-то кому-то продиктовать. Вроде бы выход вполне очевиден: отказаться от простой ЭП и перейти на использование УНЭП или КЭП. Но и здесь возникает сложность: КЭП очень строго регулируется законодательством, и выдать её всем физическим лицам, мягко говоря, непросто (читай: дорого). Остаётся УНЭП.

УСИЛЕННАЯ НЕКВАЛИФИЦИРОВАННАЯ ПОДПИСЬ В НАШИХ РЕАЛИЯХ

Прежде всего предлагаем детально разобраться, что говорит законодательство. Согласно п. 3 ст. 5 Федерального закона 63-ФЗ, УНЭП «получена путем криптографического преобразования...» и «создается с использованием средств электронной подписи...»

В Постановлении Правительства РФ от 16 апреля 2012 г. № 313 разработана, а также внедрение шифровальных и криптографических средств обозначены как работы, которые *подлежат лицензированию*.

Если компания-разработчик получает лицензию, то она обязана выполнять требования к лицензиатам, в том числе по разработке тех самых криптографических средств. Одним из руководящих документов в этой области является ПКЗ-2005, где прописана

рекомендация использования *национальных стандартов* при разработке криптографических средств.

Более того, если работа предполагается в банковской сфере, то есть Положение Банка России 683-П, которое говорит следующее: «в случае если кредитная организация применяет СКЗИ российского производства, то СКЗИ должны иметь сертификаты соответствия федерального органа исполнительной власти в области обеспечения безопасности».

Путём несложных умозаключений получаем следующее: если кредитная организация использует средства ЭП для УНЭП российского производства, то это должны быть сертифицированные средства, работающие с ГОСТ-алгоритмами. А это, в свою очередь, мало чем отличается от «зарегулированной» КЭП, что «убивает» идею простоты использования ЭП.

Если использовать УНЭП и следовать букве закона, то её применение в ряде цифровых платёжных каналов становится сложным, дорогим и просто неудобным для клиентов.

Что интересно, при использовании СКЗИ (средства ЭП) нероссийского производства такого требования нет.

СЛЕДУЕМ ЗАКОНУ И ТРЕБОВАНИЯМ БИЗНЕСА

Главные требования бизнеса к подписанию и подтверждению действий в цифровых каналах можно обозначить тремя пунктами.

Во-первых, это должно быть удобно и мобильно: все устали от ввода «коди-ков», дополнительных устройств и привязки к рабочему месту.

Во-вторых, должен обеспечиваться высокий уровень безопасности, как минимум на уровне УНЭП.

В-третьих, это должно быть экономически эффективно (даже средний банк тратит на рассылку SMS-кодов десятки миллионов рублей в год).

И здесь сам собой напрашивается вопрос: а что если реализовать все функции безопасности по принципу УНЭП, но назвать получившееся решение простой ЭП?

И снова обратимся к 63-ФЗ. Статья 9 описывает использование простой электронной подписи и говорит о том,



что простая ЭП также имеет ключ, который применяется в соответствии с правилами, предусматривающими определение лица, подписавшего документ, и обязывающими соблюдать конфиденциальность этого ключа. Очень похоже на «закрытый» ключ при использовании криптографии, не так ли?

Статья 6 говорит о том, что условия признания электронных документов должны быть описаны в соглашении между пользователем и оператором, например, информационной системы, то есть между двумя участниками. Опять же такое соглашение должно

быть подписано и при использовании УНЭП.

Резюмируем: получается, что по законодательству простая ЭП и УНЭП равны — у них есть ключ ЭП и двустороннее соглашение, определяющее порядок проверки подписи и разрешение конфликтных ситуаций.

Следовательно, мы можем использовать простую ЭП со всеми признаками УНЭП, кроме использования сертифицированных криптосредств, но не называть её УНЭП. Тем самым мы получим удобное, безопасное и экономически эффективное средство электронной подписи.

КАК РЕАЛИЗОВАТЬ «ПРАВИЛЬНУЮ» ПРОСТУЮ ЭП?

Реализация «правильной» простой ЭП требует следующего порядка действий:

Первое. Берём устраивающее нас решение для формирования электронной подписи — безопасное и удобное, которое реализует контроль авторства и целостности, а также неотказуемость. Оно должно удовлетворять как минимум следующему списку требований.

- ♦ Подпись вырабатывается только на устройстве клиента. То есть не должно быть генерации кода подтверждения на стороне банка и его отправки через агрегаторов/операторов.

- ♦ Должен обеспечиваться контроль целостности и авторства транзакции с доказуемой надёжностью. Другими словами, математические алгоритмы электронной подписи (ГОСТ, ECDSA и др.) обеспечивают нужные свойства. Отправленная SMS и «прилепленная» к ней сноска в договоре, что «доставленная SMS является доказательством авторства», — не обеспечивает.

- ♦ Должна выполняться визуализация документа перед подписанием, чтобы пользователь точно понимал, что именно он подписывает. «Безымянный» кодик в сообщении «123456 — Ваш код подтверждения» вовсе не отвечает на вопрос «Я перевожу деньги на безопасный счёт?» или «Я перевожу все свои деньги гражданину Вазгену?»

- ♦ Реализация решения должна удовлетворять всем современным практикам в области безопасности: по хранению ключей, по защите данных, по противодействию различным техническим и нетехническим атакам и т.д.

- ♦ Пользователь не должен испытывать неудобства при работе: с мобильного устройства, в роуминге, в офлайн-режиме, на смарт-часах, прямо в приложении банка и пр. Здесь требования по удобству у всех разные, но они очень важны.

В случае использования простой ЭП также отсутствует необходимость соблюдения требований регулятора в области криптографии. Алгоритмы вполне могут быть западные (например, ECDSA, SHA-256, AES-256), устройства тоже западные (iPhone и

Android), и приложения распространяются через западные цифровые магазины (AppStore и Google Play). Главное здесь — уровень защиты от злоумышленника и удобство наших пользователей.

К тому же исключение, описанное в пп. «В» п. 3 Постановления Правительства 313, говорит нам о том, что оно не распространяется на деятельность с использованием товаров, содержащих шифровальные (криптографические) средства, имеющих функцию либо аутентификации, либо электронной подписи. Другими словами, лицензия на распространение в этом случае не требуется.

Второе. Составляем для этого решения «юридическую обвязку» для наших конкретных целей и нашей системы. То есть прописываем соглашение, в котором фиксируется порядок выработки и проверки ЭП, включая описание работы с ключами и процедуры разбора конфликтных ситуаций.

Третье. Реализуем техническую интеграцию.

Четвёртое — радуемся жизни.

Следуя данному алгоритму действий или изучая опыт других коллег по цеху, вы непременно столкнётесь с платформой мобильной аутентификации и электронной подписи PayControl. Безопасность работы решения основана на использовании встроенных криптографических механизмов мобильных и серверных операционных систем (ECDSA, HMAC-SHA-256, AES), асимметричных ключах для контроля целостности и авторства, визуализации данных транзакции, анализе уязвимости мобильного устройства и многом другом.

ЮРИДИЧЕСКИЙ АСПЕКТ

Когда мы начинаем работу с заказчиком, то, кроме технической интеграции, всегда помогаем реализовать и юридическую обвязку всех бизнес-сценариев. У нас довольно большой опыт в составлении юридических конструкций использования ЭП: от очень простых до «железобетонных», которые опровергнуть нет никакой возможности, с примерами различных вариантов процедур формирования подписи и разбора конфликтов.

С технической точки зрения, PayControl — богатая возможностями платформа, которая очень просто встраивается в процессы заказчика. В качестве примера: один из наших самых крупных проектов был реализован за полтора месяца под ключ, а рекорд по технической интеграции составляет всего 4 часа.

ПРО РАДОСТИ ЖИЗНИ

И конечно, про радости жизни: по данным наших клиентов, время подтверждения транзакций пользователем сокращается в несколько раз. Это следует из того, что уменьшается количество действий: не надо переколачивать ОТП-коды, не надо ждать, пока придёт SMS. И не менее важно для бизнеса — сокращение расходов составляет до пяти раз в сравнении с SMS.

В качестве итога, простая электронная подпись — это не только ОТП-коды из SMS или пароли. Если сделать простую ЭП правильно, то она может обеспечивать очень высокий уровень безопасности, быть удобной для пользователя и экономически выгодной для бизнеса.

Если сравнивать простую ЭП с УНЭП, то с точки зрения юридической конструкции и нюансов, связанных со встраиванием и распространением, простая ЭП — проще (простите за тавтологию). С точки зрения безопасности при правильной реализации простая ЭП не отличается от УНЭП. С юридической точки зрения — они эквивалентны.

* * *

На сегодняшний день правильная реализация ЭП — это одно из наиболее эффективных средств противодействия техническим атакам и социальной инженерии. Использование платформы аутентификации и мобильной электронной подписи PayControl позволит сделать работу конечных пользователей максимально удобной, значительно повысить уровень безопасности в цифровых каналах, обеспечить соответствие требованиям регулятора, а также повысить экономическую эффективность цифровых каналов банка.



Кай МИХАЙЛОВ
главный инженер
по информационной
безопасности,
IPROTECT GROUP

ПРОКАТИТЬ ХАКЕРА!

О ВОЗМОЖНОСТЯХ РЕШЕНИЙ «ЛАБОРАТОРИИ КАСПЕРСКОГО» KATA И KEDR

Целевые атаки происходят не так часто и занимают незначительную по количеству долю всех кибератак, но ущерб от них на порядок превосходит потери от традиционной массовой киберпреступности. Атака становится целевой в тот момент, когда используется не для широкого распространения, а, напротив, направлена на конкретную организацию или объект.

КАК ОНИ ДЕЙСТВУЮТ

В современном мире крайне сложно угадать особенности и недостатки ИТ-инфраструктуры организации — все данные как на ладони. «Безопасность через неясность» уже не работает, выяснить тип или версию используемых средств защиты может любой злоумышленник, например, придя на собеседование или в беседе с бывшим сотрудником.

В силу достаточной трудоёмкости и больших финансовых затрат на преодоление защиты крупных корпораций киберпреступники нередко проникают внутрь сетевого периметра через взлом сетей или устройств небольших и плохо защищённых подрядных компаний.

При целевой атаке для злоумышленника важно не быть обнаруженным как можно дольше. Также для повышения вероятности успеха атаки киберпреступники выясняют версии и уязвимости конкретных сервисов, используемых в конкретной сети.

Часто используется комбинация из социальной инженерии и одной или

нескольких технических уязвимостей. Это позволяет доставить используемый вредоносный код через небольшое количество шагов на рабочую машину сотрудника атакуемой организации.

«ПЕСОЧНИЦА»

Изначально для защиты от таких угроз применялись антивирусы на конечных точках и межсетевые экраны на сетевом периметре, но сегодня этого может оказаться недостаточно. За счёт ограниченных ресурсов рабочие устройства неспособны глубоко анализировать постоянно усложняющиеся кибератаки, вследствие чего функции проверки были вынесены на отдельные модули — так называемые песочницы.

Теперь рассмотрим саму песочницу. Её основной отличительной чертой и компонентом являются виртуальные машины, имитирующие обычные рабочие станции пользователя и мобильные устройства. На них и попадает потенциальный вредоносный объект.

Далее включается механизм анализа каждого шага запущенного в виртуальной машине вредоносного объекта. Ему нужно дать раскрыть себя во всей

красе, поместив его в десятки различных условий и собрав данные о последующем поведении.

Песочницы являются одним из главных компонентов защиты от направленных атак, так как они справляются со специально разработанными под конкретную атаку вредоносными объектами, сигнатуры которых ранее не были известны. На сегодняшний день у злоумышленников сформировался ряд излюбленных методов обхода песочниц.

- ♦ Проверка домена, чтобы выявить, принадлежит ли окружение, в котором находится вирус, целевой организации. Если не принадлежит, то атака останавливается.

- ♦ Отложенный старт — выжидание некоторого времени до начала вредоносной активности для обмана средств защиты. Для обработки таких сценариев песочницы научились ускорять время в контексте виртуальных машин.

- ♦ Запущен ли вредоносный код в среде виртуализации? Многие целенаправленные атаки проводят подобную проверку, считая, что рабочая станция сотрудника не может быть виртуальной. Песочница должна уметь

Песочницы являются одним из главных компонентов защиты от направленных атак, так как они справляются со специально разработанными под конкретную атаку вредоносными объектами, сигнатуры которых ранее не были известны

эмулировать физический CPU, выдавая себя за настоящую рабочую станцию пользователя.

♦ Есть ли в данном окружении активность пользователя? Песочницы эмулируют поведение пользователя — сетевая активность, клики мышкой по ссылкам, нажатия на клавиатуру и прокрутка экрана.

Перечисленные методы лишь примеры технологий сокрытия присутствия и ответов на них со стороны средств защиты, которые переносят задачу проверки угроз далеко за грань классического антивируса. Для нападающей стороны такое усложнение способов эксплуатации не остаётся незамеченным — затраты на обход защиты подобного уровня увеличиваются в разы, и попытки её «пробить» становятся нецелесообразными.

ВЗЯТЬ ПОД КОНТРОЛЬ

Исторически подход к защите от комплексных угроз менялся сначала от защиты периметра (доверяю всему, что внутри, не доверяю всему, что снаружи) к сегментации (разделяем сеть и бизнес-процессы на части, каждая сущность имеет права только в своём сегменте) и наконец к концепции нулевого доверия (полное отсутствие доверия кому-либо — даже пользователям внутри периметра). В современном представлении о безопасности периметр размыт (например, BYOD — Bring Your Own Device), а злоумышленник существует как внутри сети, так и за её периметром. При таком подходе остаётся взять под контроль потоки передачи данных между доверенными сегментами, которые злоумышленники могут использовать для проникновения с использованием методов социальной инженерии.

ТОЧКИ ВХОДА

Выделяют три основные точки входа данных, которые необходимо контролировать с помощью средств защиты:

- ♦ веб-трафик;
- ♦ обмен почтовыми сообщениями;
- ♦ рабочие станции пользователей.

Для каждой из них существуют специализированные решения защиты, которые, хотя и могут выявлять отдельные инциденты, обычно не способны

распознать их как часть сложной направленной атаки. Проблема решается за счёт интеграции специализированных решений с песочницей. Например, антиспам-система получает возможность отправлять на проверку в песочницу письма, спам-рейтинг которых не удастся выставить без глубокого анализа содержимого (вложений и ссылок). В таких условиях преимущество получают разработчики средств защиты, предлагающие комплексный набор различных решений, позволяющих собирать образцы для проверки из разных источников. Продуктовая линейка производителя превращается в экосистему продуктов безопасности, а их интеграция производится с наименьшими затратами и может быть выполнена одним кликом.

КАТА

Рассмотрим такую интеграцию на примере Kaspersky Anti Targeted Attack (КАТА) — системы защиты от целенаправленных атак. Система осуществляет сбор данных для проверки со всех основных потоков передачи данных компании, при этом поддерживая интеграцию как с продуктами «Лаборатории Касперского», так и с решениями сторонних вендоров.

Если для защиты почтового и веб-трафика достаточно анализа копии трафика, то для рабочих станций такой подход не работает. Классический антивирус в силу ограниченности ресурсов рабочей станции не способен поставить потенциальную угрозу в разные условия для наблюдения за её поведением (в т.ч. неограниченный доступ в сеть для связи с командными центрами), при этом не мешая работе пользователя.

KEDR

Учитывая появление всё более сложных методов обхода средств защиты, использования только антивируса может быть недостаточно для обнаружения и устранения угрозы. Появилась необходимость в компоненте, непрерывно наблюдающем за происходящим в ОС и проводящем анализ соответствия событий и обнаружений индикаторам атак (IOA — Indicator of Attack). Новый класс решений, получивший название



Endpoint Detection and Response (EDR), помимо формирования полной картины инцидента, занимается такими задачами, как сбор и долгосрочное хранение исторических данных для расследования, а также предоставляет инструменты реагирования, недоступные классическим антивирусным решениям.

У «Лаборатории Касперского» такой модуль называется Kaspersky EDR, или сокращённо KEDR. KEDR ориентирован на мониторинг и выявление аномалий в рядовых процессах ОС, таких как:

- ♦ работа с реестром;
- ♦ создание/удаление файлов;
- ♦ загрузка модулей в память;
- ♦ параметры командной строки, передаваемой в ОС;
- ♦ сетевая активность процесса/службы;
- ♦ события журналов Windows Event Log.

Сенсоры KEDR собирают данные о локальной активности и передают их на центральный узел КАТА компоненту



Target Attack Analyzer, который отвечает за анализ информации, поступающей со всей экосистемы средств защиты «Лаборатории Касперского» (антиспам-системы, веб-фильтрация, песочница, сенсоры на рабочих станциях) и делает вывод об обнаружении в инфраструктуре целевой атаки.

Подобный подход позволяет детектировать угрозы, недоступные для анализа классическому сигнатурному антивирусу.

Ещё одним немаловажным преимуществом KEDR является возможность активного реагирования на угрозы. Это позволяет офицеру безопасности выполнять на компьютерах различные операции, например:

- ◆ блокировка сетевых соединений (вплоть до полной изоляции АРМ);
- ◆ запрет и остановка файла либо процесса;
- ◆ запрос файлов на рабочей станции на проверку;
- ◆ запуск произвольных команд в ОС;

◆ выявление индикаторов компрометации.

Возможность активного реагирования на угрозы из единой консоли открывает для администраторов безопасности широкие возможности для оперативного предотвращения атак. Так, в ходе одного из проектов специалистами службы безопасности банка совместно с экспертами iTPROTECT GROUP ещё на этапе пилотного тестирования была заблокирована целевая атака с использованием социальной инженерии. Сотрудникам банка приходили письма spear-фишинг с содержимым, интересным для конкретного сотрудника. В качестве вложения выступали файлы офисного формата, которые неопасны сами по себе, однако в их заголовках были обращения на внешние ресурсы. При открытии файлов офисными программами создавался SMB-запрос на внешние сервера, который содержал в себе хеш пароля сотрудника. По критериям события было создано

правило IOA (Indicator of Attack), с помощью которого были найдены и обезврежены все подобные вредоносные файлы, попавшие во внутреннюю сеть.

* * *

Подводя итог, можно сказать, что использование в инфраструктуре интегрированных средств защиты информации, таких как песочница и EDR, существенно расширяет возможности по выявлению направленных атак, а также ускоряет реагирование на инциденты и облегчает их расследование, позволяя офицеру безопасности более точно восстанавливать хронологию событий. Интеграция с различными классами средств защиты информации позволяет модулю песочницы КАТА получать образцы для проверки со всех потоков данных в организации, обеспечивая при этом возможность реагирования, недоступную классическим «хостовым» средствам защиты.



Евгения КОЛОДИНА
директор по развитию
ГК «ЦИБИТ»

ОБУЧЕНИЕ В СФЕРЕ ИБ

АКТУАЛЬНЫЕ НАПРАВЛЕНИЯ

Согласно исследованию Assempure, 95 % российских школьников задумываются о том, чтобы в будущем работать в сфере информационных технологий. В опросе приняли участие четыре сотни детей из разных городов страны. Однако трудиться в IT мечтают не только дети. За 2020 год, по статистике job-сервисов, прирост активных резюме в области технологий и информационной безопасности составил 27,3 %. При этом, по данным аналитиков рынка труда, это сфера уже в течение 8 лет держит вторую позицию по приросту вакансий, уступая лишь сегменту продаж. Работа в области цифровых технологий и информационной безопасности — это перспективы, финансовая стабильность и востребованность на рынке.

Отдельно стоит отметить спрос на специалистов именно в сфере информационной безопасности, который растёт с каждым годом, и пандемия только «подстегнула» и ускорила эту тенденцию. На всех важнейших мероприятиях индустрии в этом году обсуждают критическую нехватку кадров, вопросы обучения и подбора профессионалов, которые не только соответствуют требованиям, но и обладают нужными компетенциями, чтобы работать с вызовами новой реальности.

Эксперты отмечают: конкуренция на рынке, к сожалению, не в пользу работодателя. На одну вакансию приходится только 2–3 резюме, и фактически это означает реальный кадровый голод в сфере IT и информационной безопасности. Потому что есть ещё целый ряд

нюансов, например, необходимость соответствия соискателей на должность требованиям регулирующих органов к квалификации и навыкам.

Исследования показывают: нехватка кадров в сфере кибербезопасности — не национальная, но глобальная проблема. 82 % компаний по всему миру подтверждают дефицит специалистов по кибербезопасности в своей организации, а 71 % опрошенных признали, что из-за отсутствия кадров организации становятся более уязвимыми для злоумышленников.

Всё это актуализирует тему обучения в сфере информационной безопасности: повышения квалификации и профессиональной переподготовки. Прохождение соответствующих учебных программ является необходимым и оптимальным способом получения нужных компетенций для работы в этой области.

Учебный центр, входящий в состав Группы компаний «ЦИБИТ», полностью отвечает потребностям компаний в обучении персонала в сфере защиты информации. Кроме того, у клиентов «ЦИБИТ» есть возможность получения полного комплекса услуг, ведь одним из подразделений ГК является кадровое агентство, которое квалифицируется на сложном подборе кадров в IT и информационной безопасности.

Сегодня законодательство предъявляет целый ряд требований к соискателям на должности для работы в сфере ИБ и IT. В связи с этим в Учебном центре «ЦИБИТ» разработаны программы обучения, согласованные с регулирующими органами — ФСБ России и

ФСТЭК России. Кроме этого, для слушателей предлагается большой перечень краткосрочных и электронных курсов.

ПРОГРАММЫ ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ, СОГЛАСОВАННЫЕ С РЕГУЛИРУЮЩИМИ ОРГАНАМИ (ФСТЭК РОССИИ, ФСБ РОССИИ)

Программа профессиональной переподготовки «Технологии и средства обеспечения компьютерной безопасности». Данный курс согласован с ФСБ России и Учебно-методическим объединением по образованию в области информационной безопасности. Объём всей программы составляет 540 часов в соответствии с нормативным сроком обучения, указанным в Постановлении Правительства РФ № 313.

Обучение на данной программе обеспечивает выполнение требований, предъявляемых к соискателям лицензии и лицензиатам ФСБ России на осуществление деятельности по разработке, производству и распространению шифровальных (криптографических) средств.

В данном курсе разработан целый блок лекций на тему «Криптографические средства и методы защиты компьютерных систем».

Программа профессиональной переподготовки «Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну». Данная программа согласована с ФСТЭК



России и соответствует требованиям Постановления Правительства РФ № 79 от 03.02.2012 г. (в ред. ПП РФ № 541). Объём курса составляет 504 часа, включая 360 аудиторных часов в соответствии с нормативным сроком обучения, указанным в Постановлении Правительства РФ № 541.

Обучение по программам профессиональной переподготовки Учебного центра «ЦИБИТ» обеспечивает выполнение требований, предъявляемых к соискателям лицензии и лицензиатам на осуществление деятельности по технической защите конфиденциальной информации, о прохождении обучения персонала по программам профпереподготовки в области информационной безопасности.

Программы повышения квалификации разработаны для следующих направлений:

1. программа повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры;

2. техническая защита информации. Организация защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну;

3. техническая защита информации. Способы и средства защиты информации от несанкционированного доступа;

4. технологии и средства защиты компьютерных систем;

5. обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных;

6. средства электронной подписи в защищённом документообороте;

7. обеспечение информационной безопасности в соответствии с требованиями Положения Банка России № 382-П;

8. безопасность бизнес-процессов при использовании мобильных технологий.

Отдельно отметим **программы, направленные на формирование компетенций специалистов, работающих в области средств использования электронной подписи в защищённом документообороте.**

♦ Программа повышения квалификации «Средства электронной подписи в защищённом документообороте» разработана для качественного изменения у слушателей имеющихся профессиональных навыков и направлена на получение компетенций, необходимых для соответствия требованиям Федерального закона РФ от 06.04.2011 № 63 «Об электронной подписи».

Данный курс соответствует требованиям Минкомсвязи России. Нормативный срок освоения программы составляет 72 часа.

♦ Краткосрочный лекционный курс «Электронная подпись» является введением в тематику истории возникновения и развития, правовых основ, а также практического опыта реализации технологии электронной подписи. Продолжительность программы — 4 часа.

Учебный центр «ЦИБИТ» является ведущим специализированным центром обучения в отрасли информационной безопасности и ИТ. Обратитесь к нам за консультацией, чтобы узнать более подробную информацию.

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



ГРУППА КОМПАНИЙ
ЦИБИТ

ФОРУМ DLP+

ТЕОРИЯ И ПРАКТИКА ОКАЗАЛИСЬ ВПОЛНЕ СОВМЕСТИМЫ

Утечки конфиденциальной информации из-за угроз внутри периметра организации. Вот где зарыта одна из проблем информационной безопасности. Возможные пути её решения 26 мая обсудили на московском форуме DLP+ в «Цифровом деловом пространстве» на Покровке, 47.

ОТДАЛИ ДАНЬ

Технологии DLP сложны не только с технической точки зрения, но и в контексте возможного влияния на моральный климат в компании в условиях фактически тотальной DLP-слежки. В ряде стран Европы именно этот фактор при рассмотрении его сквозь призму идей прав человека на законодательном уровне препятствует использованию систем DLP.

