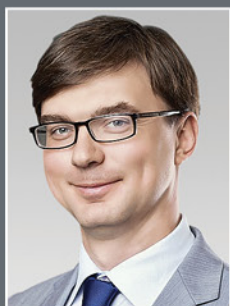




20 Владимир ЕЛИСЕЕВ
ИнфоТекС
Доверие по всей стране. Как?

28 Василий ПИСКАРЕВ
Государственная Дума РФ
У хакеров будут изымать деньги



34 Александр БАБКИН
Газпромбанк
Интеграция на сверхскорости

63 Ольга СКОРОБОГОВА
Банк России
Технологии: что в фокусе внимания ЦБ?

94 Амина ЗАМУЛИНА
Сбербанк
Защита ПДн: индийский опыт

КВАНТ. ПОБЕДИТЕЛЬ ПОЛУЧИТ ВСЁ



МОСКВА_КЛАСТЕР «ЛОМОНОСОВ»

25 МАЯ 2023



ФОРУМ

ЦИФРОВАЯ ЭКОНОМИКА

технологии доверенного
искусственного интеллекта

**Главная тема текущего десятилетия —
ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ**

Основные темы форума:

- Вопросы создания систем доверенного ИИ
- Безопасность данных и ИИ
- Атаки на системы ИИ и методы защиты
- Применение технологий искусственного интеллекта в обеспечении ИБ
- Особенности использования открытого ПО в искусственных интеллектуальных системах
- Подготовка квалифицированных кадров в области ИИ и машинного обучения



ib-bank.ru/trust-ai/

Организаторы



ИСП РАН

При поддержке



Минцифры
России

Оператор

АВАНГАРД



Елена ПОКАТАЕВА
обозреватель BIS Journal

Тема этого номера звучит как «Квантовая криптография на практике», но рабочий вариант названия немного другой: «Квантовое шифрование: битва алгоритмов или Победитель получит всё». Эти слова четко обозначают специфику момента. В нем — три составляющих:

1. Все ждут прихода Страшного Квантового Компьютера на несколько тысяч кубит. Как только он появится в виде коммерческого продукта, а ближе всего к этому США, его первым делом возьмут на вооружение силовые структуры и разведки этой страны и будут использовать для взлома важной информации в корпоративных и государственных сетях российских организаций.

2. Современное шифрование — это хитроумные алгоритмы. Квантовый компьютер будет ломать зашифрованную передачу данных тоже с помощью алгоритмов. На рынке есть целое направление — ПО постквантового шифрования, с которым не сразу справится даже Страшный Квантовый Компьютер. Но на стороне взломщиков через некоторое время придумают новый алгоритм, который сможет взломать и это постквантовое шифрование. И так далее.

3. Победитель получает всё, ведь на каждом очередном витке постквантового шифрования тот алгоритм, от которого еще не придумали защиту, будет способен ломать любую криптографическую защиту текущего уровня. А тот алгоритм, который обеспечит защиту от всех квантовых взломов с помощью квантового компьютера, включая самый-самый новый и продвинутый, тоже «получит всё», потому что у него какое-то время не будет конкурентов.

На практическом уровне речь идет о том, что за те годы, которые остались до появления коммерческого Страшного Квантового Компьютера, нацеленного на взлом защищенных российских сетей (это считанные несколько лет), нужно обеспечить постквантовую защиту всей страны, как минимум, критической инфраструктуры. Это большая задача. Компания «ИнфоТекС» в своем комментарии рассказывает о практическом подходе — создании федеральной сети центров квантового шифрования, которыми все организации смогут пользоваться как сервисом. Это еще один аспект тезиса «победитель получит всё» — та страна, которая сможет быстро и эффективно модернизировать криптозащиту своих предприятий на постквантовом уровне, будет полностью защищена от квантового взлома со стороны других стран.

Пора становиться победителем!

ОБЩЕСТВЕННЫЙ РЕДАКЦИОННЫЙ СОВЕТ

Войлуков А.А. — вице-президент Ассоциации банков России
Сычев А.М. — доцент МГТУ им. Баумана, доктор технических наук
Шипилов В.В. — исполнительный директор Ассоциации российских банков, кандидат технических наук

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Былевский П.Г. — шеф-редактор, доцент департамента ИБ Финансового университета при Правительстве РФ, доцент кафедры международной ИБ МГЛУ, кандидат философских наук
Велигура А.Н. — председатель комитета по банковской безопасности Ассоциации российских банков, руководитель комитета по безопасности НП «НПС», CISA, кандидат физико-математических наук
Виноградов А.Ю. — старший научный сотрудник ФГУП «ЦНИИХМ»
Вихорев С.В. — советник генерального директора по информационной безопасности IT Expertise
Держинский Ф.Я. — независимый эксперт
Зубков А.Н. — генеральный директор ООО «Медиа Группы „Авангард“», директор Фонда содействия развитию безопасных информационных технологий (ФСРБИТ)
Калашников А.И. — директор проекта, Газпромбанк (АО)
Курило А.П. — советник по вопросам ИБ ФБК и FBK CyberSecurity, 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», доктор 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. — управляющий директор Управления по обеспечению ИБ Банка ВТБ (ПАО)
Филипчук А.А. — технический директор ГК ЦРТ
Шумский Л.С. — руководитель службы информационной безопасности Яндекс Банка
Янсон И.А. — бизнес-партнер по информационной безопасности, Департамент безопасности ПАО «Сбербанк России», кандидат физико-математических наук

ЭКСПЕРТНАЯ ГРУППА

Баранов А.П. — доктор физико-математических наук, академик Академии криптографии РФ
Батранков Д.В. — руководитель направления сетевой безопасности Positive Technologies
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 Positive Technologies
Сабанов А.Г. — заместитель генерального директора АО «Аладдин Р.Д.»
Сумманен К.Т. — директор по управлению проектами — вице-президент, Банк ВТБ (ПАО), кандидат физико-математических наук
Хайретдинов Р.Н. — заместитель генерального директора компании «Гарда Технологии»

РЕДАКЦИЯ ЖУРНАЛА

Главный редактор: **Некрасов И.В.**
Директор по развитию: **Минаков А.В.**
Арт-директор: **Мельников Н.С.**
Руководитель интернет-проектов: **Воробьева А.А.**
Ответственный редактор: **Седов О.В.**
Обозреватели: **Куликов В.А., Бродская М.А., Покатаева Е.Н.**
Иллюстрация на 1-й обложке: **Midjourney**
Фото в номере: **Envato.com, Depositphotos**
Цветокорректор: **Науменко М.Б.**

УЧРЕДИТЕЛЬ-ИЗДАТЕЛЬ

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

Зарегистрирован 13 августа 2010 года Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). 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 14.04.2023. Тираж 5000 экз. Заказ № 1092023. Цена договорная. Отпечатан в типографии «Московский Печатный Двор», 123298, г. Москва, 3-я Хорошевская 16, корп. 1, офис 201А

© BIS Journal, 2023



НОВОСТИ

5 В России, криминал, технологии

ТЕМА НОМЕРА — КВАНТОВАЯ КРИПТОГРАФИЯ НА ПРАКТИКЕ

- 8 Елена Покатаева (BIS Journal)
Квантовый переход финтеха
- 20 Владимир Елисеев (ИнфоТеКС)
«Как покрыть всю страну сетью равного уровня доверия?»
- 23 Сергей Петренко (Академия АйТи)
«К концу 2023 г. исследовательские проекты в области квантовой защиты информации могут перейти в более зрелую фазу коммерческих прототипов»
- 27 Дмитрий Плохов (QSpace Technologies)
«Технология квантового шифрования находится в самой начальной стадии своего развития»



РЕГУЛЯТОРЫ

- 28 **Государственная Дума РФ**
Василий Пискарев (Государственная Дума РФ)
«У хакеров, причинивших ущерб гражданам и банкам, необходимо изымать деньги и ценности, полученные преступным путём»
- 31 **Банк России**
Оксана Дяченко (BIS Journal)
Подробнее, пожалуйста!



БАНКИ

- 34 **Текущая ситуация**
Александр Бабкин (Газпромбанк)
«Интеграцию новых решений в ИБ можно сравнить с ремонтом автомобиля на скорости 150 км/ч»
- 36 **Проверка ЦБ**
Александр Виноградов (ФГУП «ЦНИИХМ»),
Вадим Андреев (КБ «АРЕСБАНК»),
Анастасия Николаева (BIS Journal)
Готовься, товарищ!
- 40 **Ассоциация ФинТех**
Александр Товстолип (Ассоциация ФинТех)
Открытый код в финсекторе
- 43 **Продолжаем разговор**
Рустам Гусейнов (кооператив «Рад Коп»)
Опасности директивной централизации

УГРОЗЫ И РЕШЕНИЯ

- 46** **Импортозамещение**
Павел Луцик (КриптоПро)
Полноценная замена
- 48** **DLP-системы**
Алексей Парфентьев (СёрчИнформ)
«Заглянуть под каждый камень»
- 50** **Сетевые экраны**
Иван Чернов (UserGate),
Артём Туренок (ДиалогНаука)
Конкурент зарубежным аналогам
- 53** **Социальная инженерия**
Лев Якубович (ГК «ЦИБИТ»)
Осторожно, мошенники!



34



59



55

ИНФРАСТРУКТУРА

- 55** **Деловые мероприятия**
Марина Бродская (BIS Journal)
«Магнитка» — 2023
- 59** **Деловые мероприятия**
Оксана Дяченко (BIS Journal)
«Кибербезопасность в финансах» — 2023
- 63** **Деловые мероприятия**
Ольга Скоробогатова (Банк России)
Технологии: что в фокусе внимания ЦБ?
- 65** **Опыт Дзен**
Дмитрий Куколев (Дзен)
Автоматизация AppSec
- 68** **Типология атак**
Данила Чежин (Servicepipe)
Защищая пользователей, защищайтесь сами
- 70** **DevSecOps**
Рами Мулейс, Дмитрий Кудинов (Yandex Cloud)
Что такое DevSecOps

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

- 74 Другая сторона**
Андрей Жаркевич (Антифишинг)
Зачем мошенники мучат кота Шрёдингера?



74

ОБРАЗОВАНИЕ И КАРЬЕРА

- 78 Обзор**
Ксения Трохимец (hh.ru)
На одну вакансию два резюме
- 79 Обзор**
Марина Бродская (BIS Journal)
«Требуется сисадмин со знанием ИБ»
- 82 Обзор ИноСМИ**
Анна Катанкина (BIS Journal)
С учётом национальных особенностей



94

ПРОГНОЗЫ

- 98 Опыт Сбера**
Михаил Анистратенко, Илья Болотов,
Дмитрий Кудияров, Александр Кузьмин
(ПАО СберБанк)
Горизонт — 0–10+ лет



108

ЗА РУБЕЖОМ

- 83 Обзор ИноСМИ**
Марина Бродская (BIS Journal)
Глобализация кибербезопасности
- 88 США**
Пять столпов одной безопасности
- 94 Индия**
Амина Замулина (Сбербанк)
Опыт Страны цветущего лотоса

СУБЪЕКТЫ

- 104 История**
Борис Столпаков (историк криптографии)
Первые громкие публикации по криптографии
- 108 История**
Борис Столпаков (историк криптографии)
«Свет мой, братец Васенка...»
- 112 Заметки безопасника**
Александр Игонин (BIS Journal)
«Есть в графском парке чёрный пруд...»

18 МЛН РУБ. НА ИНЦИДЕНТ

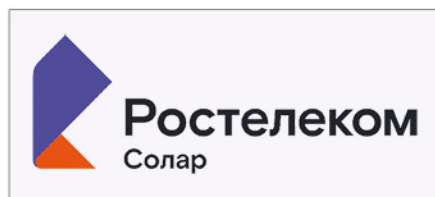
Компания «РТК-Солар» представила результаты исследования сетевых угроз российским компаниям, проведенное в марте 2023 года.

Самым дорогостоящим инцидентом в этом году стал перехват внешним злоумышленником контроля над сетевым оборудованием компании — потери составили 10,7 млн руб., а затраты на восстановление — 7,9 млн руб.

Выяснилось, что целевые атаки — наиболее распространенный тип угроз в сфере сетевой безопасности (35%). Особенно актуальными эти атаки являются для средних (48%) и крупных компаний (36%), а также госорганизаций (33%). 36% крупных компаний столкнулись с атаками

на управляющие протоколы систем. В остальных сегментах этот тип угрозы встречался гораздо реже. Для госорганизаций самой актуальной угрозой стала кража персональных данных — ее назвали 47% респондентов из госсектора. Кроме того, российские организации наиболее часто сталкиваются с фишингом, компрометацией корпоративной почты, потерей данных, атаками на веб-приложения и др.

На просьбу оценить опасность инцидентов и финансовые потери, 70% опрошенных отметили опасность заражения сети и сегментов инфраструктуры вредоносным ПО. При таком инциденте организация теряет в среднем 11,5 млн руб. (6,7 млн руб. ущерб от инцидента и 4,4 млн руб. затраты на восстановление). Для крупных компаний эти цифры еще выше: 77% отметили опасность заражения сети, а потери и затраты на восстановление в этом сегменте оценили в 17,1 млн рублей (9,4 млн и 7,7 млн руб. соответственно).

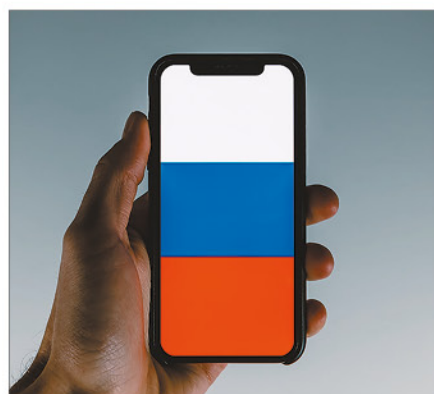


РЫНОК КРИТИКУЕТ ПРЕДЛОЖЕНИЕ МИНЦИФРЫ

Ассоциация торговых компаний и товаропроизводителей электробытовой и компьютерной техники, в которую входят, например, Samsung, Huawei и «М.Видео-Эльдорадо», подготовила критический отзыв на проект постановления Минцифры, описывающий новые правила предустановки магазина ПО Rustore.

В РАТЭК уверены: требования по интеграции Rustore с ОС продаваемой в России электроники «в большинстве случаев технически невыполнимы». Так, Google запрещает использовать сторонние магазины на лицензируемой компанией версии Android, а попытка обойти это условие в России может спровоцировать «отзыв лицензии на модель по всему миру». В Минцифры же отметили, что на устройствах Samsung и Xiaomi и так установлены альтернативные магазины приложений — Galaxy Store и GetApps.

Согласно новым требованиям, производитель должен обеспечить интеграцию Rustore с ОС: не только предустановить на устройство, но и предоставить ему те же системные разрешения, что и другим магазинам. Участники рынка считают, что из-за этого компании, продолжающие официально работать на российском рынке, могут задуматься об уходе из страны.



ГОСУСЛУГИ И НАЛОГОВАЯ ТАЙНА

Госдума в окончательном чтении приняла законопроект, согласно которому граждане смогут получать уведомления об уплате налогов через Госуслуги. Норма вступит в силу с июля.

Сейчас налоговые уведомления рассылаются либо в бумажной форме заказным письмом, либо в электронном формате через личный кабинет налогоплательщика. Чтобы начать получать налоговые уведомления через сайт госуслуг, россиянину нужно иметь подтвержденную учетную запись в ЕСИА. От сообщений можно позже отказаться, — направив уведомление в налоговый орган. Сведения, составляющие налоговую тайну, будут передаваться через портал только с согласия пользователя.

КАРТА ДЛЯ БАНКОВ

В Москве прошел Съезд Ассоциации российских банков (АРБ). Делегаты подвели итоги 2022 года, обозначили злободневные вопросы и определили планы на ближайшую перспективу.

По поводу импортозамещения интересно выступил Ренат Лашин, исполнительный директор АРПП «Отечественный софт». Совместными усилиями АРБ, АРПП и др. структуры создали Каталог отечественного взаимозаменяемого ПО для финансового рынка, который включает 528 решений от 240 разработчиков ПО; по формату Банка России подготовлена сводная Функционально-технологическая карта, которая включает более 620 приложений для решения бизнес-задач от 130 компаний разработчиков. В 2023 г. планируется оценка безопасности использования ПО с открытым кодом, создание национального репозитория типового ПО, формирование нормативной базы для публикации ПО с открытым кодом.

СТРЕЛЬБА ИЗ-ЗА УТЕЧКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Клиент «Сбера» открыл стрельбу из пневматического пистолета в офисе банка в Неманском проезде на северо-западе Москвы. Повод — утечка персональных данных, якобы допущенная сотрудником финучреждения.

В пресс-службе ГУ МВД России по г. Москве сообщили: «Житель района Строгино, 1951 года рождения, в ходе телефонного разговора с мошенниками получил информацию о том, что его персональные данные стали открытыми по вине сотрудников одного из отделений банка, куда мужчина и направился с целью выяснения обстоятельств, взяв с собой пневматический пистолет».

В ходе конфликта мужчина произвел несколько выстрелов вверх, после чего был задержан, добавили силовики.

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ: ЗАФИКСИ- РОВАН РЕКОРД 2022 ГОДА

Самой крупной суммой, похищенной у россиянина кибермошенниками в прошлом году, оказались 500 млн рублей. Об этом на форуме «Кибербезопасность в финансах» рассказал глава Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России Филипп Немов.

Он отметил, что преступники активно используют методы социнженерии, и жертва может постоянно переводить аферистам деньги: «Люди попадают в тяжелейшие ситуации: действия, которые совершает человек под воздействием социальных инженеров, подпадает под договор между гражданином и банком, и банк ответственности не несёт. Нет оснований для возмещения средств жертве».

У ХАКЕРОВ ИЗЪЯЛИ КРИПТОВАЛЮТУ НА МИЛЛИАРД РУБЛЕЙ И ОТПУСТИЛИ ИХ С МИРОМ

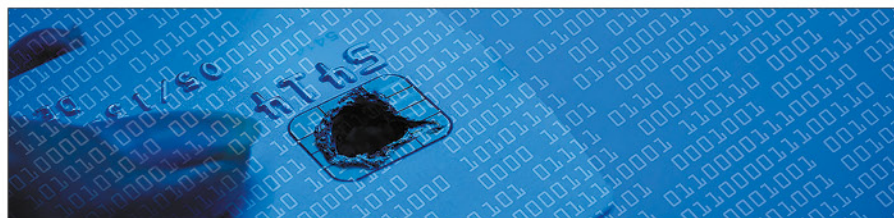
Таганский районный суд Москвы вынес приговор членам группировки Infraud Organization по делу о торговле данными банковских карт.

Все подсудимые — Марк Бергман, Константин Бергман, Кирилл Самокутяев и Андрей Новак — признаны виновными по ч. 2 ст. 187 УК РФ («Неправомерный оборот средств платежей, совершённый организованной группой»). Все они получили условные сроки от 2,5 до 3,5 лет с такими же испытательными периодами. Сначала фигурантам грозило до 7 лет тюрьмы, но они полностью признали свою вину, и суд учёл это как сильно смягчающее обстоятельство.

Согласно данным стороны обвинения, братья Бергманы создали торговую площадку, на которой продавались похищенные данные банковских карт и иностранных

номеров социального страхования. Новак и Самокутяев к группе присоединились позже.

Злоумышленники были задержаны в начале прошлого года после контрольной закупки. У них изъяли криптовалюту на сумму более 1 млрд рублей.



СКАМЕРЫ «АРЕСТОВЫВАЮТ» НАКОПЛЕНИЯ ПОТЕНЦИАЛЬНЫХ ЖЕРТВ

Российские абоненты стали получать звонки и письма якобы от Росфинмониторинга с сообщением о блокировке их денежных средств и предложением снять ограничения за определённую плату.

«Федеральная служба по финансовому мониторингу информирует об участвовавших случаях поступления гражданам звонков и электронных писем от имени Росфинмониторинга с извещениями о блокировке (замораживании) их денежных средств и предложениями снять ограничения за плату под различными предлогами

(оплатить штраф, пени, комиссию, услугу по оформлению «справки о легализации» и другие)», — отметили в самом ведомстве.

И добавили, что Росфинмониторинг не имеет полномочий арестовывать денежные средства и иное имущество граждан, взимать обязательные платежи и оказывать платные услуги по оформлению юридически значимых документов. А в случае получения гражданином такого звонка или сообщения ведомство просит уведомить об этом его дежурную службу, а также правоохранителей.

БАНК РОССИИ БУДЕТ ИЗУЧАТЬ ИИ

Банк России планирует создать центр компетенций по искусственному интеллекту, заявила первый заместитель председателя ЦБ Ольга Скоробогатова.

По словам Скоробогатовой, с учётом того, как развивается тема ИИ, «надо реально понять и осознать, каким образом мы будем этим управлять». ИИ позволяет автоматизировать огромные массивы данных и создавать логические цепи, а также помогает принимать решения. Однако есть и риски: когда машины

выходят на уровень, где они сами себя программируют и обучают, они могут выйти из-под контроля. Именно поэтому Банк России будет изучать этот вопрос.

Преимуществами ИИ активно пользуются участники финансового рынка. Сбер оценил финансовый эффект от внедрения ИИ в банке в 230 млрд руб. Банк использует ИИ в основных процессах ипотечного кредитования и сопутствующих услуг. Главными угрозами аналитики Сбербанка назвали сильный ИИ, который сможет создать самообучающееся ПО и будет обходить методы защиты данных, а также квантовые компьютеры, которые могут поставить под угрозу надёжность классических методов шифрования.

В марте этого года российский брокер «Открытие инвестиции» внедрил отечественную облачную платформу Beorg Smart Vision на базе ИИ для автоматической оцифровки документов и распознавания изображений.



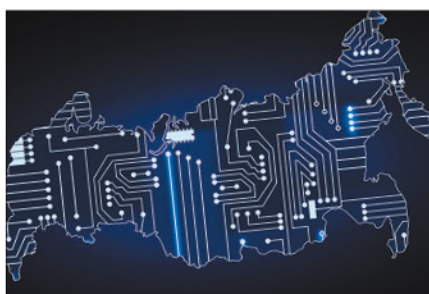
В СТОРОНУ ТЕХНОЛОГИЧЕСКОГО СУВЕРЕНИТЕТА

С 20 апреля электроника с процессорами российского производства получит наивысший приоритет при госзакупках.

«Правительство продолжает работу по обеспечению технологического суверенитета. Подписано постановление, которое даёт преимущество отечественной электронике с российскими процессорами в ходе закупок для государственных и муниципальных нужд. Если на конкурс поступит такая заявка, у неё будет наивысший приоритет», — заявил Михаил Мишустин.