DLP+ отдал дань этой европейской фишке двумя дискуссиями — «Этика, право и безопасность» и «Человек для бизнеса: главная ценность или основная угроза?», а также докладом «Надлежащее процессуальное оформление доказательств и результатов внутренних расследований в компании».

ВЕРНУЛИСЬ К СУТИ

На профильных DLP-мероприятиях популярны «кейсы» о том, как использование технологий DLP вкупе с дополнительной информацией из систем безопасности и информационных систем, формально к DLP не относящихся, позволяет решать более общие задачи корпоративной безопасности или, например, помогает службе персонала в её деятельности. Но 26 мая на прямой вопрос модератора, что же представляет собой новое поколение систем DLP, президент ГК InfoWatch предпочла акцентировать внимание слушателей на том, что это по-прежнему системы для предотвращения утечек конфиденциальной информации.

ДУМАЙ ИНАЧЕ!

Уместно заметить, что Наталья Касперская на ключевой дискуссии Форума занимала достаточно консервативные

позиции. Она не поддержала модные тезисы о безусловности «новой реальности» в виде всеобщей дистанционной работы и о приобретении молодёжью неких новых черт в ходе пандемийной «лихорадки».

Нет, заявила Касперская, молодёжь всё та же, ей по-прежнему интересна «контактная» работа в компании.

Наталья Ивановна также обратила внимание на расширение канала утечки «мозгов» из страны в связи с вознесением на щит технологий дистанционной работы и рассказала об инициативах в её компании для совершенствования внутрикорпоративных отношений.

В дискуссии о моральности применения концепции «нулевого доверия» Наталья Ивановна не приняла активного участия, однако вскользь упомянула о появлении в новых версиях DLP от InfoWatch новых возможностей для выявления недобрых намерений персонала.

Президент ГК InfoWatch также озвучила ряд интересных соображений по иным затронутым на дискуссии вопросам, что инициировало или плодотворную полемику, или явно выражаемое всеобщее согласие.

ЧЕЛОВЕК: ЦЕННОСТЬ ИЛИ УГРОЗА?

Отечественный рынок уже давно не обращался к достаточно нишевой теме DLP с привлечением столь широкой аудитории. К раскрытию темы организаторы подошли фундаментально, предложив гостям после обсуждения «философских» вопросов ещё и ключевой доклад «Внедрять нельзя игнорировать» об этапах развития технологии на российском рынке. Об этом системно, под разными углами зрения — вендора и интегратора — рассказали Галина Рябова («Ростелеком-Солар») и Анна Попова (Infosecurity). После этого ход форума перешёл в прагматичное русло информационно-технических докладов в стиле «и это всё о ней» (или о нём?).

«DLP: от инцидентов к рискам», «От классической DLP к комплексной аналитике», «Идеальная DLP. Что нужно для счастья?», «DLP и интеграция бизнес-сценариев»... Это названия докладов только Большого зала, всё ещё выдержанные в духе политкорректности по отношению к роли Человека во внутреннем корпоративном мире.

А вот большинство названий докладов в Малом зале давали прямой и недвусмысленный ответ на вопрос «Человек для бизнеса: главная ценность или основная угроза?»: «Комплексный подход к защите от внутреннего злоумышленника: IdM, PIM/PAM, MDM и не только», «Контроль сотрудников в информационной среде компании», «User Behaviour Analytics. Поведение инсайдера»...

ОТ ТЕОРИИ DLP К ПРАКТИКЕ ВНЕДРЕНИЯ

В ходе круглого стола «DLP: ожидание и реальность» под управлением В.А. Окулесского (банк «Возрождение») его участники сообща набросали базовую траекторию внедрения DLP-системы. Ключевой, возможно, рекомендацией при этом стало выстраивание процесса не с формального заполнения поставщиком или интегратором опросных листов по функциональности DLP, а с постановки задачи, которую планируется возложить на DLP. И Анна Попова (Infosecurity), и Степан Дешевых (InfoWatch) привели конкретные примеры плодотворности такого подхода.

Ещё на одном из круглых столов тема DLP позволила обсудить гораздо более широкий круг вопросов, чем можно было ожидать. А выступление Максима Королёва, директора по ИБ УК «Сегежа Групп», стало настоящей «вишенкой на торте» этого мероприятия.

Формально его доклад должен был огласить взгляды представляемой им службы на «специфику защиты конфиденциальной информации в крупном холдинге». По факту гостям открылся успешный живой пример построения



системы ИБ на самых «трендовых» подходах в очень крупной компании (с численностью персонала, измеряемой тысячами человек и «филиалами» в России и Европе).

Для построения системы ИБ в холдинге были использованы технологии аутсорсинга, включая услуги стороннего СОСа, и собственная служба ИБ, включающая лишь около десятка человек, которая сумела подготовить всеобъемлющий пакет «нормативки» и успешно эксплуатировать сторонние ИБ-компетенции.

А в том, что касается принципов DLP, на которых зиждется безопасность конфиденциальной информации в компании Максима Королёва, то тут не удалось усмотреть и толики того «пацифизма», с которого начался форум, рассуждая об этике и возможности совмещения прав сотрудников с концепцией Zero Trust.

«Залитые» внешние порты рабочих компьютеров, подписки о неразглашении, тотальное обучение «кибергигиене» и отлучение от Интернета «двоечников» вплоть до успешной пересдачи экзаменов, регулярные проверки бдительности

и прочее, прочее, прочее, о чём приходилось слышать на тренингах в качестве добрых советов, в УК «Сегежа Групп» работает «по-взрослому».

ЗВАНИЕ «СЕРЕБРЯНОЙ ПУЛИ» ПОД ВОПРОСОМ

О конкретных примерах и перспективах DLP-технологий рассказывали и дискутировали на форуме DLP+ на четырёх треках докладов, в ходе двух круглых столов и на паре дискуссий, открывших, как уже упоминалось, мероприятие.

Нашлось место и для обсуждения вопросов о зрелости технологии DLP как таковой и зрелости заказчика для неформального внедрения DLP (потому что иногда такое внедрение лишь дань пресловутому «комплаенсу»), о возможности помощи в созревании заказчика со стороны интегратора, о зрелости технологий поведенческой аналитики в DLP и возможностях использования этой UEBA в более широких масштабах, нежели «простое» предотвращение утечек данных.

В целом было признано, что технологии DLP ещё не доросли до уровня

«серебряной пули» по части гарантированной защиты от утечек информации, их «искусственный интеллект» автоматизации требует не только настройки, но и периодического контроля. Поэтому вопрос о том, должна ли система DLP мониторить и оповещать о сомнительных перемещениях информации или жёстко пресекать движение данных, которые будут сочтены системой неприемлемыми, чаще решался в пользу «мониторить».

Плодотворности дискуссий на DLP+ способствовал гармоничный подбор спикеров со стороны как зарекомендовавших себя вендоров, так и квалифицированных потребителей DLP-технологий, которым было о чём рассказать коллегам. «Ростелеком-Солар», InfoWatch, Zecurion, Infosecurity (ГК Softline) с одной стороны, ПАО «Сбербанк», Банк «Возрождение», «М.Видео-Эльдорадо», hh.ru — с другой. И это далеко не исчерпывающий список мест работы экспертов, выступивших на форуме.

PHDAYS 10

ОБРАТНЫЙ ОТСЧЁТ
ПРИ УСПЕШНОМ
СТАРТЕ?Круглый стол «Экономика практической кибербезопасности».
Фото: пресс-служба Positive Technologies

На PHDays 10 был озвучен лозунг новой идеологии ИБ: «Неприемлемое должно стать невозможным!». О готовности взять его на вооружение в первый же день заявили компании Positive Technologies, ГК Innostage, «Инфосистемы Джет».

Идеология победителей наконец-то пришла на смену пораженческой покорности («Пока мир охвачен идеей цифровой трансформации, только хакеры решают, кто станет жертвой, а кто получит выгоду...»).

Соответственно, и набивший оскомину торгашеский подход «Планирование рисков, убытков и ущерба» было предложено сменить на принцип «Сделать невозможным нанесение неприемлемого ущерба для предприятия и государства».

В качестве примера нового подхода послужила концепция «Аэропорт» компании «Инфосистемы Джет». В основе этой системы защитных мероприятий — правильно выстроенная КИИ, сама архитектура которой создаёт первый эшелон непреодолимых (ну, или практически непреодолимых) препятствий для непрошенных кибергостей (преступников и киберсолдат), а инструментарий ИБ вступает в игру лишь на последнем этапе.

Однако за «спиной» нового подхода видятся не только достижения, но и проблемы. Проблемы, связанные с капиталом: и человеческим, и инвестиционным. Причём, как оказалось, вопросы инвестиций на рынке ИБ сегодня тесно увязаны с качеством кадров ИБ-компаний.

ИСТОРИЯ ПРО ЛЮДЕЙ

Инвест-банкир Евгений Коган, делаясь в кулуарах PHDays 10 соображениями

на счёт инвестирования, отметил, что «в случае с ИБ капиталом являются прежде всего люди. И сегодня ценность этого капитала, т. е. мозгов и опыта, сильно растёт».

Ну а руководству ИБ-компаний значимость профессионализма их сотрудников давно ясна. Но Владимир Дрюков (Solar JSOC) на круглом столе «Экономика практической кибербезопасности» всё же напомнил, что «технологии — это скорее некий ИБ-каркас, а в непосредственной работе ИБ всё равно — история про людей». А Дмитрий Гадарь («Тинькофф»), подхватив «подачу», отметил, что «в настоящее время специалист по безопасности должен обладать базовыми знаниями в области математики, сетей, операционных систем и т. д. Не хватает тех, кто понимает, как устроены сетевые протоколы, операционные системы и другие базовые вещи... А вот тыкать кнопки в ArcSight можно научиться довольно быстро».

И вот тут возникает когнитивный диссонанс!

На работу после вуза предпочитают брать тех, кто как раз уже умеет «тыкать кнопки в ArcSight». Именно для этого студенты начиная с младших курсов бегают по компаниям — учиться этому тыканью. А «базовые знания в области математики, сетей, операционных систем и так далее» в этой ситуации как бы побочку? Тем более что всё меньше остаётся в вузах тех, кто способен эти базовые знания (с учётом их развития) дать.

ТАК В ЧЁМ ПРОБЛЕМА?

Трудно не доверять оценкам специалистов Positive Technologies о том, что на

всю страну сегодня есть от силы пара сотен специалистов, способных эффективно и доверенно работать в структурах SOC. И именно в связи с такими оценками Positive Technologies дополняет новый подход «Неприемлемое должно стать невозможным» второй частью: «Обнаружить и остановить киберпреступника одним человеком!»

Не исключено, правда, что оценка «от силы пара сотен» всё же маркетингово заострена, ведь в материалах PHDays 10 прозвучали и другие цифры. Например, «лишь в нескольких центрах киберзащиты крупнейших компаний трудится около полутысячи специалистов: в Сбере около 400 человек, в «ВымпелКоме» около 40, в НЛМК порядка 60». А есть ещё и «Ростелеком-Солар», и «Лаборатория Касперского», «Ангара» и много других.

Тем не менее проблема кадров, способных сделать «неприемлемое невозможным», существует. Это продемонстрировал и круглый стол «Безопасная разработка — обязательное условие цифровой трансформации», в котором приняли участие представители ПАО «Ак Барс Банк», ПАО «Газпромнефть», ПАО «Сбербанк», АО ИК «АСЭ», «Газинформсервис».

В ходе этого мероприятия все попытки модератора подтолкнуть гостей к обсуждению технической, по сути, темы раз за разом сводились к проблеме кадров: их индивидуальной квалификации, способам их удержания, невозможности формировать работоспособные коллективы программистов и т.д. и т.п.

Сводились к проблеме, но без предложений, как её решить. За исключением не блещущего оригинальностью

понимания необходимости подготовки ТЗ и документирования процессов разработки кода, не более того. И похоже, эта скупость управленческой мысли не была связана с коммерческой тайной.

И это указывает на наличие кадровой проблемы не только на уровне исполнителей, но и на уровне руководства. Причём и те и другие должны быть не только квалифицированными, способными в нужный момент мыслить нестандартно, но при этом готовыми и к каждодневной рутине.

А с этим, действительно, проблемы!

«ГОРАЗДО ТРУДНЕЙ НЕ СВИХНУТЬСЯ ОТ СКУКИ...»

Да, некоторые «распальцованные» ИБ-компании горделиво утверждают, что латают прорехи нынешнего высшего образования своими корпоративными университетами. Но когда на одном из круглых столов была помянута одна из областей Центральной России в связи с дефицитом «ибэшников», то представитель московской «киберИБэлиты» высказался, что нет, мол, в российской глубинке «творческой» работы для ИБ-специалистов, подготовленных в этих замечательных корпоративных университетах.

В связи с этим стоит вспомнить популярный и уважаемый у советских учёных роман Даниила Гранина «Иду на грозу». Там один из центральных персонажей, оказавшись в заурядной заводской лаборатории, смог оживить её рутинную работу силой своей творческой мысли. Перефразируя Булгакова, можно утверждать, что творчество — оно в головах. И оно там либо есть, либо нет. А также напомнить, что путь к звёздам лежит через тернии.

Но тяжёлому и зачастую нудному преодолению рутины тоже надо учить, как и «базовым знаниям в области математики, сетей, операционных систем и так далее». Именно на этом основывались успехи в создании некогда надёжных ракет и первенство над миром в области балета.

Ежедневное многолетнее стояние у балетного станка и лишь потом часовой триумф на сцене.

СВЕЖИЙ ВЕТЕР ИЗ ГЛУБИНКИ

Сегодня живость ума и готовность высказывать нестандартные идеи свой-

ственны скорее сэлфмейдбизнесу из глубинки. В ходе круглого стола «Реальность российского кибербеза» глава казанской ГК Innostage Айдар Гузаиров заявил о том, что рассматривает складывающуюся ситуацию как своеобразные «тепличные условия» для выхода отечественной отрасли ИБ на новый этап развития. И эти условия надо эффективно использовать.

— Сейчас время запретов. Запрещаем не только мы, запрещают и нам. Имею в виду и санкционное давление и невозможность приобретения зарубежных продуктов кибербезопасности, и в то же время нарастающее недоверие к ним.

Но в этом времени возникают буквально тепличные условия, чтобы преоформить отрасль и развивать на территории России новые продукты. Важно при этом избегать спекуляций на теме импортозамещения и думать про экспортный потенциал. Один из основных путей этого развития консолидация отрасли кибербезопасности.

Пять ключевых составляющих консолидации, которые видятся сегодня:

Первая это предпринимательское сообщество российских производителей решений кибербезопасности. Вторая потребители, готовые поддерживать отрасль гарантированным спросом в долгосрочной перспективе. Третья инвесторы, вкладывающие финансы в развитие отрасли. Четвёртая регулирование отрасли со стороны государства и обеспечение мер по стимуляции развития отрасли. К примеру финансовые льготы для компаний, строящих системы кибербезопасности на отечественных продуктах. Ну и замыкает список образование, ведь без квалифицированных кадров никакие меры стимуляции не дадут роста рынка кибербеза.

ПОВОРОТ В УМАХ ПЕРВЫХ ЛИЦ

«Тепличные условия» это не синоним оранжерейности. Это, как ни странно, и совокупность санкционных политик зарубежья, которые появляются вдруг ниоткуда, и ряд жёстких, но справедливых регуляторных требований. Эти обстоятельства обратили лицо и бюджеты отечественного заказчика в сторону отечественных вендоров, приоткрывая для последних окно возможностей для внедрения своих продуктов.

А вот найти материальные ресурсы для вывода на новый уровень отечественных ИБ-продуктов позволяет инициатива нескольких банков, направленная на создание системы финансирования инноваций в сфере кибербезопасности. Об этой инициативе было упомянуто на круглом столе «Реальность российского кибербеза». И эта инициатива свидетельствует о повороте в умах первых лиц, повороте, о необходимости которого упомянул Айдар Гузаиров: «Первые лица видят свою роль в инфобезе только один раз в году во время согласования бюджетов. В вопросы кибербезопасности своего бизнеса они не вовлечены. Это должно измениться. Первое лицо должно ставить задачи своему CISO: „Я хочу чтобы мой бизнес не пострадал от хакеров. Реши это“».

А вот «политику импортозамещения» не следует рассматривать как таран, призванный «вынести» из информационной инфраструктуры всё, на чём отсутствует надпись «Сделано в России». На круглом столе «Реальность российского кибербеза» внимание аудитории было акцентировано на понятии «доверенная среда» и «доверенная платформа», а также упоминалось о возможности для начала создать своеобразную предтечу «доверенной среды» на отечественных продуктах ИБ вкуче с предложениями от израильских и китайских компаний, чтобы уйти от непредсказуемого поведения США.

* * *

Формальный числовой индекс, обозначающий «возраст» Positive Hack Days, — 10, но в этом году в логотипе конференции к аббревиатуре PHD, исполненной изысканной графикой, было добавлено слово ORIGIN, а графика «десятки» вполне позволяла трактовать это число как «ноль». Официальных пояснений к обновлённому логотипу услышать не довелось (что не означает, что их не было), но по осмыслению содержания PHD 10 затейливый вид порядкового номера мероприятия и новое слово в логотипе вызвали обнадеживающие и оптимистичные ассоциации с обратным отсчётом при успешном старте.



Валерий КУЛИКОВ
обозреватель BIS Journal

THE STANDOFF 2021

ИГРА КАК ОТРАЖЕНИЕ... РЕАЛЬНЫХ ПРОЦЕССОВ

Киберполигон The Standoff является на сегодня, пожалуй, наиболее известной российской площадкой для обкатки противодействия киберугрозам в реальной практике. В его инфраструктуре использована, например, не только действующая платёжная система от RBK.money, но и «боевые» контроллеры АСУ ТП. И главное, опыт компании Positive Technologies, а с этого года и CyberART ГК Innostage. С 2020 года учения тут проходят в масштабах, когда мощь нападения на цифровые системы предприятий ТЭК, транспорта, офисов компаний и других отраслей измеряется атаками более трёх десятков команд red team в круглосуточном режиме на протяжении нескольких дней.

ИТОГИ СО СТОРОНЫ ЗРИТЕЛЯ

Ключевой новостью можно считать, что в этом году атакующим Цифровой город удалось реализовать больше рисков, чем в прошлом, — 54% против 47%. При этом в прошлом году команда blue team одной из организаций «Росатома» сумела отстоять морской порт и железнодорожный узел, а в этом пострадала вся КИИ Города.

Интересным результатом стало распределение лидеров среди нападавших. В 2020 г. первая тройка выглядела так: Codeby (27 123 балла), back2oaz (24 463 балла), DeteAct (18 508 баллов). В этом году победителями среди «красных» стали True0xA3 (35 877 баллов), Codeby (30 183) и Invuls (17 643). При этом пятёрку лидеров замкнула

никому не известная команда-новичок из Беларуси.

Кроме творческого удовлетворения участников, The Standoff-2021 продемонстрировал заметный рост класса «красных» — победитель на каждом месте пьедестала почёта набрал больше баллов, чем соответствующий победитель в прошлом году. В то же время среди лидеров произошла смена состава:

- ♦ в первую тройку вошли две команды, не сумевшие блеснуть в прошлом году;

- ♦ спустившийся на второе место победитель прошлого года набрал больше очков, чем годом ранее на первом месте.

То есть четырёхдневный эксперимент показал, что формально угроза со стороны «красных» для цифровой экономики возросла. И это притом, что в ходе The Standoff 2021 «красные» не имели возможности пользоваться такой эффективной технологией, как «социальная инженерия».

ВИД ИЗНУТРИ

Антон Калинин, член команды судейского SOC, руководитель группы аналитиков Центра кибербезопасности CyberART ГК Innostage:

— В этом году изменился временной формат соревнований. В прошлом году они шли пять суток в режиме 24x7. В этом году учения продолжались полные сутки только с предпоследнего на последний день, а два дня до этого проходили с 10:00 до 19:00. С одной стороны, командам защиты было проще, так как они немного выдыхали от

наплыва атак. И хотя средства защиты также не были доступны после 19:00, blue teams могли проанализировать текущую обстановку и продумать дальнейшие шаги. С другой стороны, команды атакующих, наоборот, торопились дойти до нужной системы и реализовать риски до конца рабочего дня, потому что после 19:00 «сказка заканчивалась» и все пробросы из скомпрометированных систем, закреплённые на серверы атакующих, обрывались.

Ещё одно отличие от прошлого года — перевод части команд в офлайн. Пообщаться с коллегами — и защитниками, и нападающими, обменяться мнениями, обсудить проблемы... этого действительно не хватало в онлайн-формате.

В этом году защитникам фактически запретили реагировать на инциденты в их инфраструктуре. Так, один из фаворитов прошлого года — PT Application Firewall — был переведён в режим мониторинга и не блокировал даже самые простые атаки.

Среди средств защиты появилось новое — это ISIM для мониторинга сегмента АСУ ТП. И в сравнении с прошлым годом, когда было совсем непонятно, что происходит со SCADA, в этом году сети АСУ ТП стали «прозрачными», и все инциденты со SCADA оперативно детектировались.

Активно использовался Positive Technologies Network Attack Discovery, у которого расширился список детектов. В результате этот инструмент не только дополнял сработку в MaxPatrol SIEM, но и являлся



Министр цифрового развития, связи и массовых коммуникаций РФ М. И. Шадеев. Фото: пресс-служба Positive Technologies

самостоятельной системой для мониторинга и расследования реализованных бизнес-рисков.

Мы, как команда судейского SOC, также использовали в своей работе систему управления инцидентами собственной разработки — *Innostage IRP*. В ней консолидировались данные обо всех сработках из всех систем мониторинга, зафиксированные атаки из одной СЗИ обогащались информацией из другой системы, а также визуализировалась общая статистика по инцидентам и реализованным бизнес-рискам.

«ФЕНОМЕНАЛЬНОЕ ЧИСЛО ИНЦИДЕНТОВ»

И всё же главный результат The Standoff-2021 заключается в том, что защитники Цифрового города, не в пример прошлому году, проиграли нападавшим по всем статьям, не сумев удержать ни одного объекта КИИ. Поэтому не могу не сделать лирического обобщения.

О росте уровня реализовавшихся рисков для «оцифрованной» экономики свидетельствует системный анализ ситуации (в данном случае в реальном, а не виртуальном мире — авт.), представленный на PHDays 10 в докладе

«Ретроспективный анализ громких инцидентов ИБ за последние 10 лет». Экскурс в события, которые так или иначе были связаны с ИБ, продемонстрировал, что число громких взломов, утечек, атак с использованием вредоносного ПО, уязвимостей «нулевого дня» и других инцидентов столь велико, а последствия всего произошедшего таковы, что допускают использование таких экспрессивных характеристик, как «феноменально» и «катастрофически».

В нашей стране исключение из общего, «катастрофически» невысокого, уровня защиты от киберугроз представляют, возможно, только банки. По крайней мере, Артём Сычёв, первый замглавы Департамента ИБ ЦБ, не раз заявлял, что «с точки зрения ИБ банковская система РФ на голову выше западных. Опыт отражения атак и устранения последствий у наших финансовых организаций гораздо больше». Но банки всего лишь фрагмент большой картины.

И вот на фоне этой большой картины весьма сомнительными выглядят бравурные настроения «системных» экономистов, поднимающих на щит достоинства процессов цифровой трансформации, нередко

преувеличенные, а то и просто мифические. Примеры искать не нужно. Почти одновременно с PHDays 10 проходил Московский академический экономический форум (МАЭФ 2021), а в его рамках — пленарная конференция на тему «Цифровая трансформация экономики: перепроектирование нашего будущего или эволюция типовых моделей?»

Совершенно очевидно (а также следует из нормативных документов программы «Цифровая экономика России»), что цифровая трансформация экономики, независимо от того, видится ли она в головах академических мужей как «перепроектирование будущего» или как «эволюция типовых моделей», должна быть тесно увязана с РЕАЛЬНЫМ РЕШЕНИЕМ вопросов и проблем ИБ на всех уровнях оцифрованного хозяйственного комплекса: от уровней планирования и учёта до уровней управления производственными процессами, торговли и финансового обращения.

Однако многие выступающие на этой пленарной конференции исходили из сомнительных положений о том, что страна обеспечена аппаратно-программными платформами для

реализации «цифровой трансформации экономики» (при этом что, по их собственным признаниям, само это завышенное понятие до сих пор не определено), а также необходимым количеством специалистов в сфере ИБ.

Такая неосведомлённость, похоже, граничит с некомпетентностью и также достойна экспрессивных характеристик. По крайней мере, аналитика узкопрофессиональных (и потому более добросовестных) The Standoff-2021 / PHDays 10 свидетельствует о несостоятельности вышеприведённых «аксиом».

КИБЕРПОЛИГОНЫ РОССИИ

Некогда The Standoff был своеобразной «детской площадкой» в рамках конференции PHDays. Сегодня он вышел в высшую лигу ИБ как самостоятельная единица, а идея использования киберполигонов в системе совершенствования защиты КИИ нашла поддержку у регуляторов.

Отражением этой идеи стал круглый стол «Киберучения как способ проверки реальной защищённости финансовых организаций. Киберполигоны для финансовой отрасли» — одно из мероприятий конференции AntiFraud Spring Russia, проведённой Академией информационных систем (АИС) незадолго до The Standoff-2021.

С учётом того, что ещё одним из мероприятий этой конференции стала презентация Национального киберполигона, курируемого «Ростелеком-Солар», а упомянутый круглый стол собрал экспертов, представлявших, помимо Национального, ещё и киберполигоны Positive Technologies и Сбера (в лице Bi.Zone), а также киберполигон компании ООО «Киберполигон» (такая вот тавтология), то конференция АИС стала, возможно, первой публичной «презентацией» нового сегмента российского рынка ИБ.

Рассказ о своих детищах представил слушателям круглого стола вполне рыночный разноречивый набор намерений «киберполигонных заводчиков».

Из комментариев представителя Bi.Zone напрашивался вывод о социальной ориентированности проекта, целью которого на данный момент является формирование «комьюнити». При этом по мере развития беседы было

упомянуто о некой факультативности работы на полигоне Сбера для команды Bi.Zone.

«Ростелеком-Солар» и Positive Technologies по мере всё более откровенных подводок модератора круглого стола к теме бизнес-интересов в конце концов заявили о намерении поддерживать работу своих полигонов чуть ли не в режимах 24×365, что вряд ли может согласовываться с благотворительностью.

Стоит также заметить, что The Standoff от Positive Technologies и так уже несколько лет выполняет функции социально ориентированного центра кристаллизации «комьюнити».

Что касается «Ростелеком-Солар», то компания откровенно заявляет о своих технологических обязательствах перед профильными госорганами в части развития отечественных технологий в сфере ИБ, но из пояснений компании не следует, что поддержка этих процессов должна быть нерыночной.

Разнятся и технологические аспекты развития киберполигонов.

Bi.Zone позиционирует свои услуги как read team, готовая прокачивать навыки киберзащиты пришедших на её площадку компаний. Тем самым снимается вопрос оснащения защищаемых, которые приходят на полигон Сбера со своим инструментом, под своими лицензиями.

The Standoff от Positive Technologies собирает на своих «площадках» и blue-, и red-команды, а линейка собственных продуктов Positive Technologies способна довольно обстоятельно экипировать защитников КИИ.

Конкретики о технологическом оснащении Национального киберполигона услышать не удалось, но наличие определения «национальный» в его названии позволяет надеяться, что больших проблем с этим быть не должно.

Также мало что удалось узнать об особенностях киберполигона компании ООО «Киберполигон» — её представитель формально участвовал во всех раундах беседы, но так и не рассказал о своём детище ничего, кроме того, что полигон работает и все желающие могут воспользоваться его услугами.

Не удалось получить какую-либо информацию об инструментарии сторон

«read team» на упомянутых киберполигонах. Но, возможно, ответа на этот вопрос и быть не могло, так как актуальные данные о хакерском вооружении как раз и являются, на мой взгляд, одним из «профитов» для держателей площадок.

ШПИОН, ВЫЙДИ ВОН!

Кроме представления Национального киберполигона на AntiFraud Spring Russia 2021, анонс об этой площадке был дан в прессе (BIS Journal № 2/2021, с. 22–24). И материал этот был сопровождён комментарием, который выглядит странно легковесным, чем-то напоминающим по стилю и сути одновременно и публикации в «жёлтой» технической прессе о достоинствах использования Linux и Libre Office, и публикации начала 90-х вроде «ну, зачем делать своё плохое, мы лучше купим за рубежом хорошее».

Ну, действительно, цитирую: «Вместо киберполигона гораздо удобнее 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 далее: «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».

Но ощущение дежавю — это всего лишь ощущение.

А вот что думает по этому поводу Виктор Вячеславов, технический директор ГК Innostage:

— В целом можно приветствовать любые инструменты, повышающие уровень реальной защищённости и уровень подготовки специалистов в области кибербезопасности. Однако, по нашему мнению, неправильно говорить об упомянутом решении как о некой замене киберполигона.

Прежде всего, основная цель киберполигонов сейчас — это максимальное приближение создаваемых на них информационных систем к реальным.

И тут возникают два аспекта. Первый: распространённой практикой киберполигонов является использование реальных контроллеров АСУ ТП, что в виртуальной среде невозможно. Второй: имитация информационных систем предполагает воссоздание всех компонент информационных систем, а не только изучение систем виртуализации и контейнеризации, как предложено Google kCTF. Далеко не все из них можно адекватно использовать в виртуальной среде.

Кроме того, давайте посмотрим на общую политическую ситуацию.

Активно включён механизм санкций. Имитируя свои системы в облачном варианте Google kCTF, мы раскрываем чувствительную информацию недоверенной среде. Это особенности функционирования наших информационных систем, средств и методов их защиты, настройки систем. Это категорически не стоит делать в текущих условиях.

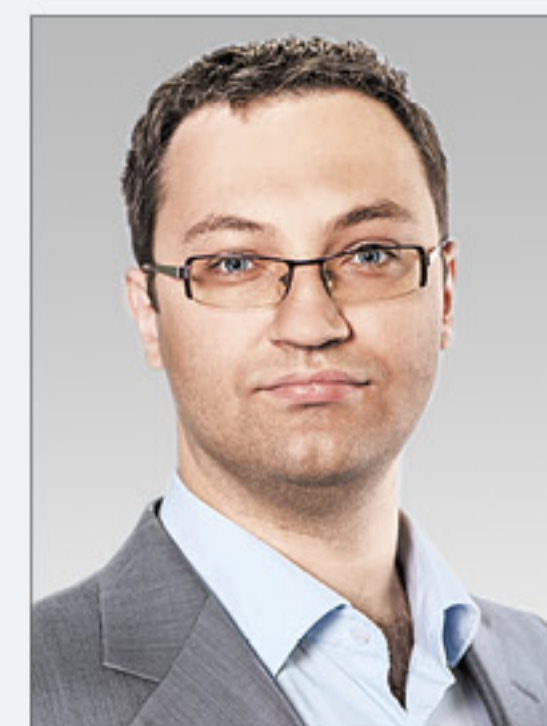
Предложенный вариант больше похож на создание так называемых honeypot — фейковых ресурсов, предназначенных для приманивания и изучения действий злоумышленников. И уже

известны кейсы, которые подтверждают обоснованность наших опасений.

В связи с таким комментарием возвращение к теме дежавю выглядит вполне обоснованным. И позволяет вспомнить не только упомянутые публикации 90-х, но и неизвестную ныне зрелым детям 90-х ситуацию, когда посулы грантов Джорджа Сороса позволили собрать заинтересованным структурам обширную базу знаний об актуальном состоянии науки в СССР на основе представляемых заявок на гранты. Сегодня в роли Джорджа Сороса на ниве ИБ выступает, похоже, Google kCTF.

BIS-КОММЕНТАРИЙ

ПРО ШПИОНОВ И ЛЮДЕЙ¹



Александр БОДРИК
эксперт BIS Journal

Отвечая на профессиональный комментарий Виктора Вячеславова, отмечу: главное — какие задачи мы решаем. Основная задача, которую по-своему пробуют решить и Google kCTF и коммерческие полигоны, — это приобретение и актуализация практических навыков специалистами.

Далее возникают вопросы организации приобретения навыков.

1. Чему конкретно учим? (Например, тестированию на проникновение)
2. Какую технологию адресуем? (Например, Kubernetes)
3. До какого уровня навыка хотим довести человека? (Например, до пятого уровня из пяти возможных)
4. Какой у человека уровень навыка сейчас?
5. Какие критерии оценки перехода на тот или иной уровень навыка?

И все эти вопросы нужно задать производителям коммерческих киберполигонов. К сожалению, обычно у них нет ни методологии обучения, ни матрицы навыков для конкретной роли специалиста, ни входных критериев квалификации специалистов, из-за чего вместо эффективного инструмента компании получают очередную дорогую игрушку, а CISO шутят: «Тот не CISO, у кого нет забытого СЗИ».

Так если всё это придётся брать не у производителя полигона, то всегда ли нужно тратить на него время и деньги? А каждый полигон, на минуточку, просит в среднем от

полумиллиона долларов сразу и ещё десятки процентов этой суммы на поддержку каждый год. Причём управлять этим полигоном придётся клиенту.

Относительно размещения Google kCTF — его возможно разместить на корпоративном Kubernetes, благо уже сотни предприятий в России имеют эту технологию внедрённой и используют в том числе для критических сервисов. Например, вот вакансия банка ВТБ на OpenShift (доработанный Kubernetes с поддержкой RedHat/IBM) <https://hh.ru/vacancy/38188270>.

А относительно эмуляции АСУ ТП — со средней квалификацией аналитиков СОС России и мира лучше держать их пока подальше от АСУ ТП, чтобы не провести потом лет 5–10 в местах не столь отдалённых. Сначала нужно научить этих специалистов, как отрабатывать use cases в обычной офисной сети, потом в микросервисном ландшафте, и уж самых опытных и хладнокровных пускать в АСУ ТП.

* * *

Что же до грантов Сороса и тому подобное — предлагаю оставить эти рассуждения тем, кто в этом понимает, наверное, экономистам. Исходя из своей практики, могу сказать, что утверждения или возражения не по существу обычно не имеют практической ценности и специалистами по ИБ просто отфильтровываются.

¹ BIS Journal № 2/2021, комментарий А. Бодрика «Киберполигоны? Пожалуйста! Не нужно ждать, когда государство их построит».

СТCRYPT 2021

КРУГЛЫЙ СТОЛ «КРИПТОГРАФИЯ ДЛЯ ГРАЖДАН И ГОСУДАРСТВА»

На 10-м симпозиуме «Современные тенденции в криптографии» (STCrypt-2021) 100-летие Криптографической службы России было отмечено не только торжественными церемониями, но и активной работой на будущее. Кроме научных дискуссий, симпозиум счёл необходимым провести обсуждение вопросов чисто прикладных и даже почти с потребительским уклоном. Этой проблематике был посвящён круглый стол «Криптография для граждан и государства». На нём разгорелась активная полемика между ИТ-вендорами, накопившими большой положительный опыт по аппаратному и программному «импортозамещению» (в силу специфики своих клиентов, использующих Интернет как технологию), и теми представителями ИТ, для кого Интернет — это глобальная площадка для бизнеса. Последние, как и следовало ожидать, заняли позицию осторожной критики «импортозамещения», увязывая свой переход на отечественные технологии с минимизацией ущерба для бизнеса.

ОТКУДА, КУДА, ЗАЧЕМ

Вообще говоря, отечественная криптография служит государству уже 100 лет. И около трёх десятков лет она служит бизнесу. Выход в «гражданскую» сферу можно связать с опубликованием в конце 1980-х стандарта ГОСТ 28147-89 на алгоритмы криптографической защиты информации и с коммерциализацией экономики в начале 1990-х, что создало спрос на криптографическую защиту информации.

Круглый стол «Криптография для граждан и государства» заострил внимание на возникновении нового этапа в экспансии криптографических технологий на рынок «общего» назначения в условиях цифровизации. Растянутый во времени старт этому этапу дали регуляторы, которые ввели требования по защите каналов связи, причём

с применением российских средств криптографической защиты информации (СКЗИ). Использование сертифицированных СКЗИ операторами персональных данных регламентирует Постановление Правительства № 1119, а также Приказ ФСБ России № 378.

В финансовой отрасли действует ряд Положений Банка России и ГОСТ Р 57580, согласно которым криптозащита необходима на всех этапах передачи данных между инфраструктурой банков и банковскими приложениями. Также приказ о необходимости использования сертифицированных средств защиты информации выпустил Минздрав РФ. Министерством энергетики утверждён приказ, в соответствии с которым для защиты информации в системах удалённого мониторинга и диагностики необходимо использовать сертифицированные средства защиты. Этот приказ стал фактически одним из первых указаний на необходимость перехода на защищённый обмен данными в системах АСУ ТП.

ИНФОРМАЦИЯ ДЛЯ РАЗМЫШЛЕНИЯ

Создание канала связи — это сложный длящийся проект (проектирование, закупка оборудования, пусконаладка, сопровождение в течение жизненного цикла). А создание защищённого канала связи — это ещё и решение таких вопросов, как введение на канале в эксплуатацию СКЗИ и соблюдение требований ФСБ России в части использования этого специализированного оборудования. Подводным камнем может стать разница в сроках действия сертификата на СКЗИ и сроке эксплуатации аппаратной части канала связи. И всё это выливается в конечном счёте в удорожание использования защищённого криптографией канала связи по сравнению с «обычным» каналом.

Если говорить об упомянутых требованиях Минэнерго, то защита информации в «интеллектуальных» системах учёта электроэнергии имеет свои

особенности: проблемы создают те обстоятельства, что фактически отсутствует базовая модель угроз безопасности информации в «интеллектуальных» системах учёта электрической энергии; отсутствуют сертифицированные СКЗИ, соответствующие условиям применения их в электроэнергетике.

И уместно заметить, что и тут возникает вопрос о деньгах: разработка специализированных СКЗИ для «интеллектуальных» систем учёта электроэнергии, последующая оценка соответствия разработки в системе сертификации регулятора — это дополнительные затраты денег и времени.

ДВА МИРА ИТ

Затравочными центрами дискуссий на круглом столе стали представители компаний «ИнфоТеКС» и «Актив» (центры компетенций в сфере промышленных коммуникаций и Интернета вещей в контексте криптографической защиты в этих областях) и Сбера и «Рамблера» (представители компаний, которым надлежит выполнять указания регуляторов в части защиты «чувствительной» для населения информации при использовании этим населением соответствующих каналов для получения госуслуг и услуг финансовых).

ПОЗИЦИЯ СБЕРА И РАМБЛЕРА

О позиции «ИнфоТеКСа» и «Актива» чуть позже, начнём с представителей сервисного сегмента экономики. Они говорили много, витиевато, не спорили с регулятором даже заочно (хотя всё же называли ГОСТ «священной коровой» и намекали на то, что не все уже могут вспомнить, а зачем она нужна), признавали, что уже многие десятки миллионов клиентов ломятся на их порталы за услугами со своими смартфонами, НО:

«Вот скиминга уже нет, вирусов на мобильных устройствах мало, злоумышленники перешли на «социальную» инженерию, а против неё СКЗИ



не действуют». Поэтому внедрим двухфакторную идентификацию, биометрию и технологиями поборемся за безопасность граждан.

Дополнительно пускались в ход классические «отмазки» — денег нет, сертифицированного отечественного оборудования нет, население лениво и скудоумно и при освоении сложных технологий тормозит на втором шаге (это в связи с внедрением ЭП для «физиков»).

Короче, «нас ставят в позицию, чтобы мы были первыми. Да, мы большие, мы могли бы навязать всё это своим клиентам. Но мы не будем навязывать! И мы не хотим экспериментов! Будем ждать готового решения, и уж его мы внедрим».

ПОЗИЦИЯ «ИНФОТЕКСА» И «АКТИВА»

«ИнфоТеКС» и «Актив» чётко обозначили свою позицию принципиальной поддержки инициатив регуляторов и сосредоточили своё выступление на инженерных проблемах внедрения криптографии в устройства Интернета вещей (IoT).

Хотя из виду не были упущены и методологические проблемы, которые аналогичны проблемам ИБ в сфере малого бизнеса — отсутствие понимания самого факта наличия киберугроз и их природы, стремление к максимальному удешевлению оборудования и систем IoT.

Инженерная же проблема, если говорить обобщённо, связана с переходом разработчиков из мира процессоров в мир микроконтроллеров (МК).

Из-за иных подходов к разработке оборудования на основе МК затруднено или даже невозможно прямое перенесение в мир IoT наработок, накопленных при криптографической защите информационных систем корпоративного уровня, где используются более мощные процессоры, имеются большие ресурсы памяти, нет столь жёстких ограничений в части энергопотребления.

Думается, что в этом материале нет необходимости подробно описывать все обсуждённые в докладах «ИнфоТеКСа» и «Актива» инженерно-технические проблемы начавшихся разработок. Уместно лишь отметить, что проблемами они являются лишь отчасти и лишь потому, что уже 30 лет разорвано некогда единое пространство отечественной микроэлектроники и радиоэлектроники и разобщены коллективы разработчиков, работающих на рынках так называемых встраиваемых компьютерных технологий и так называемых корпоративных ИТ.

А наиболее важным выводом из выступления представителей «ИнфоТеКСа» и «Актива» в контексте решения обобщённой проблемы «криптографии для граждан и государства» является тот факт, что отечественные вендоры готовы решать возникающие задачи по мере их поступления.

КАК НАМ ОБУСТРОИТЬ РОССИЮ

Одним из условий для этого является формирование единого экспертного

сообщества, которое не будет ждать сертифицированных решений от регуляторов, а будет разрабатывать эти решения и согласовывать их с регуляторными инстанциями.

С этим предложением идеологически солидаризируется вывод из краткой дискуссии в связи с жалобами на отсутствие необходимого российского оборудования.

Оппонент из зала задал прямой вопрос: а было ли сформировано соответствующее техническое задание? И напомнил, как некоторое время назад в связи с утверждениями некоторых экспертов о невозможности создания в России высокоскоростного шифратора соответствующее задание было сформулировано и оборудование появилось. «Если правильно и вовремя ставить задачи, то они решаемы!»

В целом участники круглого стола не идеализировали ситуацию.

Были названы проблемы с технологиями «безопасной разработки», организационные неурядицы процессов отечественной сертификации «кремния» и IP-ядер, «заволокиченность» процесса получения TLS-сертификатов. «Если мы говорим о массовости, то давайте сделаем это удобно!»

В отсутствие регулятора дискуссия, как и следовало ожидать, не закончилась принятием обязывающей «резолуции» или тем более «дорожной карты». Однако позиции сторон были обозначены предельно чётко.

ANTIFRAUD SPRING RUSSIA 2021

НЕ «ФРОДОМ» ЕДИНЫМ...

В рамках стержневой темы на AntiFraud Spring Russia 2021 были разобраны вопросы взаимодействия банков, операторов связи и государства для противодействия телефонному мошенничеству, также было рассказано о новых трендах «фрода» и представлены решения для противодействия «нестандартному» мошенничеству.

Угрозы мошенничества с использованием современной телефонии участники разбирали на свежую голову, причём очень представительным составом (два ведущих оператора связи, представители ФСИН, Сбера и НСПК в качестве экспертов, компетентные представители правоохранительных органов и финансовых организаций (ФО) в зале), что позволило нарисовать полную картину явления. Однако до корней такой, например, проблемы, как непобедимость технологии подмены номеров, так и не удалось докопаться. Как образно выразился один из участников конференции: «Давно пора хотя бы начать «догонять» эту проблему, в то время как добропорядочные участники рынка продолжают всё больше «отставать» от её решения».

Тут поневоле задумаешься о конспирологии, потому что упомянутый многополярный коллектив экспертов в очередной раз не смог назвать бенефициаров ситуации.

ПРО ИНДИВИДУАЛЬНЫЕ ВЫСТУПЛЕНИЯ

Докладчики секции «Технологии и тренды финансового антифрода», как

и следовало ожидать, выделили особенности ситуации, связанные с влиянием информационного шторма под «брендом» SARS-CoV-2 на умы сограждан и трансформацией бизнес-процессов в угоду «удалёнке».

А вот доклад представителя ITD Group, помимо «традиционного» мошенничества, затронул очень интересные проблемы выявления высокоуровневых противоправных действий в ходе так называемых проприетарных финансовых операций банков на рынках акций и финансовых спекуляций и поведал об инструментах для борьбы с подобным «фродом».

Упоминая об индивидуальных выступлениях, нельзя не отметить весьма интересный «скриншот» текущих проблем ИБ в контексте ФО, представленный в докладе «Практика обеспечения защиты банковских приложений в период пандемии» Алексеем Плешковым (Газпромбанк), а также доклад технического директора RTM Group «ОУД4: практика анализа уязвимостей, как перейти к оценке соответствия?».

НЕ «ФРОДОМ» ЕДИНЫМ...

Уместно отметить, что весеннее «издание» конференции не ограничилось обсуждением лишь проблем «фрода».

Обсуждались также проблемы проведения аудитов состояния ИБ в финансовых организациях с учётом появления ГОСТ Р 57580 и требований положений Банка России № 672-П, 683-П, 684-П и приказа Минкомсвязи № 321, а круглый стол «Киберучения

как способ проверки реальной защищённости финансовых организаций. Киберполигоны для финансовой отрасли» представил картину российского киберполигоностроения. При этом параллельно основному потоку конференции «Ростелеком-Солар» провёл показательные учения на так называемом Национальном киберполигоне. По завершении этого действия интересующиеся «обыватели» с основного потока смогли задать свои вопросы и узнать много нового.

КРУГЛЫЙ СТОЛ

Круглый стол собрал компетентный и информированный пул экспертов, представлявших киберполигоны, развивающиеся под эгидой «Ростелеком-Солар», ООО «Киберполигон», Positive Technologies, Bi.Zone (Сбер). ФО на круглом столе представлял Игорь Кубышко из «Банка Тинькофф», руководитель управления реагирования на инциденты ИБ. Он, в частности, кратко прокомментировал опыт «штабных» учений в «Банке Тинькофф», проведённых в этой ФО Банком России, и высоко оценил пользу от этого мероприятия.

К сожалению, в отличие от остальных мероприятий AntiFraud Spring Russia, круглый стол проводился его модератором таким образом, что аудитории была отведена роль слушателей и вопросы из зала не состоялись. В связи с этим не удалось, например, узнать, как на представленных площадках будет представляться актуальный инструментарий нападающих.

* * *

Самый общий вывод, который можно сделать по итогам круглого стола, — сильная неоднородность киберполигонов как нового сегмента рынка ИБ. Неоднородность как «бизнесовая», так и технологическая.

Угрозы мошенничества с использованием современной телефонии участники разбирали на свежую голову, причём очень представительным составом, что позволило нарисовать полную картину явления

CISO-ФОРУМ 2021

ВОЗВРАЩЕНИЕ К СТАРОЙ РЕАЛЬНОСТИ, НО...
С НОВЫМ ОПЫТОМ

14-й Межотраслевой CISO-Форум в Москве собрал представителей служб ИБ и ключевых вендоров ИБ-оборудования и услуг. Последние, помимо ненавязчивого предложения докладов, сформировали выставочную программу, которая в этом году именовалась шоурум «Все в деле». Площадка этого шоурума оказалась, помимо прочего, удобным местом для неформального общения.

НОРМАЛЬНО, НО ПО-НОВОМУ

Нынешнее мероприятие предложило мобилизующий слоган: «Новая нормальность», а базовыми чертами этой «нормальности» были названы:

- ♦ превращение «де-факто» практики удалённой работы в стандарт трудового процесса;
- ♦ ужесточающиеся требования регуляторов, в том числе в части реализации политики «импортозамещения»;
- ♦ выход уровня подготовки и проведения хакерских атак с «ремесленного» уровня на «индустриальный»;
- ♦ сохраняющийся (нарастающий?) дефицит квалифицированных кадров.

КАДРЫ: СЕКРЕТ «ТИНЬКОФФ»

Митап «Посткоронавирусное время: полёт нормальный?» с Алексеем Лукацким в качестве модератора начался с разминки на тему кадровых перестановок в верхних эшелонах департаментов ИБ и особенностей выстраивания отношений CISO с прочим топ-менеджментом «общего назначения» в условиях «новой нормальности». Как оказалось, общий уровень компетенций верхних эшелонов ИБ не изменился: определённая ротация имела место, но значимых потерь не случилось. Впрочем, новые яркие личности на этой части небосклона ИБ тоже не обозначились. Не является ли это следствием принципа «Звёзд на работу не брать!», не раз поднимаемого на щит на прошлых встречах CISO?

По результатам обмена мнениями среди спикеров, представлявших «Ростелеком», «S7 Информационные технологии», QIWI, Rambler&Co., «Азимут», Транскапиталбанк, «Тинькофф», Счётную палату РФ, «Аванпост», ФТС России и др., наиболее демократично и удобно выстроенными (в контексте нужд CISO) оказались отношения внутри «Тинькофф» (матричная структура управления). Хотя, с другой стороны, можно ли ожидать каких-то претензий по части общения и возможностей договариваться внутри организации со стороны человека, руководящего ИБ в ранге вице-президента и директора департамента информационной безопасности?

ИМПОРТОЗАМЕЩЕНИЕ, ХАКЕРЫ, «НОВИНКИ» И ДР.

В части митапа, касавшейся вопросов импортозамещения, заслуживающим внимания стал опыт ФТС России, которая смогла полностью закрыть свои текущие потребности в оснащении службы ИБ отечественным инструментарием при весьма напряжённой работе информационных систем организации.

В том, что касается темы угроз со стороны хакеров, центральной была, пожалуй, тема программ-вымогателей. И здесь нельзя не отметить исчерпывающе полный доклад Алексея Лукацкого, который «до последнего винтика» разобрал подноготную «шифровальщиков», сформулировал рекомендации для CISO и пожелания в адрес регуляторов.