«При проведении государственных закупок будет действовать трёхуровневый механизм допуска электроники. Наивысший приоритет получит российская техника, работающая на российских процессорах. Она будет классифицироваться как продукция «первого уровня» и иметь соответствующую отметку в реестре Минпромторга. Если на российской

технике установлены компоненты иностранного производства, то она будет считаться продукцией «второго уровня» и станет закупаться только в случае отсутствия предложений по продукции «первого уровня». Полностью иностранная техника определена как продукция «третьего уровня». Предложения о таких поставках будут рассматриваться в последнюю очередь», — гласит постановление Правительства РФ № 486 от 27 марта 2023 г. Постановление вступает в силу с 20 апреля.



ОТКРОЕМ СЧЁТ ПО ВИДЕО

Директор департамента финмониторинга и валютного контроля Банка России Илья Ясинский сообщил, что уже в следующем году россияне смогут открывать банковские счета по видеосвязи. Идея обсуждается как в самом ЦБ РФ, так и в Росфинмониторинге.

Представитель регулятора добавил, что новую механику протестируют, используя положения экспериментального правового режима: «Надеюсь, видеопроверка проявит себя положительно, и мы сможем, наконец, отказаться от атак в виде личного присутствия при открытии счёта».

Ранее СМИ сообщали, что Национальный совет финансового рынка предложил ЦБ провести подобный «пилот». Это было продиктовано потребностями в первую очередь граждан с ограниченными возможностями здоровья.

18 % РАБОЧИХ МЕСТ ДОЛОЙ!

Авторы доклада банка Goldman Sachs уверены, что искусственный интеллект и ПО на его основе могут привести к сокращению 300 млн специалистов по всему миру. Конкретно в США и Европе автоматизации — частичной или полной — подлежат две трети рабочих мест.

Наименьшему риску, как утверждается, подвержены работники, связанные с физическим трудом и уборкой помещений. В «красной зоне» — бухгалтеры. Темпы замещения разнятся в зависимости от уровня развития страны: «В развивающихся странах рабочие места меньше подвержены автоматизации, чем в развитых. В целом во всём мире будут автоматизированы 18% рабочих мест».

Исследователи уточнили: прогресс не только устраняет профессии и рабочие места, но и создаёт новые, а использование ИИ-разработок будет способствовать росту мирового ВВП на 7%.

КВАНТОВЫЙ ПЕРЕХОД ФИНТЕХА

ОПАСНОСТЬ, ИСХОДЯЩАЯ ОТ КВАНТОВЫХ КОМПЬЮТЕРОВ, ПОКА НАХОДИТСЯ В ТЕОРЕТИЧЕСКОЙ ПЛОСКОСТИ. НО ПОЧЕМУ С ПЕРЕХОДОМ НА КВАНТОВЫЕ ТЕХНОЛОГИИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ДАННЫХ НЕ СЛЕДУЕТ МЕДЛИТЬ?



В далёком 1959 году выдающийся американский физик-теоретик Ричард Фейнман прочитал в Калифорнийском институте технологий лекцию под названием «Внизу много места: приглашение в новую область физики», в которой впервые привёл теоретическое обоснование использования квантовых эффектов для вычислений. Более десяти лет спустя учёный из Колумбийского университета Стивен Визнер высказал идею использования квантовых объектов для защиты информации. А в 1983 г. он предложил создать квантовые банкноты — такие, которые нельзя скопировать, поскольку, согласно квантовым законам, факт измерения объекта изменяет его состояние.

Чтобы осуществить эту идею, на каждой банкноте нужно было реализовать ловушку с фотонами, причём каждая из частиц поляризована определённым образом по двум разным базисам. Например, один фотон мог быть поляризован под углом 0° или 90° от некоторой вертикали, а второй — под углом 45° и 135° . Чтобы скопировать банкноту, необходимо измерить поляризации фотонов, но никто, кроме Центрального банка страны, не знает, какие поляризации соответствуют номеру конкретной банкноты. Если расположить на каждой банкноте десяток ловушек, количество фотонов на ней будет большим, а вероятность случайного угадывания в процессе перебора вариантов стремится к нулю.

Правда, ловушек фотонов, пригодных для размещения на банкнотах, не было ни в тот момент, ни в настоящее время... Но сама идея оказалась весьма плодотворной: уже через год после публикации статьи Стивена Визнера физики Жиль Брассар и Чарльз Беннет разработали первый протокол для квантовой связи BB84, получивший своё название по первым буквам их

фамилий. Этот протокол до сих пор широко применяется в современных квантовых сетях связи.

КАК АЛИСА И БОБ ЗАНЯЛИСЬ КВАНТОВЫМИ СОСТОЯНИЯМИ ОДИНОЧНЫХ ФОТОНОВ

Беннет и Брассар предложили кодировать данные в виде квантовых состояний одиночных фотонов, например, с помощью различных вариантов поляризации. Максим Агаджанов, редактор «Хабр», рассказывает, каким образом в этом случае Алиса и Боб — два классических персонажа криптографических кейсов — осуществляют засекреченный обмен сообщениями (ключами): «Алиса посылает Бобу фотоны, поляризованные в одном из двух, неортогональных друг другу, базисах: прямоугольном или диагональном. Боб получает их, измеряет поляризацию, выбирая базисы для измерения случайным образом, и записывает результаты измерений и базисы. Затем он и Алиса обмениваются информацией об использованных базисах (но не о результатах измерения) по открытому каналу, и данные, полученные при несовпавших базисах, сбрасываются. Остаются только значения, измеренные в совпадающих базисах» (рис. 1).

Хакер Ева может перехватить одиночный фотон, измерить его поляризацию и попытаться переслать копию фотона Бобу, но это тут же вызовет сообщение об ошибке при передаче квантового ключа. Алиса и Боб сравнивают небольшую часть ключа по открытому каналу, и если уровень ошибок не превышает некоторого порогового значения, значит, связь безопасна.

Учёные создали экспериментальную установку абсолютно защищённой квантовой связи — она могла передавать данные на расстояние 32,5 см. А через несколько лет — в 1989 г. — корпорация IBM реализовала свою первую

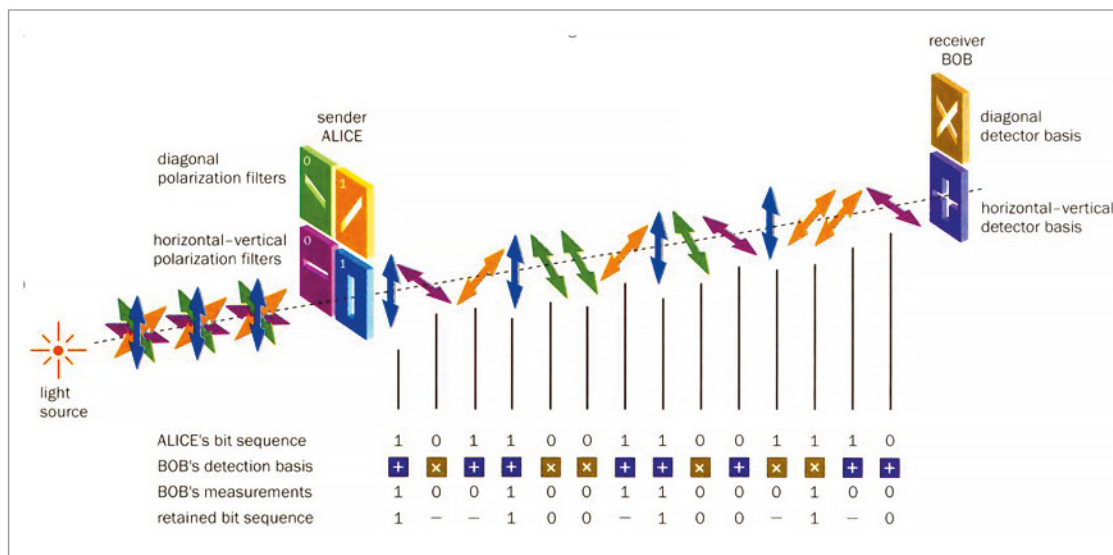


Рисунок 1. Схема кодирования данных в виде квантовых состояний одиночных фотонов с помощью их поляризации. Источник: <https://habr.com/ru/>, июль 2019 г.

квантово-криптографическую схему, работавшую на подобных принципах. В ней данные передавались приблизительно на 1 м.

КВАНТОВЫЙ КОМПЬЮТЕР: ВРЕМЯ БОЛЬШИХ ОЖИДАНИЙ

80-е годы прошлого века можно с полным правом назвать динамичным прорывом квантовых технологий в практическую жизнь. В 1981 г. Ричард Фейнман публикует очередную знаковую статью «Физическое моделирование с помощью компьютеров», в которой впервые была предложена базовая модель квантового компьютера. В частности, квантовый бит — кубит — может насчитывать большее количество состояний, чем традиционная пара значений классического бита: «0» или «1». Механизм формирования кубита определяется эффектом квантовой суперпозиции. Он предполагает, что атом вещества может находиться в состоянии «0» либо «1», а также может хранить сразу два значения. Значит, если проводить с кубитом какие-либо операции, то они будут происходить одновременно и с нулем, и с единицей. А если взять множество таких атомов, то за одну операцию можно произвести большое количество однотипных вычислений.

Эта особенность квантовых битов определяет гораздо более высокую производительность квантовых компьютеров по сравнению с традиционными, и, по сути, говорит о переходе вычислительной техники в новую реальность, в которой больше не действует закон Мура. В этой реальности компьютеры строятся на принципиально иных физических принципах. В качестве кубитов могут использоваться охлаждённые до

сверхнизких температур атомы, отдельные электроны или ядра некоторых атомов, сверхпроводящие кольца, фотоны.

За счёт своей производительности квантовые компьютеры способны эффективно справляться с задачами, где требуется перебор большого количества данных и вычислительная мощность, недоступная классическим компьютерам. Таких задач очень много: улучшенные метеорологические прогнозы, создание новых лекарственных форм, более точный расчёт химических реакций — этим направлением занимается целая отрасль науки — вычислительная квантовая химия, а также ускорение машинного обучения, анализ больших данных, задачи оптимального управления.

КВАНТОВЫЙ КОМПЬЮТЕР: ВРЕМЯ БОЛЬШИХ ОПАСЕНИЙ

Необычайно высокая производительность квантового компьютера — это, можно сказать, экзистенциальная угроза традиционной криптографии, особенно наиболее популярному сегодня варианту шифрования с открытым ключом. Дело в том, что его главные элементы: генерация пары — открытый и закрытый ключ, а также алгоритм шифрования — базируются на нескольких допущениях.

Первое — имитация случайных процессов. В традиционном шифровании генератор случайных чисел, который используется при создании ключа, имеет псевдослучайный характер: в основе генерации лежит некоторая формула, которая теоретически может быть раскрыта. Математики всего мира тратят усилия на то, чтобы генерируемый ключ был максимально

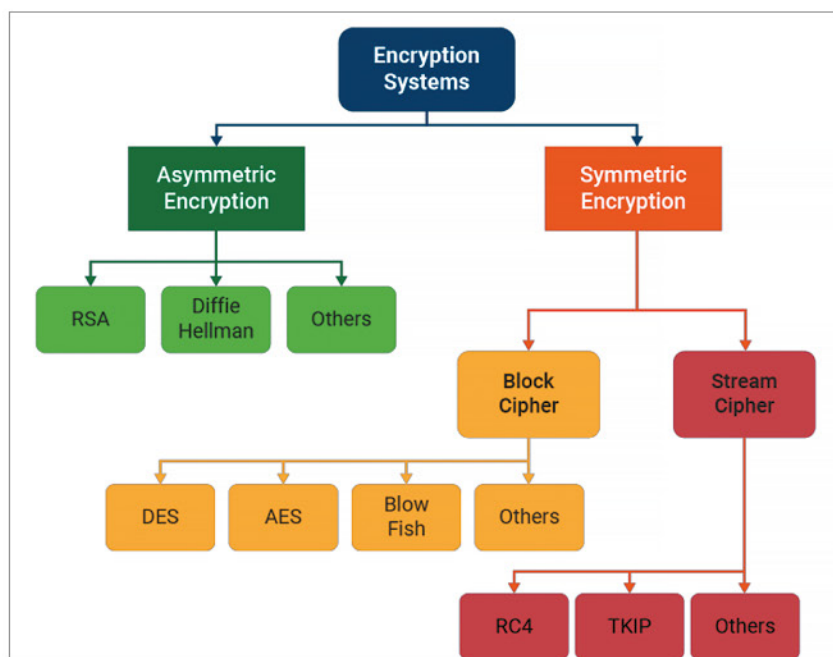


Рисунок 2. Основные виды криптографии и соответствующие алгоритмы.
Источник: Quantum Computing and Cybersecurity. Preparing for Post-Quantum Cryptography. Исследование PRESCOUTER, апрель 2022 г.