Что касается безопасности «удалённой работы», то, как отметил Рустэм Хайретдинов: «Мы возвращаемся к

старой реальности, но с новым опытом». А из системного анализа ряда докладов можно было сделать вывод, что встретившиеся в «новой реальности» проблемы были связаны с упрощением регламентов и процессов и/или неиспользованием имеющихся возможностей, имеющих десятилетнюю историю. Правда, иногда эти давно известные возможности представляются как новинки. Например, технология ZTNA, которую Palo Alto представила как сенсацию, а «оппоненты», вспомнив свою работу в StoneSoft, напомнили, что десять лет назад нечто подобное уже предлагалось.

Традиционно Форум уделил внимание профессиональному и карьерному росту CISO. На дискуссии «Профессиональное развитие директора по информационной безопасности» поднимались вопросы самообразования, «гитхабизации» ИБ и плодотворности практики киберучений.

Подводя итоги Форума, уместно выразить сомнения в том, что есть основания говорить о какой-то «новой нормальности». Есть проблемы «старой нормальности»:

- ♦ принятие как данности отставания ИБ в «гонке за лидером», в качестве которого выступает Хакер;
- ♦ «остаточный принцип» по отношению к нуждам ИБ в масштабах от организации/предприятия до государства;
- ♦ дефицит квалифицированных кадров и нерациональное использование кадров имеющихся.

Эти проблемы и нужно решать.

Заслуживающим внимания стал опыт ФТС России, которая смогла полностью закрыть свои текущие потребности в оснащении службы ИБ отечественным инструментарием



Денис БАТРАНКОВ
эксперт BIS Journal

«ДОМАШНИЙ АРЕСТ»

КАК СОЕДИНИТЬ УДАЛЁННУЮ РАБОТУ И БЕЗОПАСНОСТЬ

Безопасность компании живётся на трёх китах: люди, технические решения и процессы. Когда весь мир почти мгновенно перешёл «на удалёнку», то оказалось, что не подготовлены все три составляющих. И конечно, была спешка, и неумолимо появились ошибки реализации.

Сейчас есть время пересмотреть использованные подходы и улучшить их. Что стоит выделить:

- ♦ правильно организованное рабочее место сотрудника должно быть защищено;
- ♦ сам сотрудник должен пройти минимальное обучение по правилам работы из дома;
- ♦ корпоративные ресурсы должны быть защищены от атак с компьютеров сотрудников, как бы странно это ни звучало.

АРХИТЕКТУРА УДАЛЁННОГО ДОСТУПА

Первый важный вопрос нужно задать к вашей архитектуре удалённого доступа в сеть компании. Чаще всего мы видим простую ошибку: внутренние порталы выставлены в Интернет, где постоянно идут сканирования, и, соответственно, они сразу под атакой. Необходимо всегда использовать специальные защищённые VPN-подключения для доступа к внутренним ресурсам. Это резко снижает число доступных для атаки сервисов и соответственно число атак из Интернета. Но VPN — это, по сути, туннель из вашего дома внутри

компании. Никогда не нужно делать туннель сразу к конфиденциальным ресурсам без какой-либо фильтрации. Поставьте на все такие подключения шлюз безопасности, который будет проверять, кто, что, куда и почему отправляет. Такой фильтр создают устройства под названием межсетевые экраны нового поколения (сокращённо NGFW). Они «принимают на себя» все подключения по VPN и также все атаки. Вы сможете контролировать, какие пользователи, какие приложения и какие файлы используют из дома, и сможете блокировать атаки и утечки данных, поскольку в NGFW встроены современные технологии анализа трафика и защиты. Этот подход к построению удалённого доступа в мире называют Zero Trust Networks Access (ZTNA).

СВОЙ? ЧУЖОЙ?

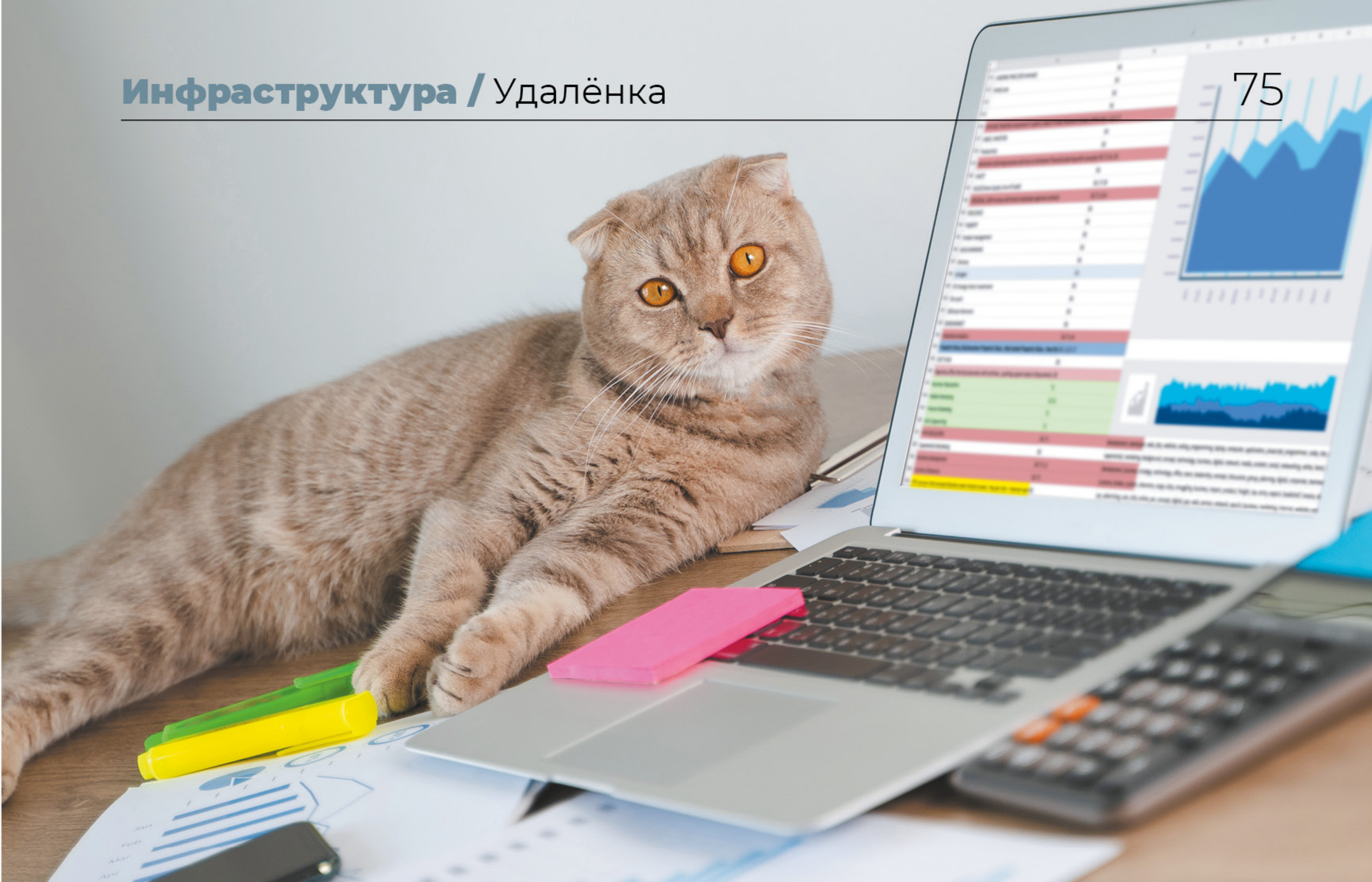
Самой частой угрозой вашей сети является то, что логин и пароль сотрудника воруют. И тогда, если открыт какой-то ресурс компании для доступа из Интернета, то к нему уже не будут подбирать логин и пароль, а просто воспользуются украденным и будут работать от имени вашего сотрудника.

В случае с удалённой работой на первое место должны выйти системы, которые контролируют, кто сейчас зашёл в сеть: сотрудник или тот, кто украл его коды доступа. Такие системы тоже есть, они контролируют поведение сотрудников. Они называются у специалистов User Behavior Analysis (UBA).

Существует важное дополнение к технологии удалённого доступа под названием двухфакторная аутентификация. Причём мы рекомендуем ей пользоваться для доступа и к личным ресурсам: gmail, instagram, facebook, интернет-магазинам, банкам и госуслугам. Что такое фактор? Это стандартный пароль, который сотрудник знает и хранит в секрете (желательно помнит наизусть). Что такое второй фактор? Это что-то дополнительное, что есть только у этого сотрудника: аппаратный генератор паролей, программа в смартфоне, набор одноразовых паролей на листочке или просто СМС, которая приходит только на телефон сотрудника. При доступе сотрудника в сеть важно проверить и пароль, и какой-то второй фактор из перечисленных. Это позволяет минимизировать угрозу того, что пароль украден, потому что второй фактор украсть не так просто.

ПОД ОДНУ ГРЕБЁНКУ. И ЭТО НЕПЛОХО

Не все компании могут позволить выдать сотруднику ноутбук домой. И если человек пользуется личным компьютером, то, скорее всего, он не защищён и его можно рассматривать как заражённый. Давать доступ с заражённого компьютера во внутреннюю сеть нельзя. Поэтому нужно обеспечить все компьютеры системами защиты. Современные системы защиты контролируют саму операционную систему и все приложения, а также могут вылечить компьютер от заражения. Но самое идеальное,



если система защиты будет защищать чистую операционную систему, которая только что установлена. На рынке информационной безопасности сейчас звучит всё чаще слово eXtended Detection and Response (XDR), что означает, что система не только проверяет и блокирует уже известные исследователям угрозы, но и отслеживает поведение сотрудника и всех приложений на его компьютере. Такие решения поддерживаются крупными исследовательскими лабораториями, где круглосуточно следят за новыми видами атак и сразу же распространяют защиту всем своим заказчикам. Их интересной особенностью является то, что они смотрят не только то, что происходит на самом компьютере, но и то, что происходит в сети, — корреляция двух типов событий позволяет быстрее выявлять атаки, поскольку злоумышленнику не получается скрыться.

СВЕДЕНИЕ К НУЛЮ

И завершает всё перечисленное ещё одна технология, которая соединяет все проверки в одну: тот самый человек, с того самого компьютера, с той самой

Безопасность компании зиждется на трёх китах: люди, технические решения и процессы. Когда весь мир почти мгновенно перешёл «на удалёнку», то оказалось, что не подготовлены все три составляющих

настроенной и включённой защитой на компьютере должен получить доступ к тому самому приложению, которое ему нужно по работе. Такая функция называется «проверка соответствия требованиям». Она должна быть реализована совместно в клиенте VPN и в NGFW, которые совместно дают доступ к нужным ресурсам, если ваш компьютер и вы сами прошли все проверки, заложенные службой безопасности. Это практически сводит до нуля возможности хакеров зайти к вам удалённо.

ОХ УЖ ЭТИ ДЕВУШКИ!

Важно коснуться обучения. Ваши специалисты по безопасности должны обучить всех не только правильному взаимодействию с собственными

ресурсами компании, но и со всеми ресурсами Интернета: какие программы нельзя скачивать, почему нельзя публиковать данные о компании на форумах, как получить помощь, если что-то пошло не так. Например, я встречался с тем, что компьютеры девушек заражены вредоносным кодом, который, показывает порнокартинки, и они просто боятся обратиться в службу поддержки по морально-этическим соображениям. При этом наносится урон компании — вредоносный код продолжает распространяться на другие компьютеры по сети и через электронную почту. Так что анонимная служба спасения тоже должна быть, а её контакты должны быть всем известны.



Андрей ЖАРКЕВИЧ
редактор
ООО «Антифишинг»

HUMAN FIREWALL

ДЛЯ УЛУЧШЕНИЯ РАБОТЫ ТЕХНИЧЕСКИХ
СРЕДСТВ ЗАЩИТЫ

Большинство современных кибератак достигают цели не благодаря уязвимости операционных систем, программ и сетевого оборудования, а из-за небезопасных действий сотрудников. Социальная инженерия, фишинговые письма с вредоносной нагрузкой и фишинговые ресурсы для кражи учётных данных оказываются эффективнее, чем попытки обойти межсетевой экран или воспользоваться ошибкой удалённого выполнения кода в VPN-сервере.

Воздействуя на эмоции людей, преступники крадут учётные данные, с помощью которых могут проникнуть в сеть под видом легальных пользователей. Но можно обойтись и без кражи, убедив получателя письма открыть вложение и разрешить выполнение макросов. И если аргументы подобраны правильно, пользователь будет рад отключить защищённый режим и, по сути, дать доступ мошенникам «ради важного документа».

Для борьбы с современными атаками технических средств недостаточно. Требуется системная работа по развитию у пользователей навыков противодействия уловкам социоинженеров. В результате компания получит новый уровень защиты в дополнение к техническому, так называемый human firewall, или «человеческий межсетевой экран», который сработает как цифровой иммунитет в организации.

В этой статье мы поговорим о том, почему привычные способы внедрения мер кибербезопасности в бизнес-процессы оказываются малоэффективны и как сформировать работающий human firewall на практике.

ЦИФРЫ И ФАКТЫ

По данным Group-IB, с 2019 года фишинг прочно закрепился в топ-3 векторов первичной компрометации корпоративных сетей ввиду высокой эффективности и значительно меньших затрат на подготовку, чем исключительно технические атаки.

Самые громкие инциденты последних месяцев связаны с вымогательским ПО, причём успех атакам обеспечила эксплуатация человеческих слабостей.

♦ 7 мая 2021 года произошла кибератака на оператора крупнейшего в США топливопровода Colonial Pipeline. Злоумышленники использовали фишинговую схему для получения доступа к инфраструктуре компании: один из сотрудников перешёл по ссылке в фишинговом письме и заразил все информационные системы. Заплатив выкуп в размере 5 млн долларов США, компания получила неработающий инструмент для расшифровки данных.

♦ 9 июня 2021 года компания JBS, владелец крупнейшего в мире мясоперерабатывающего производства, выплатила преступной группировке Revil 11 млн долларов США за восстановление доступа к зашифрованным в результате кибератаки системам. Для проникновения операторы вымогателя применили комбинацию из фишинговых писем и похищенных с помощью фишинга учётных данных для служб удалённого доступа.

Ещё одна примета времени, которую отмечают эксперты, — это целевой характер кибератак на крупные компании, а также участие в них различных по специализации группировок, каждая из которых выполняет свои задачи:

- ♦ сбор информации;
- ♦ проведение фишинговых кампаний для кражи учётных данных;
- ♦ проведение фишинговых кампаний для загрузки в сеть жертвы вредоносного ПО;
- ♦ сбор конфиденциальных данных внутри сети компании, их кража и шифрование;
- ♦ переговоры о получении выкупа и распределение полученных средств.

Учитывая суммы выкупов, которые получают вымогатели, к подготовке очередной кибератаки они могут привлечь самые дорогие команды.

Неграмотные и нетренированные сотрудники чрезвычайно уязвимы к атакам с использованием продвинутой социальной инженерии. А это значит, что для защиты необходимо вложиться в формирование корпоративной киберкультуры и выработки у людей навыков безопасного поведения.

Но каким образом можно повысить уровень защищённости сотрудников и снизить вероятность успеха кибератак, построив human firewall?

ШАГ 1. ЗНАНИЯ

Стандартная для компаний практика после инцидентов кибербезопасности — обновление парка технических средств и проведение

дополнительного обучения, информирования сотрудников. Некоторые организации приглашают экспертов для проведения тренингов по кибербезопасности, но чаще всё сводится к обучению с помощью электронного курса соответствующей тематики, например курса по безопасной работе с почтой или базового курса по информационной безопасности.

Окончив курс о безопасности электронной почты, сотрудники в лучшем случае будут знать, как действуют мошенники, в идеальном — по каким признакам можно отличить фишинговые письма от настоящих и как правильно действовать в случае, если обнаружена атака.

Для проверки знаний курс содержит итоговый тест, по результатам которого можно определить степень усвоения материала и при необходимости назначить дополнительное обучение.

Однако успешное прохождение итогового теста не означает, что полученные знания найдут применение в ходе реальных инцидентов. Проведённое компанией «Антифишинг» исследование поведения 20 тыс. пользователей различных организаций выявило интересный момент: после прохождения самых разных курсов навыки сотрудников улучшались лишь у 9 % сотрудников.

Этот эффект хорошо знаком всем, кто сдавал экзамены в институтах: буквально через неделю после сессии даже у отличников в голове мало что остаётся.

Ещё одна яркая иллюстрация того, что знаний недостаточно для безопасного поведения, — недавний инцидент с генералом МВД, который перечислил телефонным мошенникам более 600 тыс. рублей. Крайне маловероятно, что высокопоставленный силовик не знал о подобных преступлениях, однако в реальной ситуации знания просто не сработали.

Важно, чтобы знания стали умениями и навыками, то есть чтобы сотрудники научились совершать осмысленные действия на базе полученных знаний.

ШАГ 2. УМЕНИЯ И НАВЫКИ

Единственный способ превратить полученные знания в умения и навыки — их отработка на практике. Пример — получение водительского удостоверения. Чтобы стать водителем, необходимо не только сдать теоретический экзамен, но и пройти практический курс вождения. И никого это не удивляет, ведь автомобиль — средство повышенной опасности.

В случае с навыками в сфере информационной безопасности о практической стороне подготовки почему-то вспоминают значительно

Рисунок 1. Редактор имитированной атаки платформы «Антифишинг»

1. Домен отправителя
адрес похож на настоящий, но домен отправителя — поддельный

2. ?

3. ?

4. ?

Рисунок 2. Финальная страница с объяснением неправильных действий пользователя во время имитированной атаки

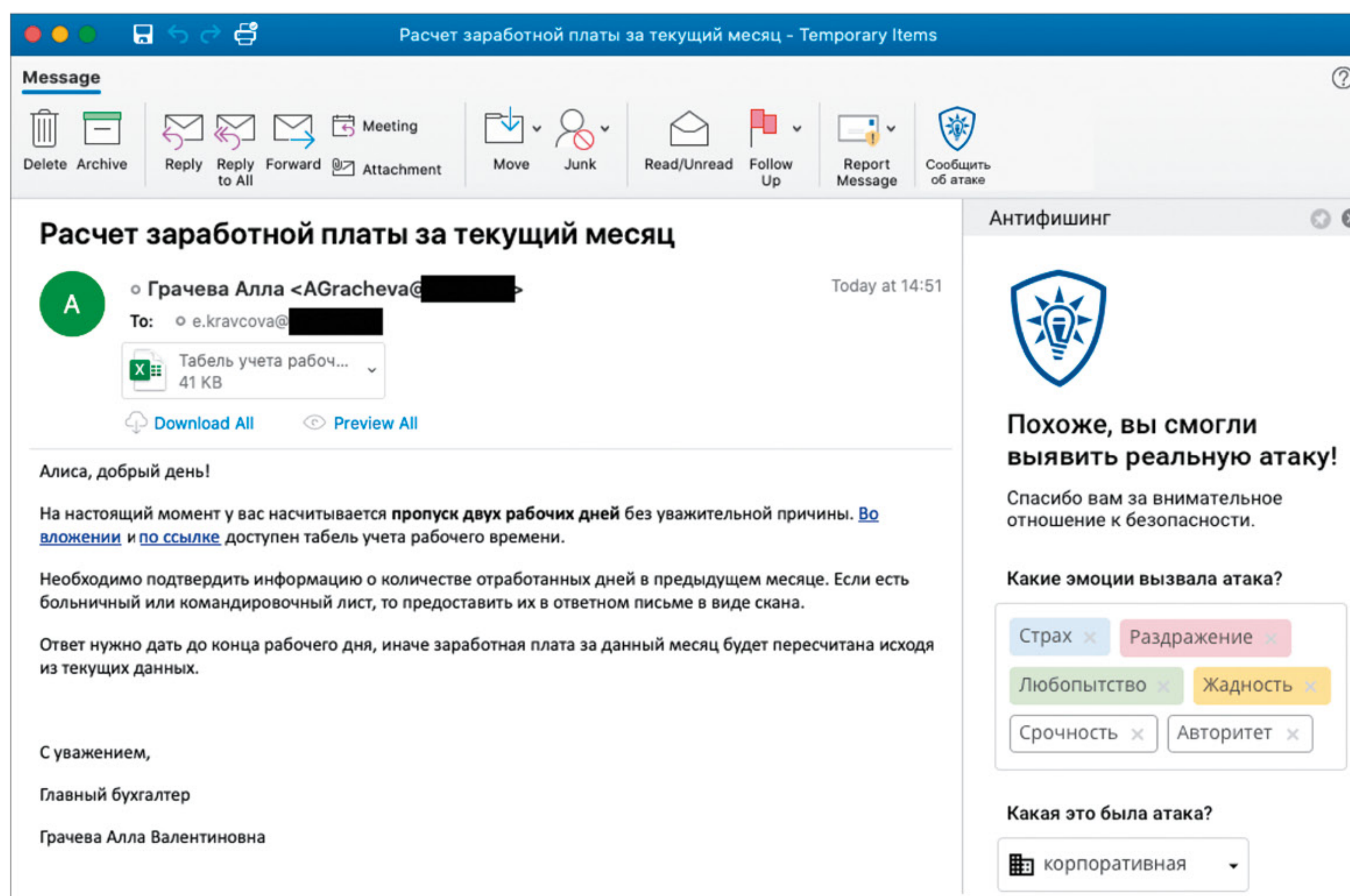


Рисунок 3. Интерфейс плагина «Антифишинг» для MS Outlook.

реже, хотя, как показывают те же инциденты с JBS и Colonial Pipeline, последствия небезопасных действий неподготовленных сотрудников могут быть крайне разрушительными.

Чтобы научить сотрудников правильно распознавать кибератаки и реагировать на них, нужно поместить их в условия, максимально приближенные к реальным. Сделать это своими силами сложно. Для имитации тактик мошенников требуется серьезная подготовка, как техническая, так и психологическая, методическая и организационная.

Решить проблему с подготовкой имитированных атак можно путём использования специализированных платформ.

В качестве примера подобного решения можно рассмотреть платформу «Антифишинг» (рис. 1). Входящий в её состав редактор имитированных атак позволяет на базе множества шаблонов подготовить разнообразные варианты целевых атак с нужными векторами эмоционального воздействия и целевым результатом. Сама платформа после запуска атак отслеживает действия сотрудников при получении писем и даёт им мгновенную обратную связь, обеспечивая не только формирование, но и закрепление и оценку навыка (рис. 2).

По данным исследования «Антифишинга», формирование навыков с помощью регулярных имитированных атак приводит к тому, что безопасное поведение вырабатывается уже у 49% сотрудников.

ШАГ 3. ПРИВЫЧКА

Если навык можно рассматривать как целенаправленное автоматическое действие в знакомой ситуации, то привычка предполагает, что оно не просто становится автоматическим, а превращается в потребность. Другими словами, пользователь, получивший фишинговое письмо, не только распознаёт его как мошенническое, не только не совершает небезопасных действий, но и ощущает потребность немедленно «отработать» атаку, уведомив ИБ-подразделение.

Для формирования привычки важно, чтобы между желанием и реализацией не было препятствий. В платформе «Антифишинг» эта задача решена через плагин для MS Outlook, с помощью которого пользователь может сообщить об атаке в один клик (рис. 3).

Плагин умеет различать имитированные атаки и не пересылает их на анализ в службу безопасности.

Если же сотрудник выявит реальную атаку, копия письма со всеми заголовками и содержанием будет отправлена на адрес службы безопасности и переместится в папку нежелательной почты в почтовом ящике сотрудника.

Кроме того, сотрудник может дополнительно разметить атаку по психологическим векторам и атрибции. Положительная обратная связь, предоставляемая плагином, способствует быстрому превращению навыка распознавания атак в привычку.

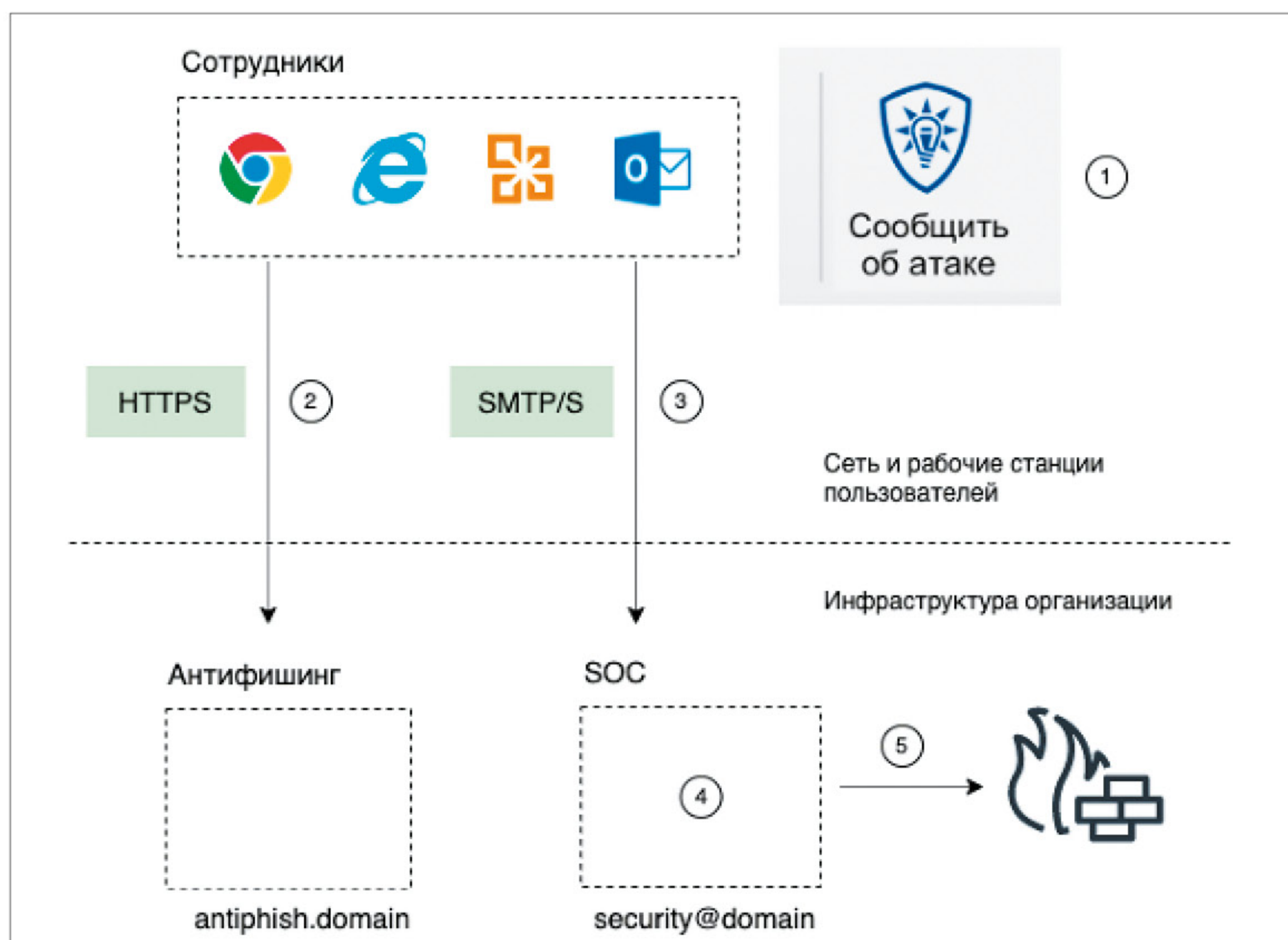


Рисунок 4. Формирование социоинженерного фида Threat Intelligence благодаря коммуникации пользователей и экспертов SOC

Благодаря плагину «Антифишинга» ИБ-служба получает максимально актуальный внутренний поток данных об угрозах (Threat Intelligence-фид), который генерируется сотрудниками. Его можно использовать для быстрого реагирования и блокировки активных цифровых атак (рис. 4).

По сути, это и есть Human firewall в действии:

1. Тренированные сотрудники выявляют цифровую атаку.

2. Статистика об этих безопасных и корректных действиях сохраняется в «Антифишинге».

3. Исходные данные направляются для анализа в корпоративный центр мониторинга и реагирования на инциденты (Security Operations Center, SOC).

4. Аналитики проводят расследование и привлекают собственные индикаторы компрометации (IoC).

5. SOC блокирует атаки по выявленным IoC на технических средствах защиты до того, как информация об этих IoC станет доступна во внешних фидах.

Таким образом, удобный для пользователей, основанный на привычках процесс выявления атаки и отправки оповещения повышает эффективность работы ИБ-подразделения, создавая тот самый дополнительный уровень защиты.

ПОСТРОЕНИЕ HUMAN FIREWALL: ГЛАВНОЕ

Обучающие курсы, дайджесты, буклеты — важные способы повысить осведомлённость, но они могут дать сотрудникам только знания.

1. Для превращения знаний в умения и навыки требуются регулярные тренировки в условиях, максимально приближённых к боевым, — проведение имитированных атак, максимально напоминающих реальные, но не создающих рисков для компании.

2. Организовать качественные, сильные и разнообразные имитированные атаки можно с помощью специализированных платформ.

3. Чтобы человеческий файерволл стал по-настоящему прочным, необходимо перевести навыки на уровень привычек, превратить безопасное поведение в потребность.

4. Для этого следует обеспечить тренированным пользователям «путь наименьшего сопротивления» в виде удобного и простого способа отправки уведомления о возможной атаке в ИБ-подразделение.

5. Поток таких уведомлений позволит службе реагирования на ранних этапах получить новые индикаторы компрометации, тем самым в несколько раз ускорив реагирование и повысив общий уровень защищённости организации.



Твоя сеть. Твои правила.

KASPERSKY.RU/BUSINESS

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



Марина БРОДСКАЯ
обозреватель BIS Journal

ВОЗВРАЩЕНИЕ К АЗАМ

НА ЗАПАДЕ АКТИВНО ВНЕДРЯЮТ ПРОГРАММЫ ПО ПОВЫШЕНИЮ ЗНАНИЙ В СФЕРЕ ИБ

Человеческий фактор стал главным препятствием на пути всеобщей кибербезопасности, считают на Западе и активно внедряют программы по повышению знаний в сфере ИБ.

НАУЧИТЬ ЗА 3,5 МИНУТЫ

Удалённая работа и онлайн-обучение в период пандемии COVID-19 показали, что перемены необходимы для выживания, пишет Хизер Стратфорд — основательница Drip7 и эксперт в области IT-обучения и кибербезопасности — в своём блоге на платформе Security Boulevard. Как показал период пандемии, вопрос взаимодействия сотрудников организации и доверия между ними лежит в основе выживания любой компании. А доверять в условиях онлайн-взаимодействия стоит, применяя модель безопасности Zero Trust.

Поэтому началась новая волна обучения сотрудников азам информационной безопасности, она помогает улучшить знания и навыки обычных работников. В основе нового подхода к обучению — не длинные лекции и

практические семинары, итогом которых становится экзамен и страх его не сдать, а геймификация, микрообучение и вознаграждение. Такой подход актуален для всех предприятий и соответствует всем глобальным изменениям в мире.

В основной массе киберпреступники неразборчивы в целях, поэтому риску подвергаются все организации. Если в прошлом основной вопрос ИБ заключался в том, какие бизнес-активы необходимо защищать, то сегодня хакеры всё реже собирают данные и всё чаще требуют выкуп за зашифрованную информацию в обмен на ключи шифрования.

Атакующих не интересует форма собственности или платёжеспособность жертвы. По данным Cloudwards, в 2020 году требования выкупа возникали каждые 11 секунд, а в среднем выкуп составлял почти \$ 200 тыс. Слабым звеном в организации мог стать каждый пользователь.

По оценкам экспертов, в настоящее время существуют различные типы вредоносных программ, которые атакуют организации. Популярны программы-вымогатели, которые шифруют

данные, — DearCry и Black Kingdom, нацеленная на серверы Microsoft Exchange. Вредоносное программное обеспечение CopperStealer крадёт данные, а вредонос XcodeSpy — вариант бэкдор-вируса Eggshell, специфичного для macOS, — активирует микрофоны, камеру и клавиатуру жертв.

Сотни вариантов вредоносного ПО постоянно атакуют серверы организаций. По оценкам компании по киберзащите Cybersecurity Ventures (США), в 2021 г. киберпреступность обойдётся миру в более чем \$ 6 трлн.

Для сокращения убытков есть один универсальный способ — повышение грамотности пользователей. По данным Cyber Security Intelligence, 90 % всех нарушений напрямую связаны с ошибками или действиями сотрудников, работающих в сети. И пока не существует технических возможностей, нужно полагаться на человеческий фактор, чтобы бороться с растущим числом киберугроз.

Почему обучение работников затруднительно, несмотря на значимость повышения квалификации для любой компании? Большинство корпоративных тренингов воспринимаются как неудобства. Их не воспринимают всерьёз, и, согласно исследованию Университета Ватерлоо, без закрепления новых сведений сотрудники забывают от 50 до 80 % изученного материала за два дня. Если изменить подход к обучению, согласовывать тему и время повышения квалификации, а также ввести вознаграждение по итогам учёбы, то ситуация

Если в прошлом основной вопрос ИБ заключался в том, какие бизнес-активы необходимо защищать, то сегодня хакеры всё реже собирают данные и всё чаще требуют выкуп за зашифрованную информацию в обмен на ключи шифрования

меняется. Вознаграждение — ключевая функция обучения, которую часто ожидают молодые сотрудники.

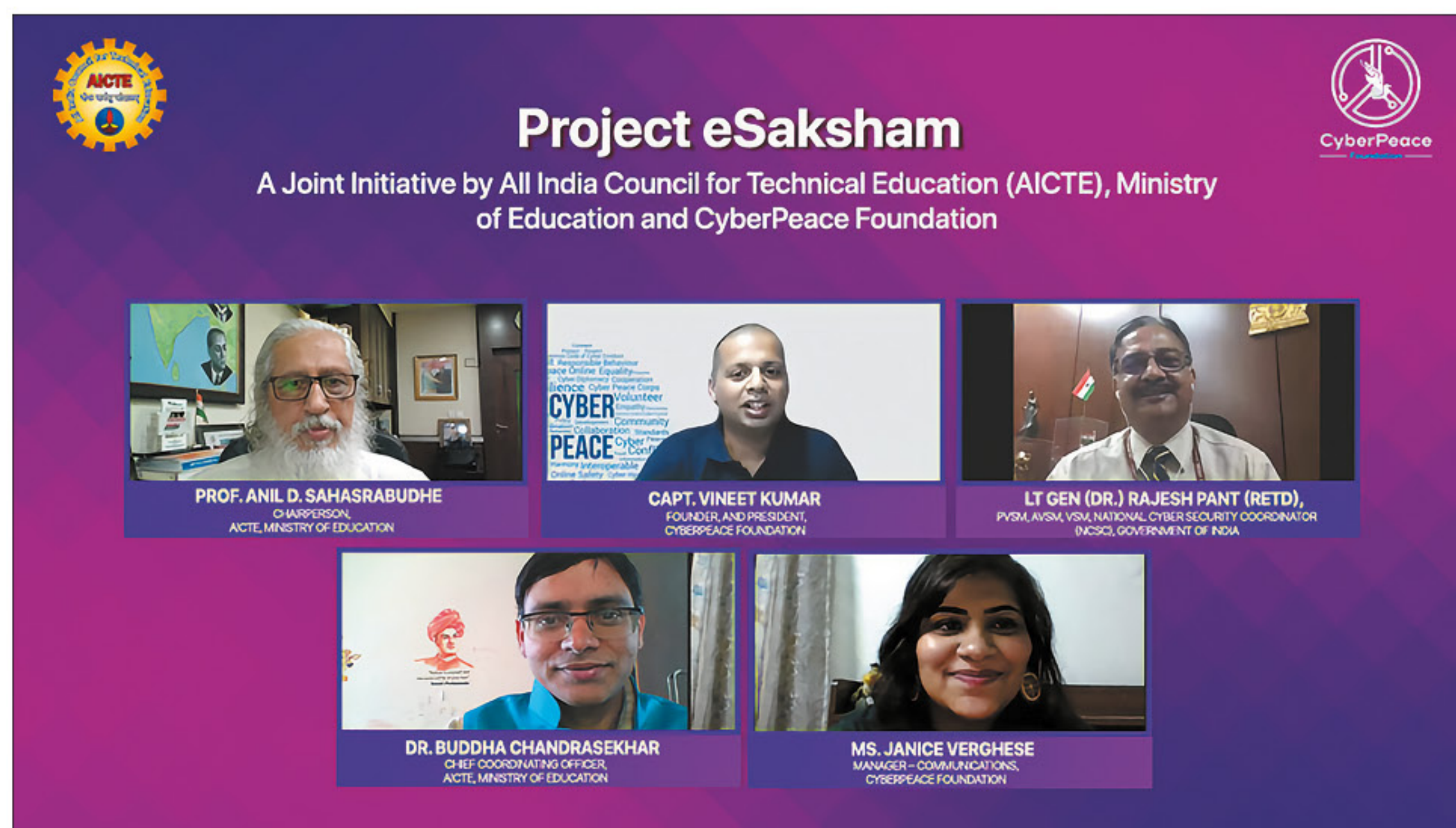
Ещё одна из тенденций в образовании — переход к микрообучению. Времена, когда человек был готов выслушать полтора часа на тренинге или лекции, давно прошли. Типичный сотрудник может сосредоточиться только на одной задаче в течение короткого промежутка времени, прежде чем его прервут. Как показывает практика, в среднем этот промежуток равен 3,5 минутам. После человек отвлекается на звонок телефона, проверку электронной почты и общение с коллегами. Обучение должно понимать этот сдвиг в психологии. Стоит поделить занятия на мелкие временные рамки, чтобы предоставлять небольшие порции информации.

Добавление игры в процесс обучения помогает привлечь сотрудников и сохранить их интерес к теме. Исследование, проведённое Science Direct, свидетельствует о том, что геймификация на основе задач в образовании приводит к увеличению измеримых результатов на 34,75 %.

Микрообучение и геймификация идеально подходят для любой отрасли, где большая часть рабочей силы — поколение миллениалов. Этот подход востребован для отраслей, которые широко используют компьютеры, а персонал работает в офисе. Хотя такое обучение можно адаптировать где угодно.

Переход к удалённой работе и размытие границ организаций потребовали от сотрудников компаний базовых знаний в области кибербезопасности. Возникли угрозы, исходящие от людей, работающих с документами и потенциально конфиденциальной информацией за пределами традиционного рабочего места. Это часть нашего нового мира, и возврат к старому маловероятен.

Многие в технологическом сообществе понимают, что пандемия COVID-19 стала поворотным моментом, который заставил бизнес кардинально измениться. Постоянное обучение, принятие новых эффективных требований, адаптация и развитие новых навыков помогут противостоять постоянно меняющимся угрозам. Изменения становятся единственной константой в постоянно меняющемся мире, считает Хизер Стратфорд.



Индийский проект eSaksham направлен на обучение студентов и преподавателей азам кибербезопасности

ИНДИЯ ГОТОВИТ НОВЫЕ КАДРЫ

Всеиндийский совет по техническому образованию (AICTE) совместно с Министерством образования и Фондом CyberPeace (CPF) запустили проект по информационной безопасности под названием eSaksham. Он направлен на обучение студентов и преподавателей азам кибербезопасности.

Согласно данным отчёта Национальной ассоциации компаний — разработчиков ПО и сервисных компаний (NASSCOM) за 2020 год, в Индии не хватает 1 млн профессионалов в области информационной безопасности, к концу 2021 года в отрасли будет около 3,5 млн вакансий в области кибербезопасности.

Основная цель программы повышения цифровой осведомлённости о кибербезопасности — создание экосистемы, в которой исследовательские работы могут быть преобразованы в готовые к реализации проекты.

Проект eSaksham включает тренинг, который будет проводиться на четырёх уровнях. Уровень 1 — двухчасовой онлайн-семинар по основным концепциям навигации в киберпространстве, включая кибербезопасность, сетевой этикет и введение в новые технологии, участвовать в нём могут все желающие.

На уровень 2 перейдут кандидаты по итогам теста, проведённого после уровня 1. Планируется, что четырёхдневный онлайн-семинар охватит 25 тыс. участников.

Уровень 3 рассчитан на 5 тыс. человек, отобранных на предыдущих этапах. Онлайн-семинары продлятся неделю и будут посвящены безопасности Интернета вещей, облачной безопасности, блокчейн-технологиям и безопасности инфраструктуры.

На последний — уровень 4 — перейдут 500 кандидатов. Они пройдут месячный интенсивный тренинг, проводимый в сотрудничестве с правительством, академическими кругами и предприятиями. Под руководством наставников студенты получают доступ к лабораториям для дальнейшего развития навыков в области ИБ. Выпускники получают сертификаты AICTE и CPF.

Ожидается, что в рамках реализации онлайн-программы появятся 25 тыс. волонтеров Корпуса CyberPeace и будет создано более 50 клубов CyberPeace по всей Индии.

РЫБАК РЫБАКА...

2020 год был не похож на другие, пишет специалист в области ИБ Эрик Крон в сетевом издании Security Magazine. Глобальная пандемия современности потрясла мир и нарушила привычный образ жизни, заставив всех адаптироваться к новым условиям в кратчайшие сроки. Вместо похода в офис — конференция онлайн, вместо обеда с коллегами — обед с семьёй, и даже запасы туалетной бумаги стали необходимостью.

Людям сложно адаптироваться к переменам, особенно в условиях

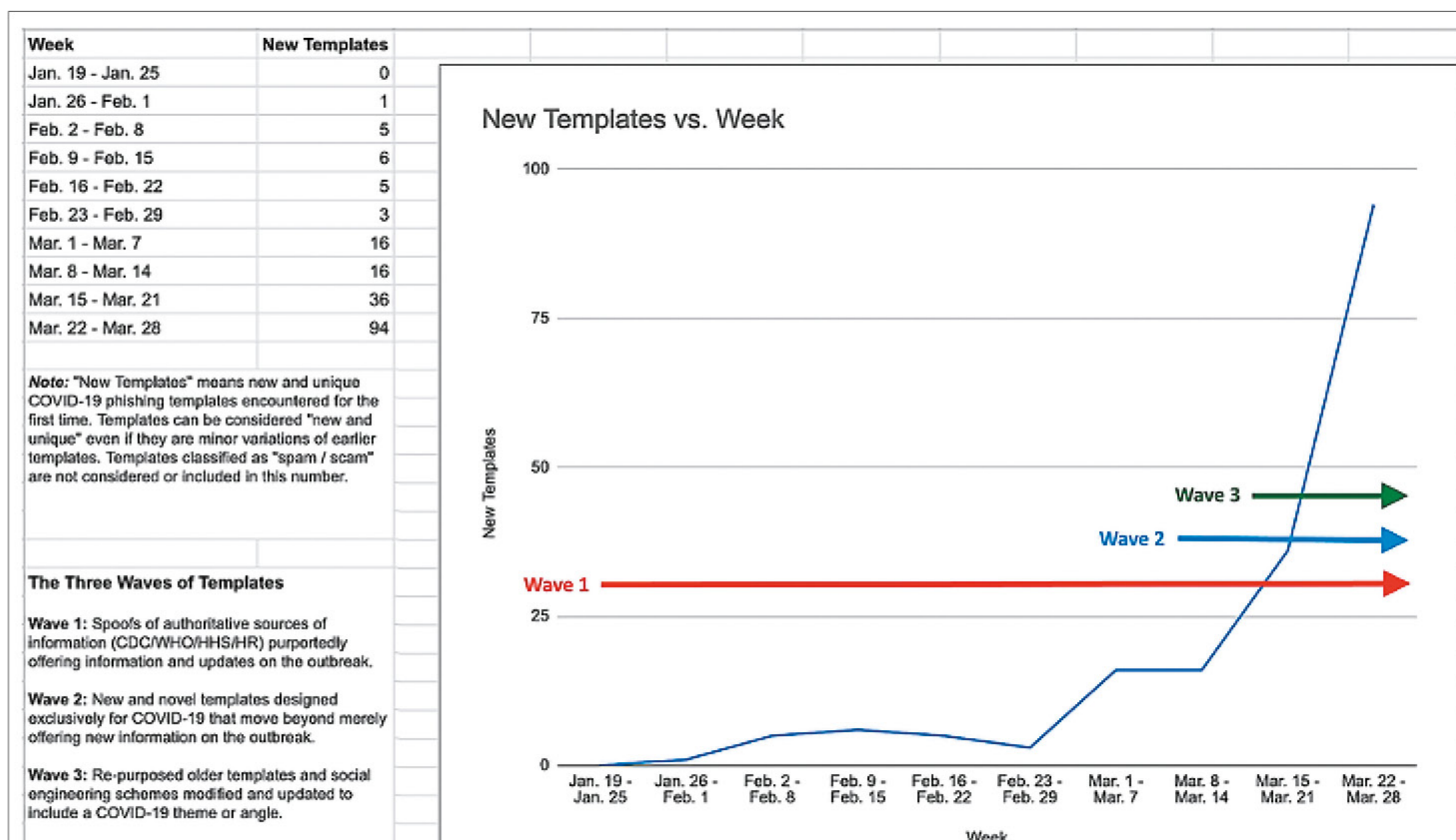


Рисунок 1. Новые шаблоны фишинга для COVID-19 по неделям. Источник: <https://www.securitymagazine.com/articles/95253-the-pandemonium-of-the-pandemic-how-working-from-home-has-changed-the-cybersecurity-formula>

продолжающейся экономической борьбы, политических потрясений и общего чувства неуверенности. Это трудное время для людей как в профессиональном, так и в личном плане. И — благодатная почва для мошенников.

Основной рецепт мошенничества почти всегда один и тот же. Мошенник заставляет жертву доверять, а затем использует это доверие в своих интересах. Если прежде такой исход грозил потерей денег или собственности, то сегодня к финансовым или имущественным потерям добавились информация и доступ к ресурсам.

За долгие годы тренировок мошенники отточили своё мастерство. История с принцем Нигерии начиналась как афера с использованием возможностей традиционных почтовых служб. Переход в виртуальное пространство упростил рассылку и снизил затраты: отправка 50 тыс. фишинговых писем через почтовые службы даркнета стоит \$65. Отправка бумажных писем 50 тыс. респондентам обойдётся в \$27,5 тыс. только за одни марки. Неудивительно, что фишинг по электронной почте так популярен.

За прошедшие годы мошенники выяснили, какие эмоциональные ловушки работают лучше всего, и знают, как противостоять практически любым возражениям или подозрительным вопросам. Они используют психологические уловки, чтобы цель оставалась в состоянии сильных эмоций. Страх, возмущение, гнев, услужливость... Эмоции заставляют людей принимать неверные решения. Этим успешно пользуются киберпреступники.

Стресс и паника первых дней пандемии, переход на онлайн-обучение и удалённую работу и даже отсутствие дома нужной для «удалёнки» техники — всё стало золотой жилой для мошенников.

В первые недели после отключений, связанных с COVID-19, киберпреступники сосредоточились на создании новых атак. На рисунке 1 показано резкое увеличение числа новых шаблонов фишинга, связанных с COVID-19, в течение нескольких недель после начала карантина.

Фишинговые письма различались по темам, содержанию и целям, однако почти все они были сосредоточены на неопределённости в жизни людей в

условиях пандемии. От имени правительства или глобальных организаций (например, ВОЗ) потенциальным жертвам предлагали ознакомиться с «обновлёнными инструкциями». Ссылки вели на документы, заражённые вредоносными программами, или на поддельные порталы, требующие конфиденциальной информации для «подтверждения» личности жертвы. Другие схемы использовали информацию о материальной помощи от правительства для сбора личной информации и доступа к банковским счетам. Поддельные мобильные приложения под видом отслеживания контрактов COVID-19 занимались распространением программ-вымогателей.

Помимо фишинга, процветало мошенничество с реализацией дефицитных в первые недели средств индивидуальной защиты (СИЗ), дезинфицирующих средств для рук и т.д. «Липовые» поставщики СИЗ помогли избавиться от денег многим организациям, в том числе больницам и исследовательским центрам. Со временем число поддельных сайтов производителей уменьшилось, однако до сих пор в сети можно нарваться на мошенников.

Спустя год на смену одним проблемам приходят другие. Рост цен на сырьё, нарушение логистики в результате закрытия сообщения между странами, остановка экспортно-импортных операций привели к дефициту товаров и комплектующих. Чем не преминули воспользоваться мошенники.

Продолжая бороться с пандемией, мы должны помогать людям учиться распознавать мошенничества, полагает автор статьи. Независимо от того, что является их целью: кража данных, личных сведений или денег — последствия будут значительными на личном уровне или на уровне организации. Информирование людей об опасностях, а также о методах выявления мошенничества и защиты себя сегодня особенно важно.

БРИТАНСКИЕ УЧИТЕЛЯ НА ПЕРЕДОВОЙ

Национальный центр кибербезопасности Великобритании (NCSC) выпустил бесплатный учебный пакет по кибербезопасности для учителей и школьных работников, описывающий практические шаги по ИБ, чтобы помочь преподавателям повысить свою защиту в ходе онлайн-обучения. На основе реальных примеров из жизни продемонстрировано влияние таких инцидентов на учебный процесс, пишет издание Computer Weekly.

Новый ресурс стал очередным дополнением к расширяющемуся пакету мер поддержки, предлагаемых NCSC для школ и университетов Великобритании. Учебные заведения страдают от волны кибератак, которые захлестнули образовательные учреждения в период пандемии COVID-19 и перехода сектора в онлайн. Атаки на школы не снижаются даже с возвращением очного обучения.

Министр школ Ник Гибб отмечает, что жизненно важно, чтобы в школах была надёжная киберзащита, и новые ресурсы и обучение помогут персоналу повысить кибербезопасность. Новый тренинг даст школьному персоналу инструменты и навыки, необходимые для выявления возможных рисков.