близок к абсолютно случайной последовательности (рис. 2).

Так, в 1984 г. Голдрайх, Голдвассер и Микали описали свою концепцию конструирования псевдослучайных функций (PRF), которые выглядят случайными для противника. Дальнейшим развитием PRF стал механизм псевдослучайных перестановок, который стал ядром блочного шифра. Яркий пример блочного шифра, использующего псевдослучайные перестановки, — AES.

В квантовой криптографии важным элементом схемы является квантовый генератор случайных чисел (КГСЧ), который имеет вид не математической абстракции, а физического оптического процесса: фотоны света от источника друг за другом направляются на полупрозрачное зеркало и детектируются двумя приёмниками. Срабатывание одного из них означает «1», другого — «0». Сегодня устройства КГСЧ — это оборудование, которое можно приобрести на рынке.

Второе важное условие секретности современного шифрования — невозможность взлома зашифрованного сообщения за приемлемое время. С точки зрения математики, ключ представляет собой результат произведения ряда простых чисел. Соответственно, поиск ключа связан с разложением некоторого большого числа на простые множители (задача факторизации). Для большого количества простых чисел задача факторизации имеет очень высокую вычислительную сложность.

Ещё одна серьёзная математическая задача — дискретное логарифмирование — связана, в частности, с задачей взлома схемы электронной подписи ECDSA, основанной на использовании эллиптических кривых. Алгоритм принят многими компаниями в мире в качестве стандарта и реализован в большом количестве криптографических библиотек. Именно этот алгоритм используется для обеспечения безопасности биткоина: каждый биткоин-адрес является криптографическим хешем открытого ключа ECDSA. Владелец учётной записи определяется тем, кто контролирует закрытый ключ ECDSA.

Таким образом, математическим основанием популярных криптографических алгоритмов, которые признаны мировыми стандартами, являются две математических процедуры — задача факторизации целых чисел и задача дискретного логарифмирования. Гарантия их безопасности — высокая вычислительная сложность этих алгоритмов, что делает практически невыполнимой взлом ключа с помощью современных компьютеров.

Однако квантовые вычисления настолько ускоряют факторизацию простых чисел, что компьютеры с квантовыми вычислениями могут легко взломать криптографические ключи с помощью быстрых вычислений и исчерпывающего поиска секретного ключа. Так на сцене появился CRQC (Cryptographically Relevant Quantum Computer, криптографически релевантный квантовый компьютер) — устрашающий образ грядущего квантового компьютера, который способен взломать большую часть нынешних криптографических систем с открытым ключом, используемых в цифровых системах во всём мире. Мало того, для него уже разработан подходящий математический инструментарий.

МАТЕМАТИЧЕСКИЙ ИНСТРУМЕНТАРИЙ «БОЛЬШОГО КВАНТОВОГО ВЗЛОМЩИКА»

Ещё в 1995 г. математик Питер Шор, трудившийся тогда в компании AT&T, опубликовал алгоритм полиномиальной сложности для разложения числа на простые множители и дискретного логарифмирования на квантовом компьютере. А через год появился алгоритм Гровера, который обеспечивает квадратичное ускорение решения задачи поиска по неструктурированной базе данных. Эти два алгоритма для квантовых компьютеров бросают вызов современным системам криптографии.

«Наиболее широко используемые на практике алгоритмы асимметричного шифрования RSA, DSA, ECDSA, EdDSA, EC-SDSA перестают быть криптостойкими и взламываются

Криптографический алгоритм	Тип	Цель	Влияние квантового компьютера
AES	Симметричный ключ	Шифрование	✓ Безопасно для больших ключей (256 бит)
SHA-2, SHA-3	Алгоритм хеширования	Хеширование	✓ Безопасно для больших размеров выходных данных (256 бит)
RSA	Открытый ключ	Подписи, создание ключа	✗ Больше небезопасно
ECDSA, ECDH	Открытый ключ	Подпись, обмен ключами	✗ Больше небезопасно
DSA	Открытый ключ	Подпись, обмен ключами	✗ Больше небезопасно

Рисунок 3. Воздействие взломов квантового компьютера на популярные алгоритмы шифрования. Источник: Quantum Computing and Cybersecurity. Preparing for Post-Quantum Cryptography. Исследование Prescouter, апрель 2022 г.

(находится секретный ключ) за полиномиальное от размера публичного ключа время», — говорит Игорь Голдовский, директор Департамента инноваций, главный архитектор АО НСПК в своей статье «Постквантовая криптография. Готовимся сегодня?», опубликованной в журнале Plus World в марте 2022 г. (рис. 3).

Правда, как отмечает Виктор Алексеев в своей статье «Квантовая криптографическая катастрофа. Часть 1» («Современная электроника», № 1/2023), составные числа можно разложить на простые множители с помощью алгоритма Шора и квантового компьютера в приемлемое время, но не абсолютно точно, а лишь с некоторой вероятностью. К тому же использовать для этих целей нужно весьма производительный квантовый компьютер (свыше 7000 кубитов).

Последствия от появления квантовых компьютеров для алгоритмов симметричного шифрования и хеш-функций не столь катастрофичны, отмечает Игорь Голдовский. В случае симметричных алгоритмов шифрования можно просто удвоить длину ключа, чтобы добиться прежней криптостойкости, не меняя при этом криптографического алгоритма. Ещё меньшее влияние появление квантовых компьютеров окажет на стойкость хеш-функций: асимптотически потребуется увеличить длину значения хеш-функции в полтора раза, например, вместо функции SHA-256 применять функцию SHA-384.

Таким образом, в будущем даже надёжные криптографические алгоритмы будут значительно ослаблены квантовыми вычислениями, в то время как другие вообще не будут в безопасности. Вопрос только в том, насколько отдалённым является это будущее.

ТАК ВОТ ТЫ КАКОЙ, СОВРЕМЕННЫЙ КВАНТОВЫЙ КОМПЬЮТЕР!

Практическая реализация квантового компьютера — ровесница века. Первая эксперимен-

тальная демонстрация 2-кубитного квантового компьютера на основе технологии ядерного магнитного резонанса (ЯМР-компьютер) состоялась в 2000 году. На следующий год американские учёные из Стенфордского университета совместно со специалистами IBM создали 7-кубитный квантовый ЯМР-компьютер, который был успешно использован для исполнения алгоритма Шора: число «15» было факторизовано квантовым компьютером на массиве из 1018 идентичных молекул, каждая из которых содержала семь активных ядерных спинов.

В ноябре прошлого года корпорация IBM представила квантовый процессор Osprey на 433 кубита (рис. 4), а в 2025 г. выпустит процессор Koikaiburga с 4158 кубитов. В дорожной карте развития квантовых компьютеров IBM сформулирована долгосрочная цель — построить квантовую систему на миллион кубитов.

Канадская компания D-Wave Systems представила ещё в 2017 г. свой квантовый компьютер D-Wave 2000Q на базе 2048-кубитного процессора W2K и репозиторий программных инструментов с открытым кодом. Это коммерческое

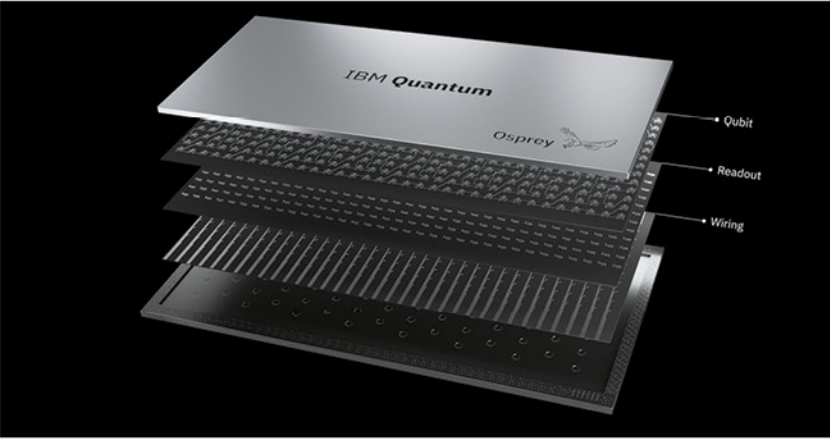


Рисунок 4. Квантовый процессор IBM Quantum Osprey на 433 кубита. Источник: IBM, ноябрь 2022 г.

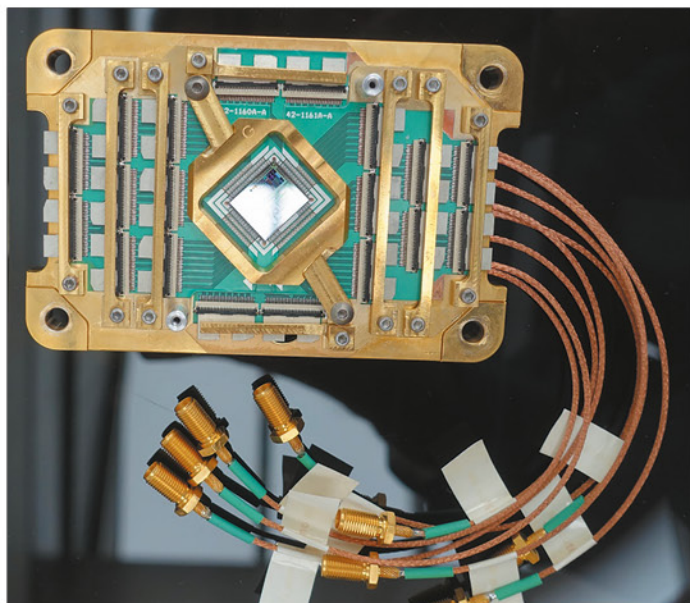


Рисунок 5. Процессор «Везувий» фирмы D-Wave на 512 кубит в обвязке охлаждения. Источник: <https://commons.wikimedia.org>, май 2018 г.