Учебный пакет адаптирован для сотрудника с любым уровнем подготовки и технических знаний. Это презентация,

доступная по ссылке, обучение ведётся по сценарию, описывающему самые опасные угрозы, с которыми сталкиваются школы, и последствия успешных кибератак.

Так, в одном из тематических исследований описывается инцидент, в ходе которого была проведена успешная голосовая фишинг-атака, в ходе которой киберпреступники выдавали себя за Министерство образования, чтобы получить данные электронной почты главы финансового отдела и директора школы. Затем директору было отправлено персонализированное фишинговое электронное письмо, которое при открытии загружало программы-вымогатели. Они распространялись по локальной сети, шифруя школьные данные. Кибермошенники потребовали £8 тыс. за ключ для дешифрования.

В другом примере киберпреступники атаковали независимого администратора школы, используя фишинговые электронные письма, чтобы украсть контактные данные родителей. Хакеры выдавали себя за специалиста по аудиту и контролю за соблюдением требований законодательства. Получив нужные данные, мошенники от имени школы отправили по электронной почте родителям новые банковские реквизиты для оплаты обучения. Персональные данные родителей также использовались в других мошеннических схемах.

Ещё один пример — оплошность учителя, который оставил свой системный пароль записанным на стикере. Этим воспользовался ученик школы, который изменил свои оценки. А учебное заведение попало под санкции Управления комиссара по информации (ICO) за нарушение Закона о защите данных.

Согласно тренингу, есть четыре основных шага, которые должен соблюдать школьный персонал:

1. Сократить объём общедоступной информации о себе в социальных сетях, чтобы защититься от попыток фишинга. Если получатель не уверен в достоверности письма — обратиться к профессионалам за помощью.

2. Использовать надёжные и оригинальные пароли для разных учётных записей, по возможности использовать двухфакторную аутентификацию.

3. Для защиты устройств необходимо устанавливать обновления, загружать программное обеспечение только из официальных источников. Блокировать экраны, если они не используются.

4. В случае возможных инцидентов как можно скорее сообщать о подозрениях.

АМЕРИКАНСКИЕ УЧИТЕЛЯ ИЗУЧАЮТ КРИПТОГРАФИЮ

Летом этого года 40 школьных учителей нескольких земель в штате Пенсильвания пройдут недельное онлайн-обучение в летнем лагере GenCyber, организованном Общественным колледжем в Шнексвилле, штат Пенсильвания, в районе Лихай-Вэлли. Колледж, уже становившийся лидером образования в области ИБ (по оценке АНБ и Министерства внутренней безопасности США), на сей раз получил грант от Агентства национальной безопасности и Национального научного центра и проведёт онлайн-тренинги для местных учителей начальной, средней и старшей школы.

В программе обучения — как базовые вопросы устройства компьютеров и компьютерных сетей, так и азы криптографии, кибербезопасности, безопасного поведения в Интернете и киберэтики. Участники летней школы получают практический опыт, а также узнают, как интегрировать новые знания в учебные программы на соответствующем возрасту уровне. В рамках последующей годовой программы учителям окажут поддержку по вопросам использования полученных знаний в школьных курсах. Помимо этого, каждый участник тренинга получит стипендию в размере \$500.

Федеральная программа летних лагерей GenCyber для студентов и учителей проводится по инициативе и поддержке Агентства национальной безопасности и Национального научного центра. Она и является ответом на необходимость повышения осведомлённости о кибербезопасности и обучения основам кибербезопасности на разных уровнях образования. Цели программы GenCyber — не только повысить знания школьников и учителей в области ИБ, но и развить интерес к карьере в области кибербезопасности в будущем.



Рустэм ХАЙРЕТДИНОВ
эксперт BIS Journal

ТОЛЬКО СЛУШАЯ БИЗНЕС

МОЖНО ПРИБЛИЗИТЬСЯ К РЕШЕНИЮ КАДРОВЫХ ПРОБЛЕМ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

По различным исследованиям, более 60 % руководителей считают проблему нехватки кадров в ИТ основным препятствием для цифровой трансформации, а остальные 40 % считают, что эта проблема входит в тройку основных препятствий. Об этой проблеме говорят на каждой ИТ-конференции, её понимают на государственном уровне. По разным оценкам, в стране прямо сейчас ощущается нехватка от 300 тысяч до миллиона квалифицированных ИТ-специалистов. Спрос кратно вырос, поскольку практически каждая компания сегодня так или иначе втянулась в цифровую трансформацию, что требует вовлечения таких специалистов: архитекторов, программистов, инженеров внедрения и поддержки, специалистов по кибербезопасности, аналитиков, цифровых маркетологов, продуктовых менеджеров и т.п. В сочетании с демографическим спадом это выливается в годами не закрываемые вакансии и рост зарплат.

Свою лепту внесла и пандемия. И не только тем, что подхлестнула спрос на определённых специалистов из-за повысившихся требований к ИТ-инфраструктуре, поддерживающей удалённую работу. Компаниям пришлось преодолеть страх нанимать людей, которых никогда не видел вживую, да и законодательство о дистанционной работе оперативно подтянулось. Теперь для того, чтобы специалисту работать на зарубежную компанию, не нужно эмигрировать и физически переезжать — можно получать зарплату в твёрдой валюте,

не меняя привычного окружения. Лично знаю семью, в которой из подмосковного дома муж удалённо работает на компанию в Арабских Эмиратах, а жена — на компанию со штаб-квартирой в Амстердаме, поэтому она встаёт и ложится на час попозже. Это ещё больше усилило конкуренцию за кадры, сократив затраты нанимателей на релокацию и социальную адаптацию специалистов.

В общем, людей нет и, сколько бы мы их ни готовили, их никогда не будет достаточно. Но цифровую трансформацию не остановить, поскольку после многих лет экспериментов компании и государства стали ощущать реальную пользу от информационных технологий в бизнесе и госуправлении. Удешевление привлечения и обслуживания клиентов, оптимизированная логистика, быстрое реагирование на изменения среды, прозрачность и контроль, возможность предотвращать, а не расследовать потери, в общем, всё то, из-за чего профессор Аузан назвал цифровую экономику «экономикой сверхдешёвых транзакций». Бизнес уже вряд ли откажется от этого, поэтому проблему кадров всё равно придётся решать.

Проблема настолько комплексная, что решать её придётся по нескольким направлениям.

ОРГАНИЧЕСКИЙ РОСТ ЗАРПЛАТЫ

Поскольку на больших периодах срабатывает рыночный закон баланса спроса и предложения, зарплаты повысятся настолько, что отток специалистов за рубеж прекратится, и к нам самим

потекут специалисты из-за рубежа. Это не выглядит невозможным: сегодня такое уже происходит для дефицитных специалистов в науке и корпоративном управлении, и такое происходит всё чаще.

При этом повысится и интерес к профессии у колеблющихся абитуриентов, ранее считавших, что профессия ай-тишника это «скучно и только для ботанов», а также у людей, проходящих переподготовку по смене профессии.

Конечно, рост затрат ляжет дополнительным бременем на потребителей продуктов цифровизации, в которой фонд оплаты труда специалистов составляет подавляющую часть. Возможно, многие проекты в цифровизации в таких условиях окажутся не такими эффективными, но, если нам нужны специалисты, придётся за это заплатить. Но если ты разрабатываешь систему, которая эффективна только при низких зарплатах разработчиков, может быть, стоит пересмотреть сразу бизнес-модель?

АВТОМАТИЗАЦИЯ

Став дорогим, ручной труд будет всё более востребован. Конечно, цифровые профессии не так легко автоматизировать, но и над этим идёт работа, которая всё интенсивнее с ростом затрат на людей.

Ещё пять лет назад рассказы о том, что программистов заменят программные роботы, выглядели скорее троллингом, но сегодня всё выглядит уже не так однозначно. Не только роботы стали умнее, но и само программирование

стало другим. Сегодня в большинстве бизнес-систем до 80 % кода — это уже ранее написанный код, и мало кто пишет целиком программы с нуля, скорее собирает из готовых частей. А с этим может неплохо справиться и робот. Системы визуального программирования lowcode/no-code хотя и выглядят пока сырыми, с каждым годом всё больше похожи на реальный рабочий инструмент. Основной двигатель их развития — дефицит кадров и связанное с этим увеличившееся время ожидания автоматизации типовых задач.

ПОДГОТОВКА КАДРОВ

Про это много уже сказано и написано, государство и крупные компании уже системно работают над этой проблемой. На уровне государства пишутся образовательные программы, вводятся новые специальности, создаются новые учебные места в университетах, переподготавливаются преподаватели, вкачиваются средства в подготовку высокотехнологичного процесса обучения. С помощью СМИ и массового искусства повышается престиж профессии айтишника, распространяется имидж «быть айтишником круто». Разрушается когда-то доминировавший стереотип «ИТ для мужчин», в отрасль приходят прекрасные дамы, которые на равных конкурируют с мужчинами, получая равное вознаграждение за равный труд.

Не отстаёт и бизнес, не очень привыкший у нас ждать милостей от государства и спешащий взять важную проблему под свой контроль. Крупные ИТ-компании создают свои полноценные университеты, компании поменьше — строят специализированные учебные центры и берут шефство над государственными университетами, профильными факультетами или кафедрами — у кого насколько болит кадровая проблема.

Стало доброй традицией за символическую плату или вообще бесплатно делегировать специалистов из успешных цифровых бизнесов в высшие учебные заведения и даже школы. Преподаватели не только несут студентам и школьникам актуальные знания, но и присматриваются к самым успешным ученикам как к потенциальным сотрудникам.

РАЗВИТИЕ ИТ КАК ДОПОЛНИТЕЛЬНОЙ СПЕЦИАЛЬНОСТИ

Довольно часто с небольшими задачами внутренней автоматизации могут справиться и профильные специалисты, если их научить основам программирования. Особенно это касается задач автоматизации обработки данных. Например, для финансистов программирование макросов в электронных таблицах стало уже частью профессии, и для финансового анализа уже давно не надо привлекать внешних автоматизаторов. Эта практика уже распространилась на интернет-маркетологов, которые самостоятельно с помощью встроенных языков программирования оптимизируют рекламные кампании и затем анализируют их эффективность. Айтишники и безопасники в поисках причин сбоев и целевых атак перелопачивают огромное количество неструктурированной информации из журналов — обычно они самостоятельно разбираются с автоматизацией этого процесса, что существенно снижает нагрузку на отдел внутренней автоматизации. Есть прогнозы, что знание языков программирования со временем станет таким же обязательным дополнительным навыком, как знание офисных продуктов и иностранных языков.

АУТСОРСИНГ

Дефицит людей часто покрывается аутсорсингом, особенно если задачи автоматизации не загружают штатные единицы равномерно. Сегодня выбор внешних сервисов огромен — от больших компаний, готовых взять на аутсорсинг целиком бизнес-процесс, до частных фрилансеров. Важно в этом случае контролировать результат работы аутсорсеров, но создание «службы

заказчика», которая определяет рамки задачи и критерии успешности, обычно улучшает управляемость. Если всё корректно посчитать и настроить, то вы сможете очень эффективно управлять процессом, а в случае правильно написанного соглашения об уровне сервиса (SLA) — и получать компенсации, что невозможно в случае выполнения работ собственными сотрудниками, которым в случае провала проекта вы сможете только объявить выговор.

Риски аутсорсинга хорошо известны — это и зависимость от исполнителя, и проблемы доверия. Поэтому, конечно, на аутсорсинг надо выводить процессы, не составляющие ядро бизнеса, и очень чётко их регламентировать. Обязательно надо иметь возможность быстро переключиться с одного аутсорсера на другого, а для этого надо очень точно прописывать в соглашениях стандарты, требования к документированию и полную передачу информации, продуктов и документации в случае разрыва соглашения. Но в экономике с хроническим отсутствием кадров аутсорсинг часто остаётся единственным выбором.

ПОСТРОЕНИЕ КАДРОВЫХ ПРОЦЕССОВ

Как уже писалось выше, пока зарплаты в российских компаниях ниже, чем в мире, мы должны быть всегда готовы к тому, что лучших людей у нас будут забирать крупные западные и, с недавних пор, восточные компании. Поэтому многие компании выстраивают кадровый процесс именно с учётом этой неизбежности. Каждый ключевой специалист «подпирается» заместителем, специалистом меньшей квалификации, перенимающим опыт и полностью погружающимся

Каждый ключевой специалист «подпирается» заместителем, специалистом меньшей квалификации, перенимающим опыт и полностью погружающимся в задачу и методы её решения. Так происходит по всей цепочке от руководителя направления до младшего специалиста



в задачу и методы её решения. Так происходит по всей цепочке от руководителя направления до младшего специалиста, которого «подпирают» стажёром. Когда ключевой специалист покидает компанию, вся цепочка сдвигается на одну позицию вверх, то есть люди растут достаточно быстро, что хорошо для образа компании на рынке, при этом не теряется преемственность, что хорошо для бизнеса. Конечно, эта схема избыточна, приходится держать на проекте несколько больше людей, чем это необходимо, но такой подход позволяет избежать рисков остановки проекта из-за ухода ключевого разработчика.

ЛИЧНЫЙ ОПЫТ

Вышеописанное — не теория, а систематизация многолетней практики в построении команд разработки продуктов,

инженеров-внедренцев, продавцов/пресейлов, специалистов в области кибербезопасности, аналитиков, аудиторов и других. Бизнес в области информационной безопасности, особенно быстрорастущий, как наш, постоянно находится в состоянии нехватки кадров, а упомянутые выше специальности всегда в дефиците. Наверняка это не уникальные знания, то же самое делают руководители большинства ИТ/ИБ-компаний.

Мы понимаем, что кадровый рынок в ИТ/ИБ — это рынок продавца, сотрудники выбирают компании, а не наоборот. Мы не считаем уход из компании предательством, сохраняем хорошие отношения с большинством покинувших компанию сотрудников, поддерживаем встречи «выпускников» компании. Мы не считаем, что уходящие сотрудники уносят от нас какие-то секреты, в

нашем мире все секреты быстро становятся общедоступны.

Поэтому мы очень активны на рынке найма, охотимся за лучшими кадрами и много усилий тратим на удержание своих. Мы выделяем ключевых сотрудников, иногда их называют «ДНК компании», то есть компания без них уже будет не той компанией, какой является сегодня. Этим людей мы удерживаем всеми силами. Понятно, что это не только зарплаты и премии, на постоянное поддержание компенсации выше рынка не хватит никаких бюджетов. Что можно предложить айтишнику, кроме денег? На самом деле много чего. Айтишники, достигнув определённого уровня доходов, ценят:

- ◆ свободный график, частичную или полную удалёнку по желанию, поддержание work/life-баланса;
- ◆ если это офис, то транспортно доступный и со всеми удобствами, бесплатными «плюшками» типа кофе и парковки, спортзалом, компьютерными играми, комнатами для сна и отдыха;
- ◆ интересные корпоративные мероприятия;
- ◆ постоянное обучение профессии как в рабочее время, так и с отрывом от производства, с получением сертификатов;
- ◆ работа над личным брендом через выступления на конференциях и публикациях;
- ◆ возможность работать с дорогими игрушками и масштабными проектами;
- ◆ возможность общаться по работе с лидерами мнений в профессии как внутри компании, так и на стороне заказчиков;
- ◆ возможность творчества на работе, например, сотрудники могут часть рабочего времени посвящать сопутствующим pet projects;
- ◆ компенсации для медицинских и фитнес-сервисов типа ДМС.

Разным людям важны разные нематериальные стимулы. Кто-то хочет работать из своей дачи и никогда не появляться в офисе, а кому-то важно регулярно общаться с коллегами. Для кого-то возможность посмотреть страну и мир в командировках — мощный стимул, а кто-то боится летать и предпочёл бы работать в комфортном офисе.

Кто-то по жизни одиночка и тяготеет к командной работе, а для кого-то наиболее важно работать в крутой команде. Кого-то мотивирует работа над крупнейшим в стране или на континенте внедрением, а кому-то важно работать над своим личным проектом. Поэтому под каждого носителя ДНК компании выбирается специальный план.

Всё, что можно аутсорсить без создания дополнительных рисков для бизнеса, аутсорсится в приоритетном порядке. Мы, как сервисная компания, хорошо научились считать риски аутсорсинга и минимизировать их. Поэтому, если есть возможность не брать человека в штат, а взять на ту же работу компанию или человека на контракт, выбор, скорее всего, будет сделан в пользу аутсорсинга.

Много работаем со стажёрами, много берём младших специалистов и учим их. В менеджменте компании уже четверть составляют люди, которые четыре-пять лет назад пришли в компанию на средние и даже начальные позиции и быстро выросли до руководителей.

Большинство наших старших специалистов и руководителей преподают в университетах, параллельно подыскивая себе сотрудников. Я и сам много преподаю — и в МВА, и в университетах, и на курсах повышения квалификации. Выступаю руководителем одного-двух дипломов ежегодно, на большее без потери качества просто не хватает времени. И даже если наши студенты и дипломники достаются нашим конкурентам, ничего страшного, мы все работаем на насыщение рынка специалистами, что в итоге хорошо и для рынка в целом, и для каждого игрока рынка в частности.

Мы развиваем менторство и наставничество, каждый руководитель не просто раздаёт задания и проверяет их исполнение, но и работает с сотрудником, помогая ему расти. Я сам время от времени езжу с нашими сейлами и пресеями на сложные переговоры, подхватывая их, если сотрудник вдруг сбивается. Я езжу не контролировать их, а помогать, страховать, поэтому они чувствуют себя свободно и уверенно. Иногда приходится брать переговоры в свои руки, и тогда сотрудник просто

Всё, что можно аутсорсить без создания дополнительных рисков для бизнеса, аутсорсится в приоритетном порядке. Мы, как сервисная компания, хорошо научились считать риски аутсорсинга и минимизировать их

получает мастер-класс по переговорам. Иногда я ничего не говорю на встрече, только здороваюсь и прощаюсь, значит, в моём присутствии сотрудник всё проводит как надо. Такой опыт нельзя получить на тренинге, только при живых контактах. То же делают и все другие руководители, личным примером выращая сотрудников.

Чего греха таить, люди уходят и от нас. Около 10% сотрудников покидают нас ежегодно, подавляющее большинство уходит на более высокие должности и более амбициозные проекты. Иногда мы сами закрываем проекты и пытаемся перераспределить их команды внутри компании, но новые позиции подходят не для всех. Контакты с «выпускниками» — это отдельная работа, мы не теряем контактов с ними и держим их в поле зрения на тот случай, если у нас возникнет проект, соответствующий их квалификации. Мы рады их видеть в нашем офисе как партнёров, заказчиков или просто гостей, а вне офиса мы чаще всего видим на «афтепати» профильных конференций. Иногда бывшие коллеги, поработав пару лет в другой компании и поднабравшись опыта, возвращаются к нам на новую позицию.

Мы кадрово резервируем все ключевые позиции, имеем план на случай ухода любого сотрудника, знаем, как распределим позиции и задачи в случае любого форс-мажора. Держим «кадровый резерв», то есть общаемся со специалистами в других компаниях, которые готовы поговорить о переходе к нам, но не спешат это делать. Много ищем людей в регионах, в случае найма помогаем с адаптацией в столице или других городах нашего присутствия.

Много работаем и над автоматизацией рутинных процессов, таких, например, как первая линия SOC, анализ событий в антифроде и пентесты.

Это позволяет загружать специалистов творческими задачами, а скучный анализ данных доверить нейросетям. Инструменты no-code/low-code активно внедряются как во внешних сервисах (правила антифрода, настройки WAF), так и во внутренней автоматизации — документооборот, CRM и другие.

То есть я могу подтвердить, что все описанные в первой части статьи методы работы с кадрами работают, только надо найти правильный баланс их использования. Для каждой компании баланс будет свой, ИТ/ИБ-бизнес неоднороден, и в разных бизнесах ключевыми процессами и сотрудниками окажутся разные люди и процессы. Но методы решения кадровых проблем уже опробованы и обкатаны, бери и применяй.

ЗАКЛЮЧЕНИЕ

Бизнесу сегодня приходится работать в тех условиях, которые есть. Те, кто выживет, адаптируются к существующим условиям, так работает рынок. Бизнес, прежде всего, несёт ответственность за своих клиентов и за своих сотрудников, он не может решать глобальные проблемы типа поддержки рождаемости и изменение системы образования. Если бизнес спрашивают — он делится опытом, если нет, не настаивает, считая найденные им способы решения ключевых проблем своим конкурентным преимуществом.

Пока государство очень далеко от решения проблем кадров для цифровизации. Если оно пустит решение этой проблемы на самотёк, то бизнес адаптируется так, как описано выше. Если государство чем-то поможет, бизнес будет готов инвестировать опыт, время, да и деньги.

Только дайте правила игры и поддержите их неизменными хоть какое-то время.

**Борис СТОЛПАКОВ**историк криптографии,
кандидат физико-
математических наук

СОСРЕДОТОЧЕНИЕ ПЕРЕД ВЗЛЁТОМ

КРИПТОГРАФИЧЕСКАЯ СЛУЖБА СССР В 1930-Е ГОДЫ

Учреждением Спецотдела 5 мая 1921 г. руководители Советской России продемонстрировали свою решимость создать единый центр, отвечающий за организацию защиты секретной информации в стране и одновременно объединяющий и направляющий криптографическую деятельность.

ОТ ДЕКЛАРАЦИЙ К ДЕЛАМ

Важно, что уже вскоре властные декларации были подкреплены конкретными делами и достижениями. Так, к 1927 г. удалось обеспечить надёжную защиту дипломатической переписки и наладить контроль секретного и шифровального делопроизводства в государстве.

В 1930-е годы предстояло решить не менее сложные, но заведомо более объёмные задачи по надёжному обеспечению секретности военной переписки, особенно радиосообщений. В связи с этим рос и потенциал криптографической службы СССР. К середине 1930-х годов она располагала уже в основном оформившимся объединённым криптографическим аппаратом в центре и на местах — в некоторых оперативно важных территориальных органах НКВД, военных округах и флотилиях.

КРИПТОГРАФИЧЕСКИЕ СВЯЗИ СОСЕДЕЙ СССР

О применявшихся тогда советских шифрах и о сложности преодоления их для противника ныне можно судить по опубликованным после Второй мировой войны исследованиям. Их авторы ссылались на документы Польши, Финляндии, Германии и Японии. Надо сказать, что криптографы Польши и Финляндии унаследовали в некоторой мере шифровально-дешифровальный опыт, накопленный в Российской империи. Здесь имеются в виду не только навыки, приобретённые во время службы в российских вооружённых силах, но и оборудование радиоразведывательных и радиопеленгаторных станций Балтийского флота, сосредоточенных на финской территории.

Польские дешифровальщики после своего успеха в Советско-польской войне 1920 г. имели репутацию крупнейших специалистов по взлому советских шифров и руководители сопредельных с СССР государств это учитывали. Не удивительно, что японское командование пригласило в 1923 г. ведущего польского криптографа капитана Я. Ковалевского в Токио. Он провёл там трёхмесячный семинар по основам криптоанализа для сотрудников

японской разведки. По итогам работы семинара японский ГШ (генеральный штаб) подготовил и разослал по соединениям совершенно секретный «Справочник по основам дешифровального дела». Там содержались общие сведения по построению и взлому шифров не только СССР, но и ведущих европейских стран. Развивая начавшееся сотрудничество с польскими специалистами, японский ГШ направил в Варшаву в конце 1925 г. на годичную стажировку двух офицеров, а затем ещё четырёх.

Параллельно японская армия разворачивала на оккупированной китайской территории сеть радиоразведывательных пунктов. Один из них — в Харбине (1932 г.). Он был специально предназначен для сбора информации из СССР. С этого времени японское командование постоянно усиливало дешифровальную службу Квантунской армии. В 1935 г. там было организовано Исследовательское управление, занимавшееся перехватом и дешифрованием советских радиопереговоров.

РЕЗУЛЬТАТЫ РАБОТЫ ГЕРМАНСКИХ ШИФРОВАЛЬЩИКОВ

Дешифровальные подразделения другого важного соседа СССР, Германии,

ФОНД
ПРЕЗИДЕНТСКИХ
ГРАНТОВ

Публикация подготовлена при поддержке гранта Президента Российской Федерации на развитие гражданского общества №21-1-009977, предоставленного Фондом президентских грантов.



Ведущий польский криптограф
Ян Ковалевский

стали заметно развиваться после 1933 г., быстро достигнув качественного прогресса. Поэтому результаты их деятельности особенно интересны. Согласно опубликованным данным, до 1937 г. 70% перехватываемого немцами советского радиообмена приходилось на НКВД, так как подразделения РККА практически не использовали радиосредства. На территории СССР интенсивность армейских радиопереговоров, как правило, возрастала лишь во время крупных манёвров. При этом Красная армия использовала нестойкие при долгом использовании «Переговорные таблицы» (ПТ) и четырёхзначный «Общевойсковой командирский код» (ОКК). Заметим, что ПТ закрывали советскую переписку в звене «полк — дивизия», а ОКК на уровне «полк — корпус». Ручные шифры НКВД, вскрытые немецкими криптоаналитиками в 1934–1941 годах, представляли собой биграммные алфавитно-цифровые, двух- и четырёхзначные системы замены, применявшиеся управлениями округов погранвойск. Из дешифрованной советской переписки немцы черпали сведения о дислокации, организационно-штатном расписании и задачах пограничных войск НКВД от Мурманской области до Крыма и далее вдоль границы с Турцией, Ираном и Афганистаном. Сведения об РККА были не столь полными. Даже вскрыв в 1935 г. четырёхзначный авиационный шифр, немцы довольствовались в основном



Плакат времён советско-финской войны

метеосводками и информацией о передислокации небольших подразделений вместе с состоянием их материальной части. Но, начиная с 1937 г., радиообмен РККА стал постоянно расти. Этим дешифровальная служба вермахта сумела воспользоваться, она добыла для командования подробные сведения о реформах в Красной армии. В сентябре 1939 г. дешифровальщики сумели вскрыть шифр «ОКК-5», закрывавший переписку советских ВВС, а в ходе Советско-финляндской войны (1939–1940) они раскрыли несколько двух-, трёх- и четырёхзначных шифров РККА. Здесь необходимо подчеркнуть, что успех сопутствовал немцам в основном в случаях нарушения советскими шифровальщиками правил использования засекреченной связи.

РАССТОЯНИЯ НЕ ПОМЕХА

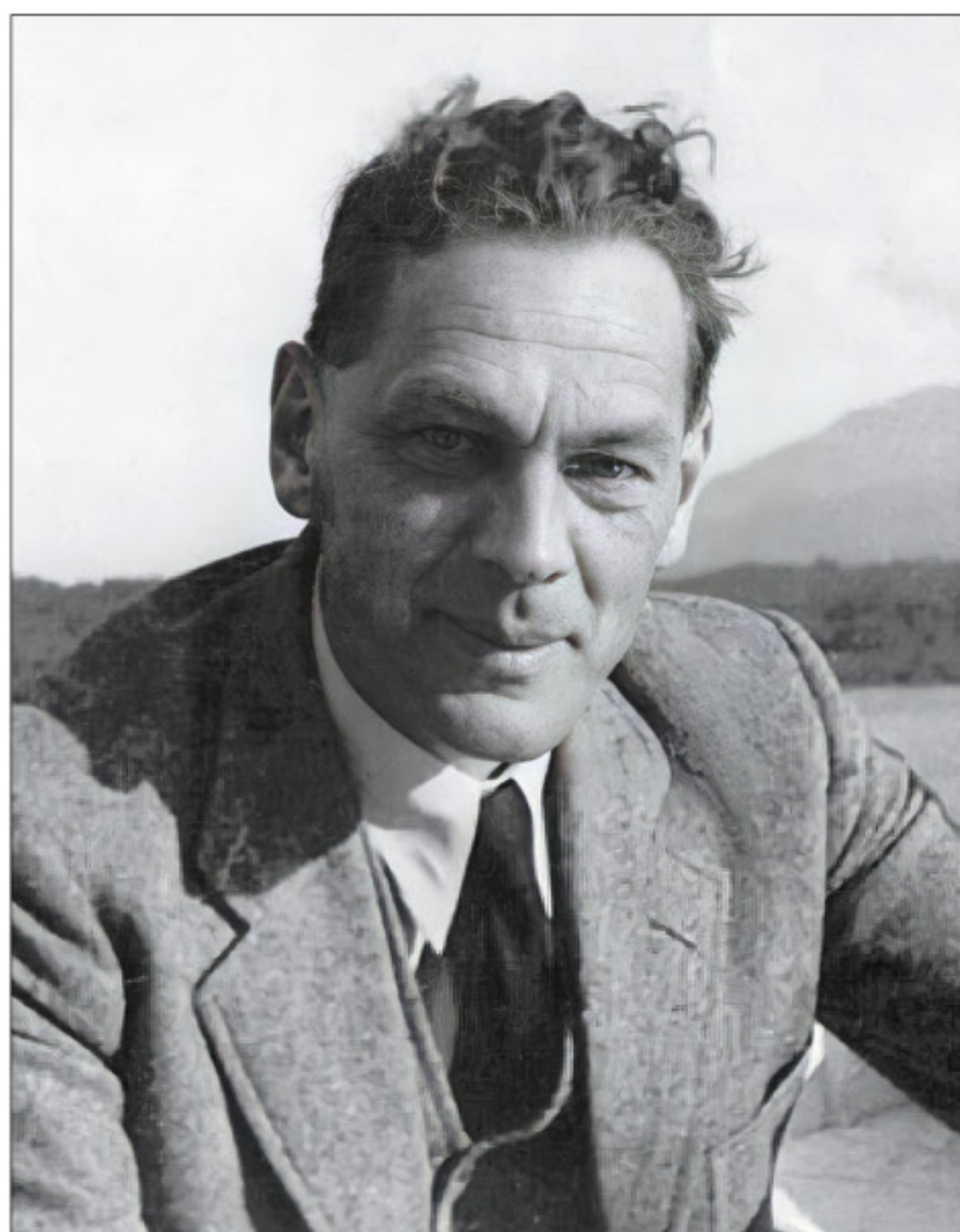
Стоит отметить, что польские криптографы справились с «ОКК-5» ещё раньше и в 1936 г. польский ГШ передал копию этого кода для использования дешифровальщиками Квантунской армии. Успехи японцев начались годом ранее, а получив копию кода они сумели раскрыть шифр «ПК 1» погранвойск и постепенно взломали ручные трёх- и четырёхзначные шифры РККА. Хотя эти шифры не применялись для передачи важных сообщений, всё же их знание позволило японцам установить дислокацию войск в нескольких советских

приграничных гарнизонах, а также расположение и перемещение ряда авиационных частей. Вскоре такая информация пригодилась. В ходе конфликта в районе озера Хасан особенно ценными для японского командования стали расшифрованные советские радиogramмы о переброске танковых подразделений из Владивостока.

Обе стороны конфликта сделали серьёзные выводы о недостатках в работе своих шифровальных служб. Важно, что прямым следствием хасанских событий стала техническая модернизация шифрорганов РККА, в том числе ввод в эксплуатацию электромеханических шифраторов. Шифровальная аппаратура В-4 приняла боевое крещение летом 1939 г. на реке Халхин-Гол. Тогда её использовали для связи штаба армейской группы с ГШ РККА. Как и ожидалось, новая аппаратура и шифры надёжно защитили переписку. Криптографы противника, а вместе с ними и японские войска потерпели поражение.

Вновь на помощь японцам пришли польские криптографы. В марте 1940 г. до расположения Квантунской армии добрался поручик М. Школа. С его поддержкой год спустя армейской дешифровальной службе удалось взломать четырёхзначный советский шифр и в течение долгого времени отслеживать изменения в его ключах.

Зимняя война СССР и Финляндии привела к появлению новых возможностей для японских криптоаналитиков.



Рихард Зорге, агент ОМС Коминтерна



Б. А. Аронский



С. С. Толстой

Первые японо-финские контакты в дешифровальной сфере начались после ввода в дивизионном звене РККА нового шифра «ОК-40», не поддавшегося японским криптографам. Финские специалисты сумели взломать этот шифр во время Зимней войны и в августе 1940 г. передали его копию в Квантунскую армию. Благодаря этому, японцы сумели раскрыть армейский, авиационный и флотский шифры и до конца 1940 г. читали переписку советских войск. Испытывая недостаток средств, финны предложили японскому командованию направить в Хельсинки офицера для обучения и совместной работы над советскими шифрами в обмен на финансирование их дешифровальной службы Японией. Уже в 1940 г. в Токио приняли предложение и направили своего представителя.

«С ТОВАРИЩЕСКИМ ПРИВЕТОМ!»

Спецотделу ОГПУ тоже было с кем кооперировать свою криптографическую деятельность. Ещё в июле 1921 г. Исполком Коминтерна (ИККИ) сформировал Отдел международных связей (ОМС). Его главной задачей стала реализация конспиративных связей между ИККИ и коммунистическими партиями. К 1930-м годам отдел располагал штатом оперативных работников, шифровальщиков, радистов, а также производственной базой для изготовления документов, мощным радиоцентром,

школой для одновременного обучения шифровальному делу и средствам связи около ста человек из разных стран. А главное, ОМС поддерживал связь с довольно эффективной агентурой по всему земному шару. К наиболее известным ныне агентам ОМС Коминтерна можно отнести Рихарда Зорге. Нередко агенты сообщали в ОМС важные сведения криптографического характера. Так, в 1935 г. в Москву на конгресс Коминтерна прибыл представитель китайских коммунистов с секретным подарком — японскими кодовыми книгами. Генеральный секретарь ИККИ Г. Димитров немедленно переправил японские коды Г. И. Бокию в Спецотдел «с товарищеским приветом».

Сложное поручение, связанное с доставкой в Москву японских кодов, исходило от члена ИККИ Чжоу Эньлая, одного из руководителей китайской компартии. Сам он не смог прибыть в Москву на конгресс, поскольку в тот момент возглавлял штаб «Великого похода» (1934–36 г.г.). Так стали именовать передислокацию Красной армии Китая из южных районов Китайской советской республики на её северную территорию. Поход проходил в условиях постоянных боёв с войсками Чан Кайши. Тогда общая борьба с Японией сочеталась в Китае с обстановкой гражданской войны.

Интересную для нас информацию о китайских событиях того времени сообщил в своих публикациях американский

журналист Г. Солсбери: «Красная армия располагала исключительно ценным секретным достоянием. Она могла расшифровывать и читать каждое сообщение националистов... Заслуга в этом во многом принадлежит Чжоу Эньлаю. Начиная с 1930 г., когда он отвечал в партии за безопасность и находился в тесных отношениях с Москвой, он договорился об обучении китайских специалистов в области радиотехники и криптографии, шифрования и дешифрования в Советском Союзе, и благодаря этому командование Красной армии расшифровывало все приказы гоминьдановского правительства, передававшиеся по радио войскам, и соответствующим образом учитывало складывающуюся обстановку».

ЗАПАХ ПОРОХА КАК СТИМУЛ

Как мы знаем, в середине 1930-х годов военный пожар возник и в Испании. То время нередко называют подлинным началом Второй мировой войны. В китайских и в испанских событиях было много иностранных участников, а значит и потенциальных источников важной информации. Военные события в Испании и на Дальнем Востоке стали хорошей проверкой и стимулом для развития советской криптографической службы.

На испанском направлении её деятельности тогда удалось оказать заметную практическую помощь респу-

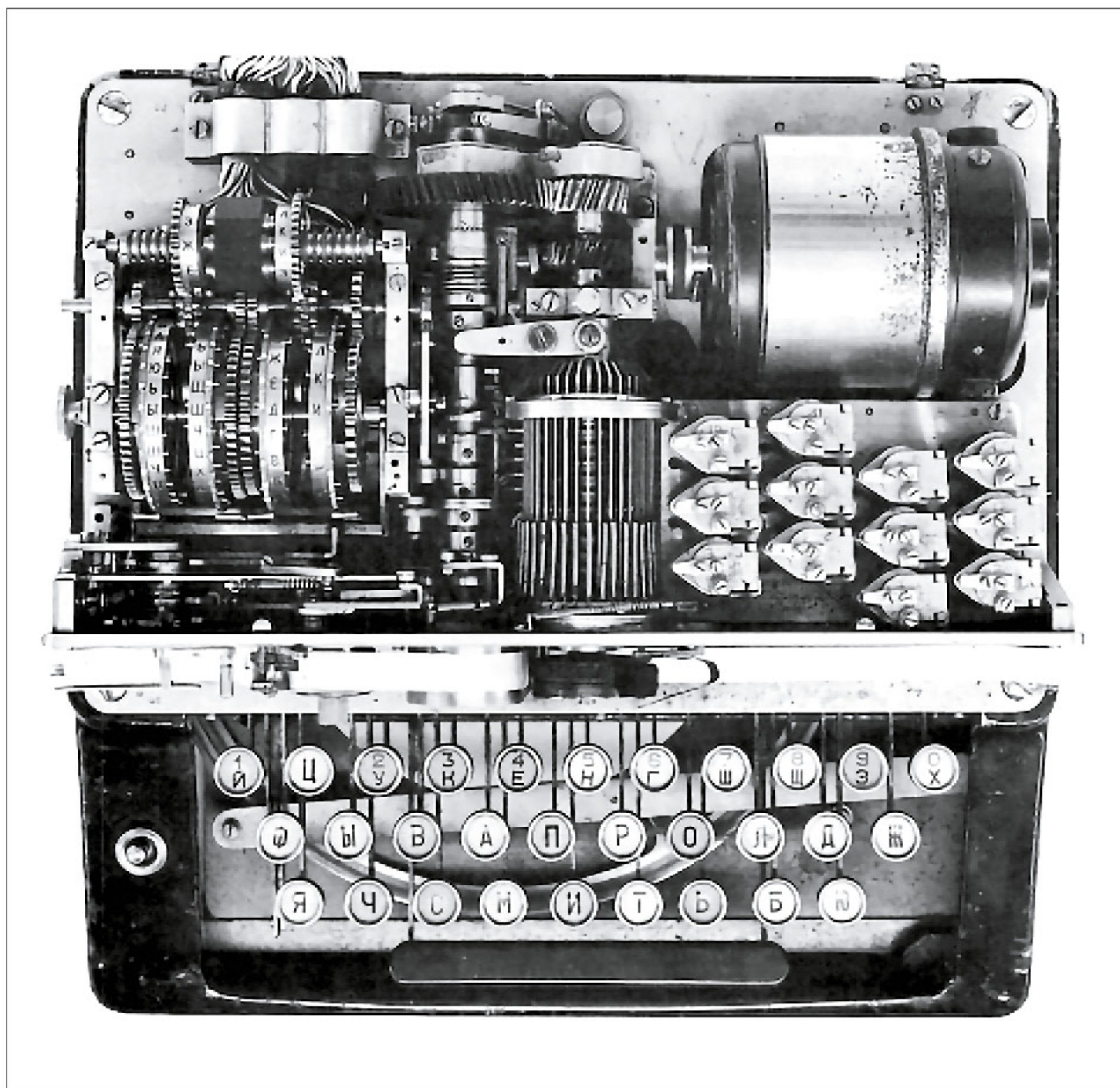


Конструктор И. П. Волосок

бликанским войскам, в Москве такую работу возглавлял Б. А. Аронский. На дальневосточном направлении дешифровальной работой в НКВД руководил С. С. Толстой. Перед ним и его соратниками встала трудная задача анализа шифров японских шифр-машин — оранжевой, красной и пурпурной. Особенно сложным оказался шифр пурпурной машины, закрывавший с 1939 г. важнейшую дипломатическую переписку Японии. Ныне известно, что усилия С. С. Толстого и его сотрудников привели к вскрытию шифров. Особенно ценно, что успех пришёл вовремя: чтение японских дипломатических шифртелеграмм позволило руководству СССР принять обоснованное решение о переброске войск с Дальнего Востока под Москву, что решило исход Московской битвы осенью-зимой 1941 г.

«ЗА СЧЁТ ПРЕЖДЕВРЕМЕННОГО ИЗНОСА УМСТВЕННЫХ И ФИЗИЧЕСКИХ СИЛ...»

Объём перехватываемых радиосообщений, нуждавшихся в дешифровании советскими специалистами, неизменно рос. Можно утверждать, что в предвоенные годы не было ни одного важного события в международной жизни, которое не нашло бы своего отражения в дешифрованной переписке. Такое добывание ценной информации достигалось напряжением всех



Шифровальная машина К-37

сил. Так, начальник разведывательного управления штаба РККА Я. К. Берзин писал: «Шифрдокументы поступают от 52 стран, однако разрабатываются совместно со Специальным отделом лишь только документы 22 стран... За 1933 г. при напряжённой работе подчас за счёт преждевременного износа умственных и физических сил работников разработано только 42 % имеющихся для разработки материалов».

А стойкость шифров ведущих государств стала заметно возрастать, их криптографические службы постепенно оснащались шифровальными машинами. Это потребовало создания новых методов дешифрования, отвечающих духу времени, именуемому «математизацией» криптографии.

Ещё с конца 1920-х годов в мире началось распространение роторных (дисковых) шифрмашин. В 1932 г. советские торговые представители в Швеции тоже купили два экземпляра шифрмашин В-211 конструкции Б. Хагелина. Но анализ работы машины и её копирование с модернизацией

в К-37 затянулись до конца 1930-х годов.

Собственные советские разработки шифровальной техники использовали принцип гаммирования, то есть наложения случайной последовательности из нулей и единиц (знаков гаммы) на представленный в двоичном виде (из нулей и единиц) открытый текст. Физическим внешним носителем знаков случайной гаммы служила перфолента. Такой выбор направления разработки вполне объясним, ведь использование гаммирования хорошо зарекомендовало себя в ручных шифрах. Первый образец шифрмашин конструкции И. П. Волоска (ШМВ-1) появился в 1932 г., но серийно подобные шифрмашин стали выпускать лишь в конце 1930-х.

С 1939 г. на каналах связи звена «округ — флот» стали появляться шифраторы В-4 и их модификация М-100, а в звене «армия — флотилия — корпус» началась эксплуатация шифровальной машины К-37. Их создание и внедрение стало результатом существенных



Г. И. Пондопуло

преобразований криптографической службы. Её организация и кадровый состав претерпели необходимые изменения, а главное был взят курс на её техническое оснащение, продиктованное утверждением новой эпохи в криптографии. В СССР были изысканы возможности для производства шифраторов собственной конструкции и улучшения криптографического обеспечения, прежде всего, вооружённых сил.

ВРЕМЯ АКТИВНОГО ВНЕДРЕНИЯ МАТЕМАТИЧЕСКИХ МЕТОДОВ

Вместе с тем создавались и новые возможности для таких преобразований. Ведь развивалась экономика государства, активно велась техническая реконструкция всего народного хозяйства и подготовка кадров. В 1930–1935 годах страна получила 435 тысяч инженерно-технических специалистов. В АН СССР было создано отделение технических наук, претерпела изменения организация образования, возродилась в новом виде система учёных степеней и званий. В 2005 г., в связи с 250-летием МГУ, стали известны интересные подробности из жизни университета в 1930-е годы. Так, в 1935 г. МГУ впервые организовал олимпиаду по математике для школьников, тогда в ней приняли участие около 300 учащихся. Олимпиада сразу стала ежегодной. В том же 1935 г. на обновлённом механико-математическом

факультете МГУ была образована кафедра теории вероятностей, её возглавил Андрей Николаевич Колмогоров (1903–1987), только что получивший без защиты диссертации степень доктора физ. — мат. наук. Это было время активного внедрения математических методов в производство. В Ленинграде в такой деятельности отличился Леонид Витальевич Канторович (1912–1986), также получивший степень доктора физ. — мат. наук в 1935 г. Заметим, что ему было тогда лишь 23 года, правда, он поступил в ЛГУ в 14 лет. Молодой, но уже авторитетный учёный занялся изучением организации производства фанеры по просьбе фабричных инженеров. При этом он обнаружил такие общие закономерности, которые не только помогли администрации фабрики повысить эффективность производства, но в дальнейшем привели его самого к созданию теории линейного программирования, отмеченной Нобелевской премией по экономике в 1975 г. «за вклад в теорию оптимального использования ресурсов». Слово программирование в этой теории надо понимать как планирование. Одним из первых применений новых методик стало их использование в организации перевозок военных грузов при подготовке победного наступления советских войск под Сталинградом в конце 1942 г. Канторович всегда подчёркивал, что является последователем Чебышёва в признании особой роли математики в



А. И. Копытцев

развитии науки, техники и производства. В подобных энтузиастах нуждалась и криптография.

ПРИЗЫВ МАТЕМАТИКОВ В КРИПТОГРАФИЮ

В 1938 г. появились математики и среди криптографов. Их количество заметно выросло в преддверии Великой Отечественной войны. Выпускник мехмата МГУ 1937 г. Г. И. Пондопуло (1910–1994), возглавлявший перед ВОВ партком НИИ механики МГУ и готовивший диссертацию, вспоминал спустя годы, как беседовал с направляемыми из МГУ на службу в НКВД и Генеральный штаб РККА кандидатами наук и как затем вскоре сам стал военным. Такой призыв оказался весьма полезным, хотя и запоздалым. Заметим, что спустя 10 лет судьба вновь связала Георгия Ивановича с МГУ. Когда в 1949 г. для подготовки специалистов по криптографии было организовано закрытое отделение мехмата МГУ, его возглавил именно Г. И. Пондопуло. Он стал также заместителем декана мехмата, хотя педагогической деятельностью Георгий Иванович занимался по совместительству без отрыва от службы.

Москвич, детдомовец Михаил Иванович Соколов (1914–1998) окончил мехмат МГУ с отличием в 1938 г. Перед самым началом ВОВ он успел завершить обучение в аспирантуре защитой диссертации и встал в строй криптографов ГШ РККА. Впереди была долгая

плодотворная работа, а затем и участие в обучении молодого пополнения специальной службы, и заслуженное уважение коллег.

ОТ МЛАДШЕГО ЛЕЙТЕНАНТА ДО ГЕНЕРАЛА... ЗА ШЕСТЬ ЛЕТ

Одним из первых математиков, пришедших в советскую криптографию, стал выпускник мехмата МГУ Алексей Иванович Копытцев (1912–1987), однокурсник М. И. Соколова. В первый год обучения в аспирантуре, в ноябре 1938, его призвали на службу в ГУГБ НКВД. Интересно проследить за его служебными назначениями. Сначала он упоминается в документах как оперуполномоченный 5 отдела ГУГБ (11.38–04.39) и младший лейтенант ГБ (с 12.38). Спустя полгода — уже начальник 7 отдела ГУГБ НКВД (04.39–02.41) и капитан ГБ (с 04.39), сразу из младших лейтенантов! Напомним, что именно 7 отдел ГУГБ НКВД стал наследником Спецотдела. Под руководством и при участии Копытцева в 1939 г. появился учебник «Криптография (шифрование и дешифрование)». Соавторами Алексея Ивановича стали Б. А. Аронский, С. С. Толстой и С. Г. Андреев. Вероятно, А. И. Копытцев успешно справлялся со своими весьма ответственными обязанностями, поскольку ещё через год он уже майор ГБ (с 03.40) и орденосец (орден «Знак Почёта» 26.04.40). А в начале 1943 г. А. И. Копытцев заслужил генеральское звание комиссара ГБ, как один из руководителей криптографической деятельности, в том числе всей дешифровальной работы в центре и на фронтах.

КАК ПРИШЁЛ В КРИПТОГРАФИЮ В. А. КОТЕЛЬНИКОВ

В конце 30-х годов началось плодотворное участие В. А. Котельникова в делах защиты информации. Как это случилось, можно представить себе по биографическим запискам Н. В. Котельниковой, дочери великого учёного. Ещё в 1935–1936 гг. правительство СССР утвердило стратегию создания магистралей ближней, средней и дальней радиосвязи. Во исполнение правительственных решений В. А. Котельникову и его сотрудникам



В. А. Котельников

из НИИС РККА удалось создать уникальную аппаратуру для таких линий. Правда, приборы пришлось делать самим, так как промышленность отказалась принять заказ на их изготовление. Новую аппаратуру установили на линии связи Москва-Хабаровск в 1939 г.

Это был выдающийся проект для своего времени. Но готовую и испытанную уникальную радиотелефонную линию к эксплуатации не приняли по веской причине — «слишком легко подслушать». Заметим, что никому из группы Котельникова криптографией до этого заниматься не приходилось, да и доступа к соответствующей литературе и специалистам не было. Пришлось начинать знакомство с криптографией «с нуля».

Здесь весьма кстати прилась статья Х. Дадли, опубликованная в октябре 1939 г. Прочитав её, Владимир Александрович сразу оценил потенциальные возможности описанного там вокодера (аппарата искусственной

речи) с точки зрения перспектив создания на его основе аппаратуры шифрования речи. И уже в начале 1941 г. в лаборатории заработал первый в СССР вокодер.

В условиях, когда «сроки поджимали», Котельников обдумывал ещё и проблемы надёжного шифрования. Свои соображения он изложил в отчете «Основные положения автоматической шифровки», представленном всего за три дня до начала войны, 19 июня 1941 г. Там впервые были «сформулированы четкие положения о том, каким требованиям должна удовлетворять математически недешифруемая система, и дано доказательство невозможности ее дешифрования». Ныне эта работа признаётся основополагающей в развитии отечественной криптографии.

Заметим, что К. Шеннон изложил свои, ныне известные подходы к построению стойких систем шифрования в секретном докладе, датированном 1 сентября 1945 г.

**Сергей ВИХОРЕВ**советник генерального директора
ООО «ИТ-Экспертиза»«Зри в корень!»
Козьма Прутков

СТАКАН НАПОЛОВИНУ ПОЛОН ИЛИ НАПОЛОВИНУ ПУСТ?