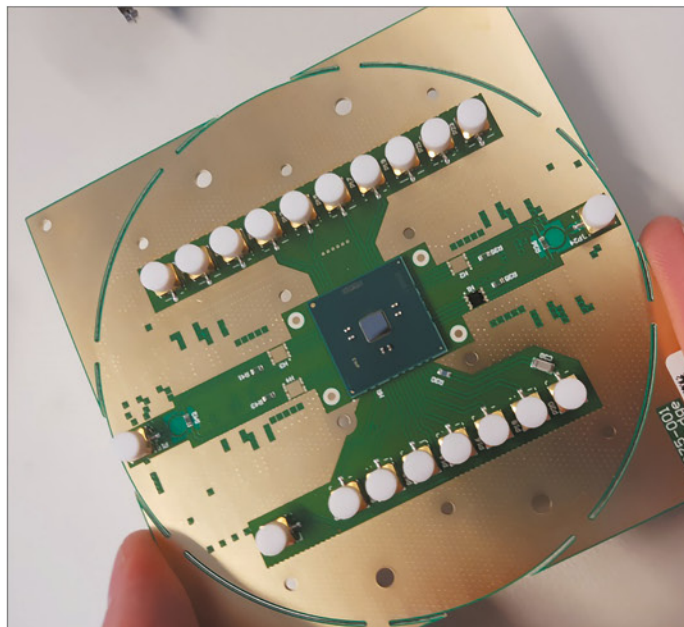
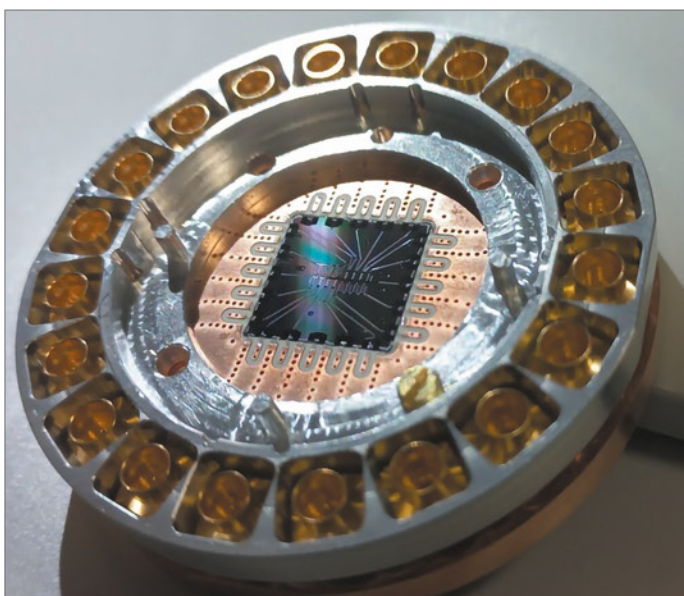
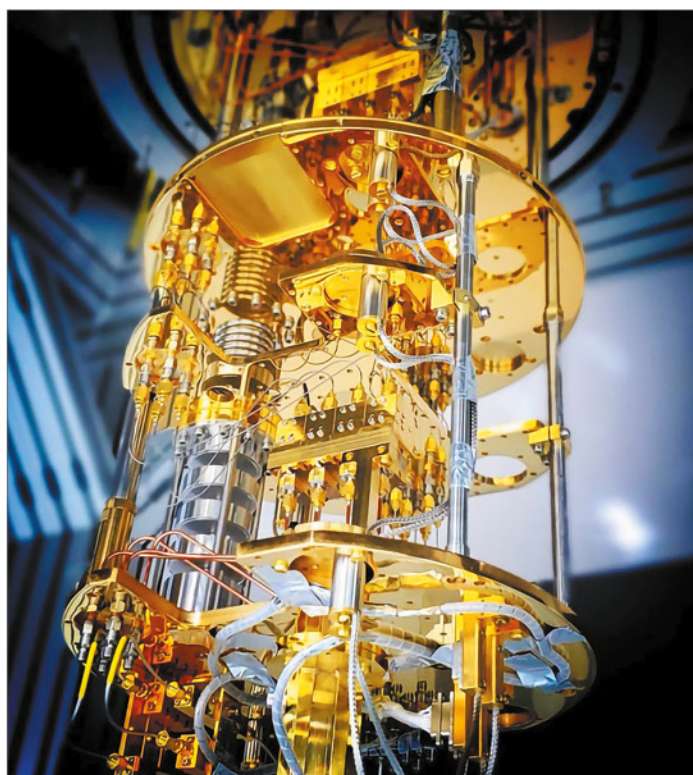


Рисунок 6. Контроллер кремниевых кубитов Intel Horse Ridge. Источник: <https://naukatehnika.com>, февраль 2020 г.



↑ **Рисунок 8.** Держатель с чипом квантового процессора в центре. Источник: Лаборатория искусственных квантовых систем МФТИ, ноябрь 2022 г.

← **Рисунок 7.** Китайская установка с квантовым процессором KF C6-130 на основе сверхпроводящих кубитов. Источник: Origin Quantum, <https://3dnews.ru>, февраль 2023 г.

оборудование, которое поставляется таким заказчикам, как Google, Lockheed Martin, NASA, по цене 10–15 млн долл. В планах компании — выпуск коммерческого квантового компьютера D-Wave Next Gen на базе процессора с более чем 5000 кубитов.

Правда, D-Wave Systems разрабатывает специфические адиабатические компьютеры, реализующие механизм «квантового отжига»,

способные эффективно решать специализированные задачи оптимизации. Однако эти компьютеры не подходят для работы с традиционными квантовыми алгоритмами (рис. 5).

Компания Intel в начале 2018 г. объявила о тестовой поставке квантового процессора Tangle Lake на 49 кубитов. Но у неё также есть уникальное направление разработки — миниатюрных кремниевых квантовых процессоров на



Рисунок 9. Российские квантовые вычисления для решения задач индустрии к 2024 г. Источник: Дорожная карта развития «сквозной» цифровой технологии «Квантовые технологии» до 2024 г., Москва, 2019 г.

миллионы кубитов, которые можно охлаждать почти до абсолютного нуля. В 2019 г. компания показала контроллер кубитов Horse Ridge, который может работать при таких температурах. В будущем он поможет масштабировать многокубитовые квантовые системы (рис. 6).

Осенью прошлого года Intel заявила, что создала квантовое устройство будущего на основе существующего оборудования, то есть готова производить устройства с кремниевыми спиновыми кубитами на базе существующих производственных процессов.

Первую «большую» китайскую квантовую систему выпустила в 2021 г. компания Origin Quantum — 24-кубитовый компьютер Wuyuan использует сверхпроводящие кубиты. При этом разработчики Origin Quantum двигаются сразу по двум направлениям: по линии сверхпроводящих кубитов они стремятся настигнуть IBM, а в части кремниевых (спиновых) кубитов наступают на пятки Intel. За три года Origin Quantum анонсировала более 10 различных квантовых чипов. В ближайших планах компании — квантовый компьютер Wukong на 64 кубита.

Кроме того, Origin Quantum создала операционную систему для квантовых компьютеров и пакет полезного ПО, включая доступ к

платформе Wuyuan через облачные сервисы. На облачный сервис квантовых вычислений Origin Quantum уже подписано более 100 компаний (рис. 7).

В нашей стране проект создания квантовых информационных систем на основе сверхпроводящих кубитов стартовал в 2016 г., а в 2018 г. добавились проекты по развитию других платформ квантовых вычислений: нейтральных атомов в оптических ловушках и интегральных оптических чипов. В ноябре 2022 г. специалисты МФТИ и МИСиС создали четырёхкубитный квантовый процессор на базе сверхпроводниковой интегральной квантовой микросхемы, которую изготовили сотрудники лаборатории искусственных квантовых систем МФТИ (рис. 8).

В этой лаборатории идёт разработка 12- и 16-кубитных квантовых процессоров и тестируется 8-кубитный процессор, который способен выполнить несколько сотен последовательных операций за время жизни кубитов. Сегодня на рабочем квантовом процессоре решается ряд задач машинного обучения, в частности, для медицинской диагностики. К 2024 г. планируется разработать четыре типа российских квантовых компьютеров размером от 50 до 100 кубитов (рис. 9).



Рисунок 10. Дорожная карта развития ПО и систем квантовых вычислений корпорации IBM. Источник: IBM, TAdviser, февраль 2021 г.

Мир движется в сторону коммерческих решений квантовых компьютеров. Корпорация IBM говорит, что её конечная цель — разработка полнофункционального квантового компьютера, развёрнутого через облако и доступного любому человеку в мире. До 2024 г. IBM делает доступными для разработчиков динамические квантовые схемы (последовательности инструкций для выполнения), язык ассемблера для квантовых компьютеров OpenQASM3, а также библиотеки готовых квантовых схем для разработчиков (рис. 10).

Российские учёные также работают над специализированным облачным софтом. Так, в апреле 2021 г. Российский квантовый центр (РКЦ) запустил универсальную облачную платформу квантовых вычислений, которая позволяет решать прикладные бизнес-задачи на квантовых процессорах без специальных знаний в квантовой механике. Собственную платформу представил также Центр квантовых технологий МГУ им. М. В. Ломоносова.

БАРЬЕРЫ ДЛЯ ПРОИЗВОДИТЕЛЬНОГО КВАНТОВОГО КОМПЬЮТЕРА

Наращивание кубитов — совсем непростое занятие. Одна из главных проблем — декогеренция,

то есть постепенная потеря системой квантовых свойств за счёт взаимодействия с окружающей средой. Учёные всего мира бьются за увеличение времени, в котором удерживается заданное квантовое состояние кубитов, для того чтобы с ними можно было производить необходимые операции. Сегодня это время составляет в разных физических исполнениях от десятков микросекунд до нескольких секунд. За это время удаётся произвести несколько сотен квантовых операций с кубитом, после чего кубит нужно снова инициализировать.

Причём проблемы с декогеренцией начинают стремительно расти по мере увеличения количества кубитов, что ведёт к снижению точности выполнения квантовых операций. Евгений Глушков говорит в своей статье «В погоне за миллионом кубитов» (ресурс <https://naked-science.ru>, декабрь 2021 г.): «Если точность выполнения квантовых операций на одном кубите составляет 99%, то на 10 кубитах правильный результат будет выдаваться уже лишь в девяти из 10 раз, а на 100 кубитах и вовсе лишь треть выдаваемых результатов будут иметь смысл».

В квантовой истории большее количество кубитов даёт скорее большее количество ошибок и неустойчивости, чем прямой рост производительности. Время появления универсального

квантового компьютера с десятками тысяч кубитов, необходимых для взлома любых современных шифров, — под большим вопросом.

Научная и практическая мысль стала развиваться по нескольким специализированным направлениям. Среди них — создание того самого криптографически релевантного квантового компьютера (Cryptographically Relevant Quantum Computer — CRQC), способного взламывать существующие шифры.

Несмотря на то что пока у квантовых компьютеров нет такой мощности, которой было бы достаточно для полноценной атаки, реальная опасность есть уже сейчас, считает Антон Гугля, руководитель российской компании QArp: злоумышленник может сохранить данные, зашифрованные традиционной асимметричной криптографией, и взломать её позже, когда получит доступ к достаточно мощному квантовому компьютеру. А это значит, что в зоне риска оказываются данные, которые будут актуальны в перспективе десяти и более лет: персональные, финансовые данные, а также данные корпоративной, государственной и военной тайны.

США уже вовсю готовятся к этому будущему. В нынешнем году завершается фаза первичного накопления и анализа различных методов, подходов, алгоритмов, практических решений постквантовой криптографии и начинается стадия стандартизации и перехода рабочих систем на стандарты криптографии, которые будут установлены Национальным институтом стандартов и технологий США (NIST). Он завершится к 2030 г. В частности, в начале марта стало известно, что структуры НАТО начали использовать систему защиты от кибератак с использованием квантовых вычислений.

Таким образом, мир, вступивший в фазу нарастающего силового геополитического противостояния, усиливает свои оборонно-наступательные киберресурсы за счёт достижений квантового и постквантового шифрования. Это очередной вызов, который из теоретических предположений на уровне технофутурологии перешёл в фазу практической потребности.

Хорошая новость заключается в том, что если использовать квантовые явления, то уже сегодня можно создать систему секретной связи между условными Алисой и Бобом, которая будет нивелировать риски атак квантового компьютера. Для создания таких систем сегодня используется два основных подхода: квантовое шифрование и постквантовые алгоритмы шифрования.

КОММЕРЧЕСКИЕ РЕШЕНИЯ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Квантовое шифрование реализуется с помощью оборудования, которое включает оптический генератор случайных чисел и устройство квантового распределения ключей.

Как рассказывает Сергей Кулик, научный руководитель Центра квантовых технологий физического факультета МГУ, с помощью протоколов квантового распределения ключей (КРК) стороны, соединённые по открытому каналу связи, могут создать общий случайный ключ, который известен только им, и использовать его для шифрования и расшифровывания сообщений. При этом ключ распределяется по всем участникам, для которых доступна квантовая связь (по абонентам квантовой сети). Таким образом, долговременные ключи шифрования уходят в прошлое, их заменяют быстро меняющиеся ключи. В результате задача, которую должен решить CRQC, существенно усложняется: он имеет дело со случайной генерацией ключей, близкой к идеальному оракулу, и сменой ключей с частотой на уровне секунд (рис. 11).

Передача информации осуществляется в квантовых состояниях: фотоны распределяются с помощью квантового канала (созданного, например, на основе волоконно-оптической связи) и обнаруживаются с помощью однофотонных детекторов. В такой системе действует квантовый принцип: подслушивание извне однозначно фиксируется как ошибка в передаче, что делает пассивное вмешательство в процесс передачи секретных данных невозможным. Более того, в такой конфигурации становится невозможной атака класса «человек посередине», так как ключи шифрования в сети формируются в автоматическом режиме.

Главной проблемой квантовой связи являются сегодня дальность действия и скорость

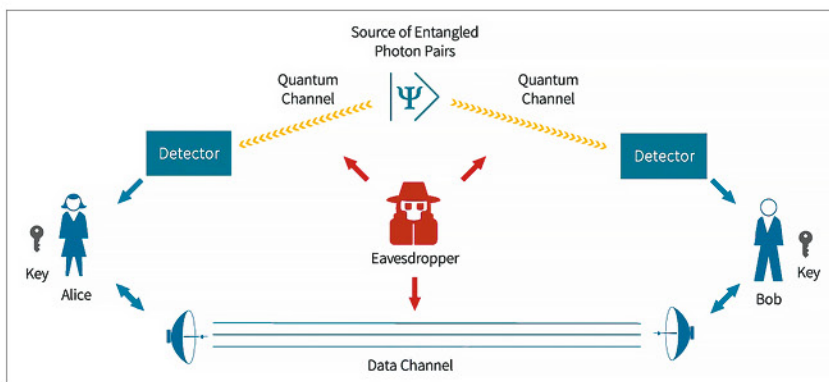


Рисунок 11. Схема двухузловой реализации квантового распределения ключей. Источник <https://s-fifteen.com/pages/qkd-horizontal-timeline>

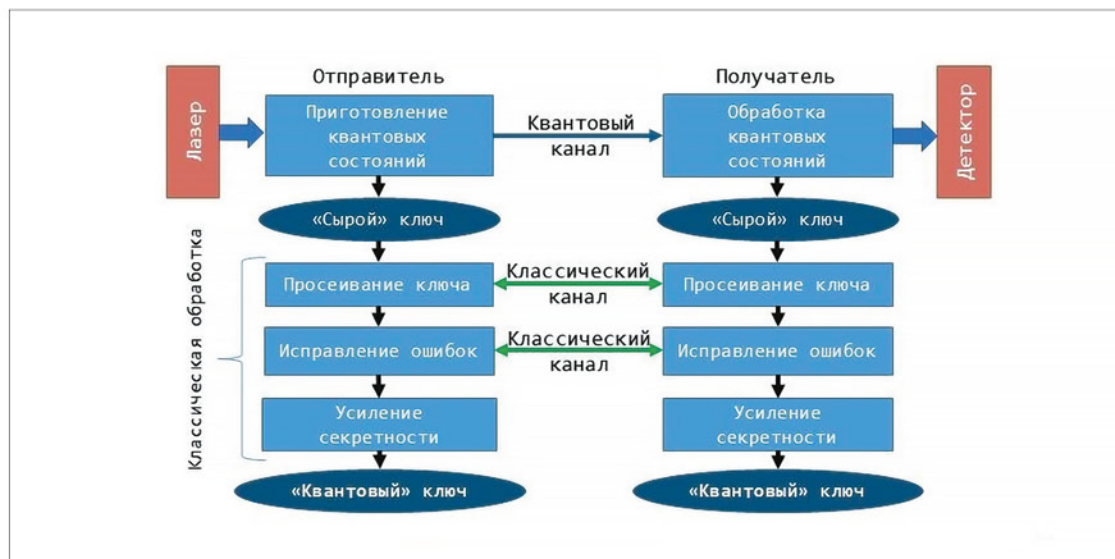


Рисунок 12. Типовая схема квантового протокола распределения ключей. Источник: «ИнфоТеКС», <https://habr.com/ru/>, ноябрь 2022 г.

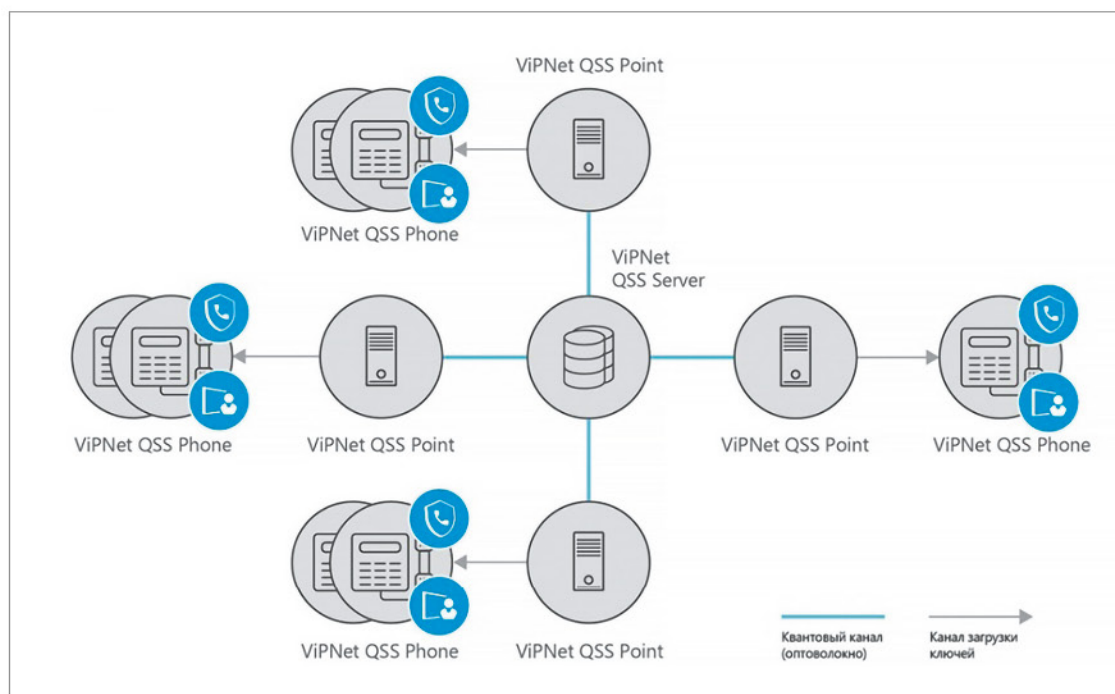


Рисунок 13. Схема работы ViPNet QSS. Источник: «ИнфоТеКС»

передачи данных в силу того, что одиночные фотоны, передаваемые по линии квантовой связи, очень уязвимы для помех и шумов. Поэтому в практических проектах магистральной линии квантовой связи обычно ориентируются на гарантированную передачу квантового ключа на 100 км.

Осенью 2022 г. компания «ИнфоТеКС» получила положительное заключение ФСБ России на свою систему квантового распределения ключей ViPNet QSS. Она стала первой в России

системой такого рода, сертифицированной по требованиям ФСБ России и готовой к эксплуатации на российских предприятиях (рис. 12).

ViPNet QSS предназначена для выработки и распределения квантово-защищённых ключей между абонентами, а также для защиты пользовательского трафика (цифровые аудиозвонки и текстовые сообщения), передаваемого между абонентами. ViPNet QSS позволяет построить сеть квантового распределения ключей топологии «звезда», к которой может быть подключено



Рисунок 14. Квантовый телефон «ИнфоТеКС»

свыше 150 тыс. СКЗИ — потребителей квантово-защищённых ключей (рис. 13). Она использует аппаратный датчик случайных чисел.

В данной разработке учтены риски различных возможных атак на квантовые состояния: PNS — атака с разделением числа фотонов, BS — атака со светоделителем, унитарная атака, UM — атака с определённым исходом, а также оптические атаки на КРК: атака Trojan-horse, атака с лазерным повреждением компонентов, атака с переизлучением (Backflash) детектора, импульсное и непрерывное ослепление детектора, атаки Time-shift и Efficiency mismatch.

На базе данного решения в МГУ имени М. В. Ломоносова в 2021 г. заработала университетская квантовая сеть. Она соединила пять квантовых устройств, распределяющих квантовые ключи на двадцать абонентских терминалов. Максимальная длина канала квантово-защищённой связи в рамках проекта составила 40 км.

Эта сеть стала полигоном для предсерийных испытаний первого в России «квантового» телефона ViPNet QSS Phone, входящего в комплекс ViPNet QSS. «Квантовый телефон» может работать также в режиме текстового чата в топологии «все-со-всеми». Таким образом, интеграционное решение системы ViPNet QSS с защищённым IP-телефоном образует криптографическую систему для защищённого информационного взаимодействия абонентов, при которой голосовая связь и обмен сообщениями в чате шифруются ключами, неизвестными даже администратору сети (рис. 14).

В принципе, к этой сети можно подключать и мобильные устройства пользователей с помощью специального ПО, также сертифицированного для определённого класса защиты.

Вместе с Центром квантовых технологий МГУ «ИнфоТеКС» ведёт разработку устройства, обеспечивающего защищённый документооборот

Аппаратное ускорение постквантовых алгоритмов	Операционные системы	Активное сетевое оборудование	Смарт-карты и криптографические токены	Мобильные платформы	Инфраструктура интернета вещей
Инструкции для аппаратного ускорения постквантовой криптографии в текущих версиях процессоров	Интеграция квантово-устойчивых алгоритмов в СКЗИ по-умолчанию	WAF (web application firewall), NGFW (Next Generation Firewall), UTM(Unified Threat Management) системы	Криптографические токены	Интеграция в аппаратный корень доверия устройств на основе ARM	Расширения платформенной криптографии в IoT-платформах
Криптографические сопроцессоры с поддержкой постквантовой криптографии	Интеграция квантово-устойчивых алгоритмов в реализации протоколов выполненных на уровне ядра	TLS-шлюзы	SIM-карты	Интеграция на уровне системного криптографического провайдера ОС на основе Android	Организация безопасного доступа к клиентским данным
	Интеграция квантово-устойчивых алгоритмов в подсистемы поддержки доверенной загрузки и криптопроцессоров	Аппаратные VPN	Карты платёжных систем	Интеграция на уровне SwiftNIO – набор API для разработчиков	Защита внутренней инфраструктуры
		Программируемые сетевые адаптеры	Специализированные смарт-карты (пропуска, аппаратные ключи и прочие смарт-карты)	Интеграция на уровне защиты всего трафика устройства	
		Маршрутизаторы (в том числе на уровне enterprise версий WiFi)			
		Прочее оборудование			

Рисунок 15. Возможности интеграции постквантовых алгоритмов в ИТ-инфраструктуру компании. Источник: QApp, 2023 г.