ЭССЕ ОБ ОПТИМИСТАХ, ПЕССИМИСТАХ, ДОВЕРИИ, «УДАЛЁНКЕ» И БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Конечно, в условиях пандемии мир меняется. И очень сильно изменились наши коммуникации и отношение к рабочему месту. Уютные домашние тапочки, мягкий диван, подмосковная дача вместо душного офиса — это уже норма. Хорошо! Но на реверсе этой благодушной картины вырисовывается большая головная

боль администратора информационной безопасности. Как в этих комфортных для пользователя условиях обеспечить безопасное и надёжное взаимодействие этого самого пользователя с информационной сетью организации? Вот и получается, новые производственные отношения возникли, а проблемы безопасности информации остались старые.

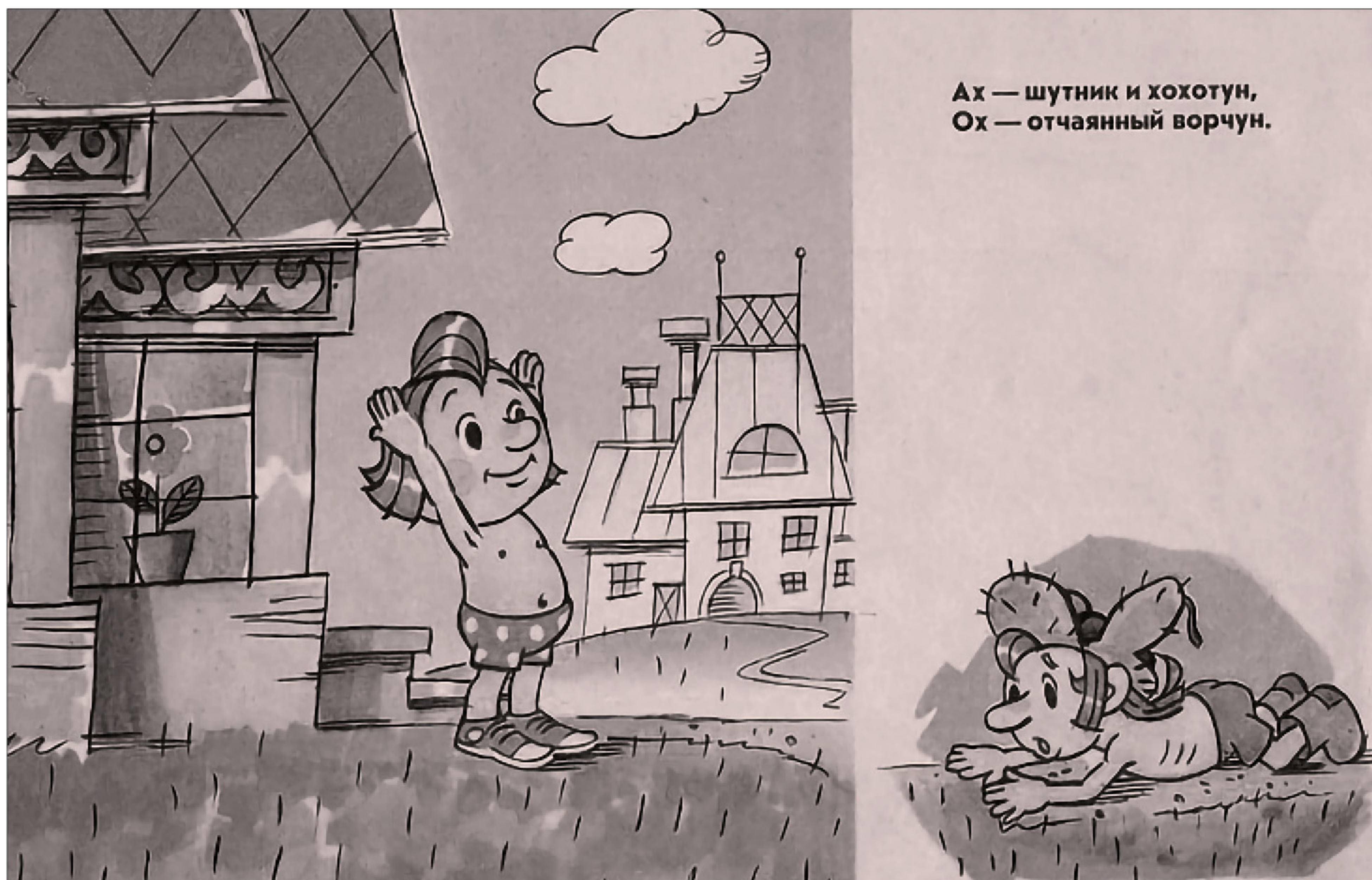
ОПТИМИСТЫ И ПЕССИМИСТЫ

В принципе, здесь нет ничего нового. Это модная в последнее время парадигма «нулевого доверия» — Zero Trust, идея, получившая второе дыхание во время пандемии. Считается, что она была придумана в 2010 году аналитиком Forrester, но на самом деле в России парадигма «доверенной среды» появилась лет на 20 раньше (как говорится, нет пророка в своём отечестве). Правда, есть и некоторые отличия.

Давайте всё-таки вспомним старый анекдот про полупустой (или полуполный?) стакан. Оптимист считает, что стакан наполовину полон, а пессимист — что наполовину пуст. В данном случае пессимистическая точка зрения присуща именно «нулевому доверию». Главный тезис: полное отсутствие доверия кому-либо — даже пользователям внутри периметра. Это значит, что каждый раз, когда пользователю надо достучаться до какого-нибудь ресурса в сети, он должен подтверждать свои полномочия. Идея проста и состоит из следующих основных компонент:

- ◆ недоверие к сети (весь трафик, независимо от местоположения, является вредоносным, пока не будет доказано, что он авторизован, проверен и защищён);

Зри в корень. Рисунок: [instagram.com/innubis](https://www.instagram.com/innubis)



Оптимисты и пессимисты. Из книги «Ох и Ах идут в поход» (автор Л. В. Зубкова)

- ◆ сегментация на уровне сети (минимум привилегий и строгий контроль доступа только к ресурсам, которые необходимы для выполнения работы пользователем);

- ◆ сетевой мониторинг и аналитика (постоянная проверка и регистрация всего трафика на предмет вредоносных действий);

- ◆ контроль пользователя (аутентификация пользователей и постоянный мониторинг и управление их доступом и привилегиями);

- ◆ контроль приложений (контроль всех приложений, особенно соединений между контейнерами или гипервизорами в облаке);

- ◆ контроль данных (защита и управление данными, шифрование данных как при хранении, так и при передаче).

Но здесь и кроется проблема. Реализовать полную модель «нулевого доверия» не так просто. Положим, удалённый пользователь прошёл все установленные процедуры идентификации — аутентификации — авторизации и у администратора безопасности

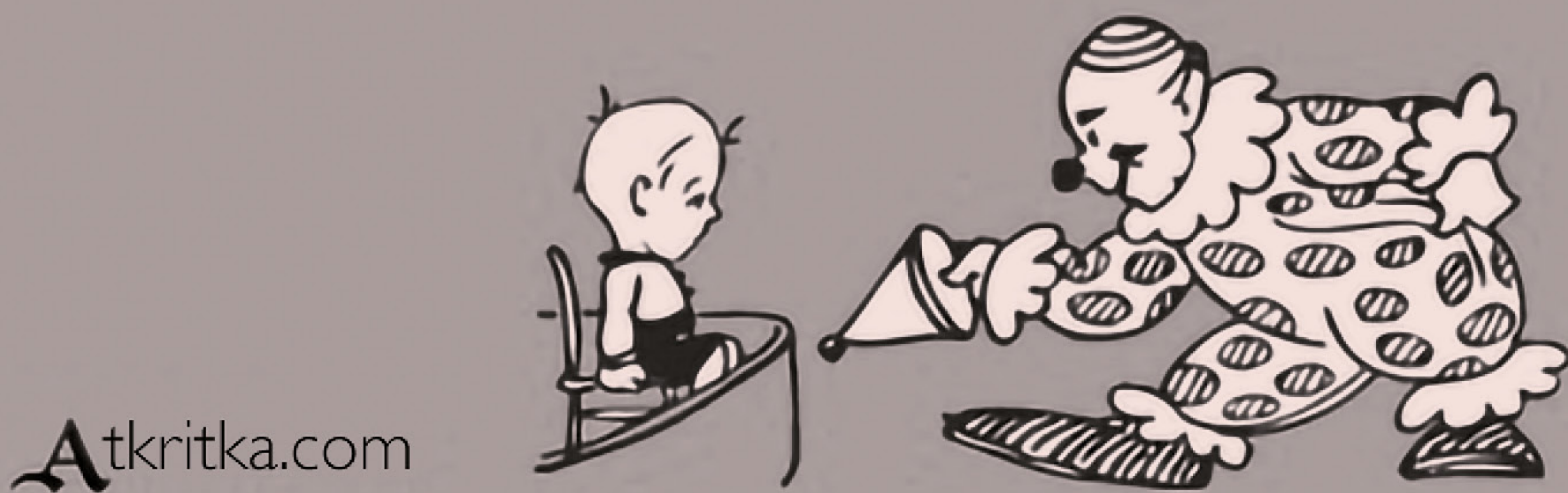
нет, кажется, оснований не допустить пользователя в закрытую сеть или к нужному ресурсу. А теперь ответьте на вопрос: по результатам успешного прохождения процедуры идентификации — аутентификации — авторизации удалённого пользователя администратор безопасности защищённой сети может быть уверен в безопасности сети? Ведь сама по себе процедура идентификации не ответит на, может быть, главный вопрос: а можно ли доверять тому компьютеру, с которого обращается пользователь? Ведь этот компьютер находится на чужой территории, неподконтрольной администратору безопасности. И в этой неоднозначной ситуации, когда исчезает само понятие «периметр», администратор безопасности сервера стоит перед выбором: либо довериться «голосу» как бы доверенного пользователя и разрешить непроверенному компьютеру доступ в защищённую сеть, либо не пускать пользователя в закрытую сеть и нарушить все бизнес-процессы. А компьютер

пользователя может быть заражён каким-нибудь вредоносом, или на нём установлен ботнет или TeamViewer, обеспечивающий обмен файлами между управляющей и управляемой машинами. Получается, что администратор безопасности, который должен стоять на страже своей сети, своими руками сделал «дыру» в сети и пустил козла в огород. Я уже как-то писал об этой проблеме¹.

А теперь оптимистическая точка зрения. Главный тезис концепции «доверенной среды»: если мы сможем быть уверенными в надёжности (лояльности, доверенности) каждого элемента, нам не обязательно изолировать их в замкнутой среде. В силу принципа декомпозиции каждый элемент защищаемой информационной системы сам по себе может быть защищён, и в этом случае соединение их в единую информационную систему с помощью защищённых каналов позволит создать вокруг информации

¹ <https://ib-bank.ru/bisjournal/post/852>

Доверие — как нервные клетки: практически не восстанавливается.



Atkritka.com

Корень доверия. Иллюстрация: atkritka.com

надёжную оболочку. «Доверенная среда» предполагает, что должно быть доверие:

- ♦ к окружению системы (доверенная территория, жизнеобеспечение);
- ♦ к субъектам отношений (счётность субъектов и объектов);
- ♦ к правилам и процедурам (доверенность конфигураций и настроек);
- ♦ к аппаратной и программной платформе (целостность всех элементов);
- ♦ к выполняемым операциям (подконтрольность и документированность);
- ♦ к каналам передачи информации (доверенность каналов).

Обе точки зрения, в принципе, говорят о похожих сущностях. Но дьявол кроется в нюансах. С точки зрения «нулевого доверия» прежде всего требуется постоянный мониторинг и управление доступом и привилегиями пользователей, а также мониторинг всего трафика на предмет вредоносных действий. И здесь остаётся открытым вопрос доверия к конечному оборудованию пользователя. С точки зрения «доверенной среды» — постоянный

мониторинг конфигураций и настроек и целостности рабочих мест, то есть прежде всего формирования доверия к компьютеру конкретного пользователя. Ну а процедура идентификации — аутентификации — авторизации в обоих случаях является обязательной. Вот и получается, что без разницы, стакан наполовину полон или наполовину пуст, главное, что в нём есть то, что можно пить.

КОРЕНЬ ДОВЕРИЯ

А теперь ответьте, что проще: постоянно контролировать права доступа или конфигурации и настройки компьютера? Например, использование Active Directory для аутентификации и контроля полномочий пользователя — распространённое явление. Система известная, и поэтому в Интернете описывается множество атак на неё.

Простейшее. Слабые или украденные учётные записи являются мощным оружием хакеров, используемым в 95 % всех атак. На каждом компьютере в сети должна быть встроенная учётная запись администратора, защищённая

паролем, который должен регулярно меняться. Но частенько, особенно когда много «удалёнщиков», к которым не всегда доберёшься, системные администраторы используют возможности самого Active Directory (групповые политики) для быстрой замены такого пароля. Одна незадача: на всех компьютерах пароль локального админа будет одинаковый. Из этого следует, что получение учётных данных администратора на одной из машин сделает злоумышленника админом сразу на всех. Особенно это актуально для удалённого компьютера, когда злоумышленник во благо времени имеет возможность использовать любые инструменты. Вот и получается: то, что хорошо работает в замкнутой среде, может не сработать в среде «без периметра». Очень важно не только контролировать полномочия пользователей, но и следить, чтобы на удалённом компьютере не было чего-нибудь лишнего.

Решение, кажется, на поверхности. Надо провести инвентаризацию удалённого компьютера, создать некий его профиль и в дальнейшем с

периодичностью отслеживать его состояние, настройки, конфигурацию, целостность. Проще говоря, надо в режиме реального времени проводить мониторинг:

- ◆ ГДЕ находится компьютер;
 - ◆ КАК подключается компьютер;
 - ◆ ЧТО установлено на компьютере;
 - ◆ ЧТО запущено на компьютере;
 - ◆ ЧТО делает сотрудник/фрилансер.
- При этом средство мониторинга должно как минимум уметь контролировать:
- ◆ геолокацию компьютера и структуру информационной сети;
 - ◆ состав программного и аппаратного обеспечения;
 - ◆ параметры настройки операционной системы, версию, обновления;
 - ◆ установку, настройку, актуальность программного обеспечения;
 - ◆ наличие, актуальность и настройки средств защиты информации;
 - ◆ тип и состав подключённых USB-устройств;
 - ◆ запущенные в операционной системе процессы;
 - ◆ Logon/logoff пользователей.

Сведения обо всех этих параметрах как раз и будут составлять профиль рабочего места. Но пассивное наблюдение вряд ли даст положительный эффект. Необходимо не только контролировать, но и иметь возможность управлять рабочим местом: уведомлять администратора безопасности об отклонениях, блокировать доступ в критических ситуациях или переводить компьютер в карантин.

Однако и этого мало. Нужно правильно построить хранилище, в котором, собственно говоря, и должен храниться тот самый профиль рабочего места, с которым будет проводиться сравнение. Это и будет корень доверия. Естественно, что такое хранилище должно быть надёжно защищено и исключать всякую возможность изменения профилей. Можно поступить по-разному: можно поместить такое хранилище непосредственно на проверяемом компьютере — это упростит процедуру контроля и сократит трафик обмена результатами, но тогда встанет проблема его защиты. Скорее всего, это можно реализовать

криптографическими методами, а это, в свою очередь, обозначит проблему доставки криптоключей и их стойкости и ещё ряд проблем, связанных с возможностью взлома такого хранилища (не будем забывать, что удалённый компьютер, размещённый на «чужой» территории, позволяет злоумышленнику спокойно во благо времени изучить все уязвимости хранилища и при необходимости выработать специальные методы воздействия). А можно поступить и по-другому. Самое надёжное место для такого хранилища — закрытый сегмент информационной сети, расположенный на строго охраняемой территории. И при этом доступ к нему должен быть ограничен, он не должен быть напрямую связан с самой информационной сетью, что исключит возможность случайного (преднамеренного?) доступа к такому хранилищу. По всей видимости, это должен быть отдельный сервер.

ЛАЗЕРМАН ПРОТИВ ЗОЛИНГЕН

Средства защиты постоянно совершенствуются. Это прогресс, и от него никуда не денешься. И прогресс этот идёт в том числе по пути универсализации этих средств. И если раньше мы с лёгкостью могли идентифицировать то или иное средство защиты используя, например, классификацию Гартнера, то сейчас это не всегда возможно. Наверное, уже можно говорить не об отдельном средстве защиты, а комплексе, который реализует функции нескольких классов средств защиты. Например, межсетевые экраны новой генерации (NGFW — Next Generation Firewall — в классификации Гартнера) не только объединяют в себе возможности традиционных межсетевых экранов, но и добавляют к этой функциональности ещё десяток новых функций, в том числе систем предотвращения вторжений IDS/IPS, управление приложениями, антивирусную защиту и прочее. Хорошо ли это? Смотря с какой точки зрения. С точки зрения ИТ-специалиста это очень хорошо: нет «зоопарка» средств, проще администрировать, поставил одно средство и решил половину проблем.

А с точки зрения ИБ-специалиста — наоборот. Давайте вспомним классику построения систем обеспечения безопасности информации в части антивирусной защиты. Основной постулат в этой части — создать трёхуровневый эшелон защиты (пограничное устройство — сервер — рабочая станция), и при этом на каждом уровне надо применять антивирусные средства разных производителей. Это нужно для того, чтобы злоумышленник, преодолев один рубеж, поняв логику и алгоритм защиты, не смог бы применить свои познания для преодоления второго и третьего рубежа. Да, антивирусы разных производителей, построенные по разным принципам и архитектурам, использующие разные алгоритмы и логику работы, создадут трудности для злоумышленника, поэтому этот тезис не такой уж и абсурдный, хотя и создаёт проблемы в обслуживании. А универсальные, многофункциональные средства защиты как-то не вписываются в такую концепцию: при нарушении одной функции автоматически создаётся угроза для всех остальных защитных функций.

И ещё, с точки зрения экономики. А все ли заявленные в универсальном средстве функции нужны в конкретной информационной системе? Не факт! Положим, хозяйка собирается на ужин подать жареное филе трески. Предложите ей для готовки на выбор два инструмента: универсальный мультитул «Лазерман» и специальный филейный нож от Золинген. Что она выберет? Конечно Золинген! И удобнее, и лучше. Часто лучше воспользоваться специализированным инструментом, чем использовать универсальный. Так и в нашем случае, учитывая особые требования к автономизации системы мониторинга рабочих мест, целесообразнее использовать специализированное средство, заточенное под такие задачи и позволяющее локализовать себя от остальных средств. При этом локализация не значит отсутствие взаимодействия. Взаимодействие важно и нужно.



Александр БОДРИК
управляющий директор
Cyberlands.io API Penetration
Testing Company, CISA

«СПАСАТИ РЯДОВОГО САНКЦИЯМИ!»

ЗАМЕТКИ БЕЗОПАСНИКА

Три-четыре года назад автор предупреждал, что возможна массовая утечка кадров за рубеж. Массовой утечки не случилось, за что в первую очередь стоит сказать спасибо санкциям и «рашн хакерс».

ПРО САНКЦИИ

Начнём с истории. В начале 2017 года было объявлено о вмешательстве России в процесс выборов президента США. Не будем углубляться в политику, но честно признаюсь: именно в это время мои переговоры об открытии в Москве крупного британского деливери-центра по ИБ прекратились со ссылкой на санкции.

Дальше — больше. Под «киберсанкции» попали диджиталы, а недавно и позитивы, и любой американский реселлер (50% мирового рынка корпоративных ИТ) стал бояться русских как огня. Проблемой стало всё — русские юридические лица, лицензии ФСБ, длительная работа в России...

Некоторые вендоры подальше от греха прекратили продажи в РФ (Splunk, Zoom). Некоторые отказались генерить совместные предприятия в РФ для трансфера технологий (хотя аналогичные, с Францией, по морской военной технике вполне существуют). Это всё результирует в ослабление глобальной конкурентоспособности нашей отрасли кибербезопасности, которой всё сложнее получить для изучения образцы

кибероружия (например, Cobalt Strike) или хотя бы банально купить платный фид правил на Snort.

Впрочем, есть лайфхаки. Во-первых, большинство нужного софта (как Zoom) можно купить карточкой. Во-вторых, покупаем на белорусские и казахские дочки (по Казахстану вообще нет никаких санкций). В-третьих, компании с русскими акционерами чуть ли не оккупировали бизнес-центры в Чехии, Эстонии и Голландии — варианты на любой вкус. Себестоимость создания и поддержания компании в Голландии — примерно 2 тыс. евро в год. Это вполне по силам любой организации. В-четвёртых, многие зарубежные компании по-прежнему работают с Россией. Это стартапы, компании поменьше, а также компании без большого доступа к западным рынкам.

ПРО КАДРЫ

Так почему спасти рядового? Ведь санкции фактически отсекали ряд мощных кадровых пылесосов от хантинга из России. Не тут-то было. Например, в одном из трёх глобальных опорных SOC IBM (в Польше) не обязательно пользоваться устным английским, будет достаточно знания русского или украинского. От чего киевские компании (те, что помощнее) не в восторге и приступили к активному хантингу DevSecOps из Москвы.

DevSecOps стал новой отдельной веткой ИБ, которая пока маленькая, но

уже по своей натуре удалённая. Как будет комплектовать соответствующие подразделения средняя российская корпорация, что по опросам в группе CyberJobsRussia хочет вернуть всех он-сайт, — непонятно. Платить она будет столько же, сколько стартапы, — 250–350к, процессы длинные и непонятные, смузи не наливают, встречи один на один в службах ИБ проводят на порядок реже, чем в стартапах, а значит, люди без понятия, как их работу оценивают и какие у них перспективы.

И напоследок: туда, куда не приходят США, приходит Китай. Зарплаты по 10–15–20к долларов в месяц из московского Huawei захантят практически любого безопасника с нерешённым жилищным вопросом. При этом старшие товарищи не объясняют младшим, что такое работать в китайской компании и сколько денег потом может потребоваться на лечение нервов.

* * *

Однако будем оптимистичны — количество отделов ИБ и ИБ-компаний в России растёт, отрасль растёт, если не хватает своих кадров, можно хантить белорусов, где на широкой груди ЕРАМ (и его американских проектах) растут компетенции по безопасности актуальных современных технологий. Впрочем, дёшево это не будет — эра дешёвой рабочей силы закончилась.

Программный комплекс «КриптоПро Архив» предназначен для подготовки и поддержания в актуальном состоянии электронных подписей (ЭП) документов для архивного хранения.

«КриптоПро Архив» не заменяет системы электронного документооборота (СЭД), а гармонично дополняет их. Это позволяет организовать полностью автоматизированный процесс подготовки подписанных ЭП документов к архивному хранению.

Основным способом обмена данными между «КриптоПро Архив» и подключаемыми СЭД, служит механизм REST-сервисов с использованием протокола JSON-RPC.



РЕШАЕМЫЕ ЗАДАЧИ

- Подготовка ЭП документов, к временному (до 10 лет), долговременному (свыше 10 лет) и постоянному централизованному хранению
- Усовершенствование ЭП документов форматов CAdES-BES, CAdES-T, CAdES-C, CAdES-XLT1 до формата CAdES-E-A, для обеспечения юридической значимости документов при их длительном хранении за счет использования хранящихся в подписи доказательств подлинности и заверяющих их архивных штампов времени
- Контроль сроков действия доказательств юридической значимости документов при их длительном хранении и при необходимости их автоматическое обновление
- Прием и передача информации о контейнерах электронных документов (контейнер содержит ЭП, хэш документа и его метаданные) временного, долговременного и постоянного хранения между «КриптоПро Архив» и СЭД
- Хранение в «КриптоПро Архив» контейнеров документов временного, долговременного и постоянного хранения и статуса проверки электронных подписей, которыми они подписаны

КриптоПро Архив

@ info@cryptopro.ru

+7 (495) 995-48-20

@CryptoProInfoBot

https://cryptopro.ru

АРХИТЕКТУРА

Модуль обработки ЭП документов

обеспечивает прием, передачу, хранение контейнеров документов и управления ими.

Модуль обеспечения доказательством подлинности

обеспечивает сбор доказательств подлинности и юридической значимости документов, подписанных квалифицированной ЭП

АРМ администратора

обеспечивает управление правами доступа пользователей и администрирование модулей.

КРОССПЛАТФОРМЕННОСТЬ

Linux:

Astra Linux, Debian, Fedora, openSUSE, Red Hat Enterprise Linux, Ubuntu

Microsoft Windows Server:

начиная с версии 2012 R2

В качестве СУБД могут использоваться PostgreSQL, Microsoft SQL Server, MySQL, Oracle.

ОТКАЗОУСТОЙЧИВОСТЬ И ДОСТУПНОСТЬ

Высокая отказоустойчивость и доступность решения обеспечивается горячим резервированием и кластеризацией всех его компонент средствами специализированных балансировщиков нагрузки и программного брокера сообщений на основе стандарта AMQP.

В случае нарушения функционирования любого из зарезервированных компонентов переключение на резервные, в том числе размещенные на территориально-удаленных технологических площадках, осуществляется автоматически без участия обслуживающего персонала и без потери данных.

Проекты Медиа Группы «Авангард»

Онлайн и офлайн-мероприятия

Отраслевой журнал BIS Journal

Интернет-телекомпания BIS TV

Энциклопедия безопасника

ib-bank.ru



**Окунись в мир
информационной
безопасности!**



АВАНГАРД