на основе квантовых ключей. Оно обеспечит защищённый обмен голосовыми и текстовыми сообщениями, а также файлами, а ещё будет поддерживать видеозвонки.

Ещё одно направление развития ViPNet QSS — поддержка квантовой криптографической сети произвольной топологии. Разработка соответствующих программно-аппаратных комплексов семейства ViPNet Quantum Trusted System (QTS) идёт в соответствии с рекомендациями российского комитета по стандартизации ТК26.

Центр компетенций НТИ по квантовым коммуникациям на базе МИСиС запустил в 2021 г. свой проект открытой квантовой сети, которая соединила два вуза: МИСиС и МТУСИ.

Совместное решение для поддержки на квантовой сети многоузлового сеанса квантово-защищённой видео-конференц-связи представили на Петербургском международном экономическом форуме в 2019 г. РКЦ и компания QRate. Квантовую зашифрованную связь протестировали руководители Сбербанка, «Газпромбанка» и другие участники финансового рынка. Эта сеть построена на базе серийной установки для квантовой криптографии компании QRate, которую можно интегрировать в существующую стандартную телекоммуникационную инфраструктуру и адаптировать для работы с криптографическими протоколами.

А ещё компания QRate провела успешный эксперимент с обеспечением квантовой защиты эталона атомного времени РФ (государственного первичного эталона единиц времени, частоты и национальной шкалы времени). В компании Qrate подчёркивают, что защита каналов синхронизации — это критически важный элемент для развития интернета вещей,

робототехники, телекоммуникаций, онлайн-всех финансовых инструментов и других задач.

ПРАКТИЧЕСКИЙ ОПЫТ РОССИЙСКОГО ПОСТКВАНТОВОГО ШИФРОВАНИЯ

Постквантовая криптография — это целое направление программных разработок, нацеленных на решение математических задач, которые необходимы для факторизации больших чисел. Отличительная особенность решений на основе постквантовой криптографии заключается в том, что они используют новый класс асимметричных алгоритмов шифрования, устойчивых к атакам с применением как классических, так и квантовых компьютеров.

Первый российский пилотный проект квантового шифрования осуществил в Москве «Газпромбанк» в 2016 г. В этом проекте, реализованном компанией QApp, по линии квантовой связи между двумя отделениями банка передавался только ключ для шифрования информации. Полноценное решение постквантового шифрования было внедрено той же командой через год в Сбербанке: между двумя офисами банка был создан канал связи с квантовой защитой длиной около 25 км, для организации связи использовалась городская инфраструктура.

В пилотном проекте, выполненном для «Газпромбанка» в феврале 2022 г., продукт QApp был интегрирован в ограниченный периметр системы host-to-host, повысив уровень её безопасности. Речь идёт о критически важных каналах коммуникаций, по которым банк обменивается транзакциями с корпоративными клиентами.

Компания QApp разрабатывает уникальные программные продукты на основе

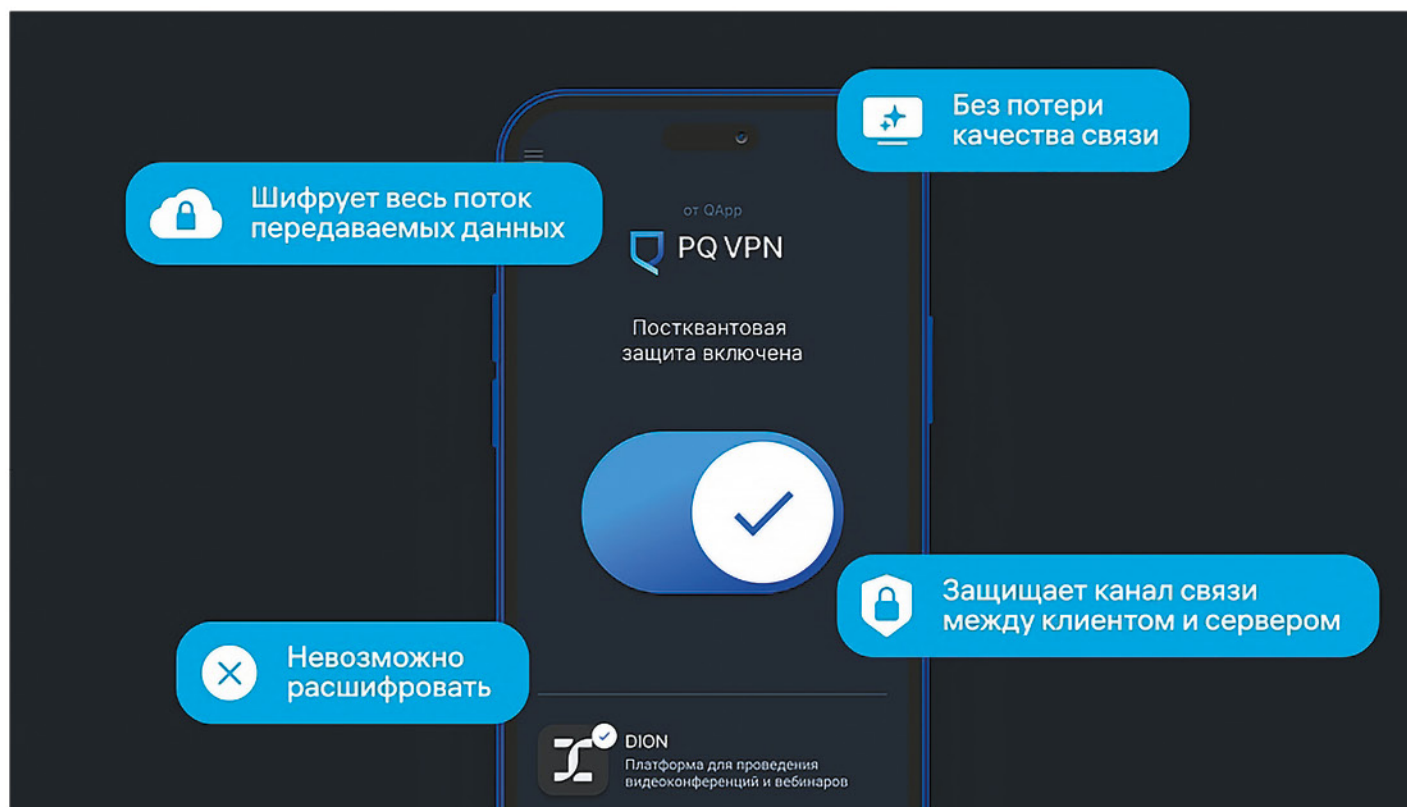


Рисунок 16. Схема ВКС с постквантовым шифрованием. Источник: TAdviser, февраль, 2023 г.

постквантовой криптографии. «Изюминка» подхода QApp к реализации постквантового шифрования заключается в способности решений интегрироваться в различные ИТ-системы и программно-аппаратные комплексы (рис. 15).

Например, квантово-устойчивые продукты QApp могут использоваться для комплексной защиты продуктов «Мой офис» на уровне приложения, операционной системы, рабочей станции, сети и информационной инфраструктуры в целом.

Учёные НИЯУ МИФИ предложили способ применения постквантовых криптографических алгоритмов для защиты обмена сообщениями в групповых чатах мессенджеров. А компания «Иннотех» из группы Т1 провела в феврале нынешнего года тестирование системы видеоконференц-связи Dion, в которой используется решение «Постквантовый VPN» компании QApp. По сообщению Т1, удалось обеспечить защищённый обмен данными участников конференции, находящихся на расстоянии 1800 км без использования дополнительного оборудования (рис. 16).

Ещё одно большое перспективное направление — финансовый блокчейн с квантовой защитой. Физики из Российского квантового центра ещё в 2017 г. впервые запустили блокчейн-систему, в основе которой лежит квантовое

распределение ключа. В этом случае транзакции подтверждаются в системе автоматически, а значит, отпадает необходимость в цифровой подписи. Фактически эту роль выполняет квантовый канал связи, где не допускается подслушивание ключа для шифрования и подделка сообщений, то есть все участники сети точно знают, кто является автором транзакции.

В ноябре 2022 г. этот подход решила применить российская блокчейн-платформа «Мастерчейн». Цель масштабного проекта, который будет реализовываться вместе с компанией QApp, — создание квантово-устойчивого блокчейна для российской финансовой отрасли.

Итак, вторая квантовая революция (первая случилась в XX веке на уровне микромира), которая кардинально переворачивает представления о надёжной криптографической защите корпоративных секретов, уже начала своё шествие по планете. В числе первых российских «революционеров» — крупнейшие банки и финансовые структуры, уже успевшие накопить опыт первых пилотных испытаний новых решений. Впереди трудоёмкий этап тиражирования апробированных продуктов и совместных испытаний новых систем.

(Полный текст читайте в электронной версии BIS Journal на сайте www.ib-bank.ru)



**Владимир
ЕЛИСЕЕВ**
руководитель
Цentra научных
исследований
и перспективных
разработок
компаний
«ИнфоТекС»

«КАК ПОКРЫТЬ ВСЮ СТРАНУ СЕТЬЮ РАВНОГО УРОВНЯ ДОВЕРИЯ?»

Разговор о квантовых эффектах всегда подразумевает философский элемент: абсолютная случайность, неопределённость в смысле Гейзенберга. Вспоминается также «мир идей» Платона: квантовый генератор случайных чисел, который генерирует абсолютно случайную последовательность, — это некая «идеальная вещь» в платоновской трактовке. В практической жизни на этот генератор можно воздействовать, чтобы ухудшить свойства этой последовательности. Например, он рассчитан на работу в конкретном диапазоне температур, а в иных температурных условиях генерируемые данные не будут «идеально случайными».

ОБ ИДЕАЛЬНОМ КВАНТОВОМ МИРЕ И РЕАЛЬНОЙ СТОЙКОСТИ КВАНТОВОЙ КРИПТОГРАФИИ

Те же соображения относятся и к системе квантового распределения ключей: к этой конкретной аппаратуре можно применить различные атаки. Например, если засветить детектор ярким светом фонарика, он будет постоянно выдавать «единички», идеального квантового механизма не получится. Можно мощным импульсом просветить Алису и по отражению от элементов системы Алисы понять, какие там использовались случайные числа. Эта ситуация известна как атака «тroyанский конь». А можно

ухудшить квантовые свойства системы за счёт того, что она выпускает информацию не одиночными фотонами, — тот самый «идеал» по Платону, а по несколько фотонов. Тогда эти фотоны можно будет расщеплять, часть отдавать Бобу, а часть забирать себе, то есть злоумышленнику. С этой целью придумана атака лазерного повреждения — повреждение мощным лазерным импульсом внутренних элементов формирователя квантовых состояний. При этом вся магия квантовой защищённости — абсолютная стойкость и секретность — тут же разваливается.

Таких довольно грубых способов атаки придумано немало. Соответственно, принято считать, что те системы, которые на нынешнем технологическом уровне защищены от всех известных на настоящий момент классических атак, довольно стойкие. Собственно, это и является главным содержанием испытаний в ходе сертификации квантовых решений в ФСБ.

В целом понятно, что на смену протоколу Диффи-Хеллмана должны прийти новые инструменты. Квантовое распределение ключей — одна из таких технологий. Ещё одна называется «постквантовая криптография». Это чистая математика, там совсем нет физики. А постквантовой она называется только потому, что математические алгоритмы, положенные в её основу, не ломаются алгоритмом Шора. Эти постквантовые алгоритмы имеют такое же обоснование стойкости, как и протокол Диффи-Хеллмана: математики пока не придумали, как их сломать. Но в любой момент может появиться некий Петров, который предложит квантовый алгоритм Петрова, способный сломать нынешние алгоритмы постквантовой криптографии. И тогда это будет, видимо, постпостквантовая криптография, также живущая в «мире идей».

А на уровне практической жизни критически важно, что дорожная карта тысячекубитных квантовых компьютеров IBM успешно

В целом понятно, что на смену протоколу Диффи-Хеллмана должны прийти новые инструменты. Квантовое распределение ключей — одна из таких технологий. Ещё одна называется «постквантовая криптография»

исполняется. Такая предсказуемость развития технологии не сулит ничего хорошего для развития асимметричной криптографии.

ВОПРОСЫ СТАНДАРТИЗАЦИИ КВАНТОВЫХ ТЕХНОЛОГИЙ ЗАЩИТЫ

Американский орган стандартизации NIST занимается стандартизацией квантовых алгоритмов с 2016 г. Интересно, что США сделали ставку на технологию постквантовых алгоритмов, и конкурс NIST был объявлен после периода довольно серьёзных исследований таких алгоритмов. С тех пор прошёл ряд промежуточных этапов конкурса NIST, однако финалисты так и не выявлены. Почему так получается? Пока там не сформировался консенсус относительно того, как объединить требования общепризнанной стойкости алгоритма (наличие широких исследований, позволяющих доверять этому алгоритму) и достаточной эффективности с точки зрения эксплуатации. Эти аспекты пока мешают стандартизовать постквантовые алгоритмы даже в США.

При этом Китай поставил на другую лошадь — квантовую криптографию. Уже лет пять идут исследования на большой квантовой сети в 4 тыс. погонных километров, созданной в Китае. Понятно, что Америка вряд ли останется без систем квантового распределения ключей — технологиями квантовой криптографии занимаются её союзники — Канада и Великобритания. В нашей стране в рамках технического комитета по стандартизации ТК26 также идёт изучение постквантовых алгоритмов, и есть наброски предварительной версии стандарта. Финалисты также пока не выбраны.

Наша страна развивает оба направления квантовых технологий. Причём квантовое распределение ключей (КРК), в котором специализируется компания «ИнфоТеКС», несколько опережает развитие постквантовых алгоритмов. Так, система квантового распределения ключей QSS, разработанная «ИнфоТеКС», — единственная система в России, которая прошла сертификацию в ФСБ. Она позволяет с помощью квантовых ключей защитить телефонную сеть, например, офисную АТС на 800 и более абонентов, гарантируя, что телефонные разговоры не будут перехвачены никем, включая системных администраторов. Обычно они имеют доступ ко всей криптографии в компании, а в случае QSS квантовые ключи меняются автоматически, без участия системного администратора, — ключи рождаются внутри коробочек с квантовыми эффектами, установленных у Алисы и Боба. Такая офисная телефонная связь

Наша страна развивает оба направления квантовых технологий. Причём квантовое распределение ключей (КРК), в котором специализируется компания «ИнфоТеКС», несколько опережает развитие постквантовых алгоритмов

некомпрометируема в принципе. Сейчас у нас в работе находятся другие системы QSS, ориентированные на защиту передачи данных, документов, возможно, видеосвязи.

«ИнфоТеКС» также принимает активное участие в процессах стандартизации технологий КРК. Так, в рамках ТК26 идёт стандартизация разработанного у нас интерфейса (рабочее название — ProtoQa) между системами квантового распределения ключей и обычными шифраторами. Ещё один стандарт, который подготовила компания «ИнфоТеКС», — IstoQ. Он описывает общие принципы распространения секретной информации по квантовой сети. Речь идёт о том, каким образом распространять секрет по сети с множеством узлов квантового шифрования. Это необходимо, во-первых, для того, чтобы сформулировать правильный и консенсусный подход к шифрованию подобного рода. И во-вторых, для того чтобы иметь возможность строить квантовые сети из оборудования разных производителей, достигая в том числе покрытия всей страны сетью равного уровня доверия.

ДАЛЬНЯЯ СВЯЗЬ С КВАНТОВОЙ ЗАЩИТОЙ

В системах квантового шифрования передача информации осуществляется квантовыми состояниями. Но для них существует ограничение по дальности квантового канала — 100 км. В классических системах телекоммуникаций электрический сигнал также затухает по мере распространения, но он передаётся на большие расстояния с помощью промежуточных узлов. Проблема в том, что квантовые состояния очень хрупкие, их нельзя усилить для передачи на большие расстояния, потому что квантовую информацию невозможно считать без ошибок. Таким образом, технология КРК даёт возможность исключить из схемы путешествие курьера с флешкой с секретными ключами на расстояние в 100 км. Но при этом в квантовом канале между Алисой и Бобом не должно

быть активного оборудования связи. Как преодолеть это «проклятие» ограниченного расстояния, если организациям нужны секретные ключи для связи между Москвой и Владивостоком?

Если для организации квантового канала использовать наземные оптоволоконные линии связи, то не реже, чем через 100 км, нужно ставить специальные пункты — некие промежуточные узлы, которые сопрягают два 100-километровых отрезка, то есть где заканчивается один квантовый сегмент и начинается другой. Информация, зашифрованная первым квантовым ключом, передаётся в этот промежуточный узел, расшифровывается, а затем зашифровывается вторым квантовым ключом и передаётся на следующий узел. Таким образом, можно взять классический секретный ключ, полученный из хорошего генератора случайных чисел, и шифровать его по всей этой цепочке промежуточных узлов на квантовых ключах. С точки зрения стойкости этого шифрования, передаваемый секретный ключ фактически такой же секретный, как и квантовые ключи.

Очевидно, что промежуточный узел должен быть очень высокого доверия. То есть злоумышленник ни в коем случае не должен оказаться внутри этого промежуточного узла. Поэтому концепцию построения таких сетей мы называем квантовой сетью с доверенными промежуточными узлами. В качестве площадки для развёртывания таких узлов могут использоваться различные помещения с высоким уровнем защищённости, например ЦОДы, защищённые пункты связи или банковские хранилища. Кстати, та протяжённая квантовая сеть в Китае также включает доверенные промежуточные узлы, они располагаются в отделениях одного из госбанков Китая.

КАКОЙ ПОДХОД ВЫБРАТЬ?

Я был бы рад сказать, что квантовое распределение ключей является серебряной пулей и всем надо переходить на квантовую криптографию. Но это не так: нельзя делать все ставки на одну технологию.

Квантовая криптография — это не информационная технология в чистом виде, она требует строительства физических каналов связи для передачи этого самого квантового состояния. Эти каналы могут иметь различную природу — передавать квантовую информацию по оптоволокну, через спутник или атмосферные каналы. Но в любом случае это некоторая инфраструктура. Она, кстати, является прекрасной основой для оказания услуг защищённой передачи ключей. Представим себе, что

некоторая крупная телекоммуникационная компания построила квантовую сеть с доверенными промежуточными узлами, сертифицированными регулятором, которые расположены во всех крупных городах России. Тогда пользователь может обратиться к ближайшему узлу этой сети, скажем, в Москве и передать свой секретный ключ своему контрагенту, например, во Владивостоке за небольшую плату. Этот секретный ключ будет передан под защитой квантовых ключей, а сама телекоммуникационная компания не будет иметь доступа к передаваемой информации. Да, флешка пользователя будет подключаться к конкретному оборудованию этой компании, но сертификация этого оборудования подразумевает, что на стороне оператора строго выполнены все необходимые меры защиты.

Тогда банку, имеющему отделения в разных городах страны, для обеспечения защищённой связи надо будет приобрести шифраторы, совместимые с квантовой сетью, и подключить их к узлам квантовой сети. А дальше только оплачивать услугу регулярной выдачи новых секретных ключей — «Передача секретов как услуга».

Но что делать с мобильными устройствами пользователей в эпоху усиливающейся корпоративной мобильности? Думается, что это тот самый сегмент, в котором найдут применение постквантовые алгоритмы. В этом случае требования абсолютной секретности не такие жёсткие, как в магистральной сети квантового шифрования, и алгоритмические подходы вполне применимы. Единственное ограничение, на которое можно указать сегодня, — это большая ресурсоёмкость постквантовых алгоритмов, которые требуют много вычислений. То есть защищённая связь для смартфона на основе постквантовых алгоритмов будет гораздо быстрее истощать аккумулятор смартфона, чем те алгоритмы, которые используются сейчас.

Но, полагаю, это временные трудности. Появятся более производительные смартфоны, а специалисты в конце концов выберут наиболее эффективный постквантовый алгоритм и оформят его в виде стандарта.

Так что, скорее всего, в недалеком будущем мы увидим на технологическом уровне некий конгломерат из квантового распределения ключей и постквантовых алгоритмов. А на бизнес-уровне — конкурирующие услуги квантово-защищённых коммуникаций, предлагаемых доверенными поставщиками.

«К КОНЦУ 2023 Г. ИССЛЕДОВАТЕЛЬСКИЕ ПРОЕКТЫ В ОБЛАСТИ КВАНТОВОЙ ЗАЩИТЫ ИНФОРМАЦИИ МОГУТ ПЕРЕЙТИ В БОЛЕЕ ЗРЕЛУЮ ФАЗУ КОММЕРЧЕСКИХ ПРОТОТИПОВ»

Появление и сравнительно быстрое развитие областей знаний под названиями «квантовая» и «постквантовая» криптография свидетельствуют о серьёзном отношении государства и бизнеса к проблеме «квантовой угрозы» и соответствующему повышению криптостойкости всех известных криптопримитивов (криптографических хеш-функций, электронных подписей, асимметричных и симметричных алгоритмов шифрования), получивших широкое распространение в ключевых цифровых экосистемах и платформах цифровой экономики РФ.

С одной стороны, достижения в области квантовой информатики (Quantum Information Science, QIS) наглядно показали высокий технологический потенциал квантовых технологий для стимулирования инноваций в национальных экономиках мира. С другой стороны, стало понятно, что в ближайшие 5–10 лет квантовые компьютеры достигнут достаточной зрелости и окажутся способны к взлому большей части криптографических примитивов.

КВАНТОВЫЕ УГРОЗЫ БЕЗОПАСНОСТИ

На квантовом компьютере можно реализовать с полиномиальной сложностью алгоритмы факторизации и дискретного логарифмирования в произвольной группе (метод Шора), что в перспективе может привести к компрометации всех асимметричных криптографических схем, стойкость которых обосновывается предположением о сложности решения указанных задач, в том числе схем RSA, Диффи — Хеллмана и электронных подписей ECDSA и ГОСТ 34.10–2018. При этом результативность криптоанализа симметричных криптосхем менее значима, поскольку известные в настоящее время квантовые алгоритмы анализа хеш-функций и блочных шифров (метод Амбайниса для поиска коллизий и метод Гровера для поиска прообраза) по-прежнему имеют экспоненциальную сложность, хотя и меньшую, чем классические.

Более того, ряд известных экспертов в области кибербезопасности ещё более категоричны. Так, по заявлению директора АНБ США Пола М. Накасоне, «криптоаналитически значимый квантовый компьютер может поставить под угрозу системы гражданской и военной связи и подорвать боеспособность стратегических систем контроля и управления критической информационной инфраструктуры США и их союзников по НАТО. Для нейтрализации этой квантовой угрозы требуется создать и внедрить на практике квантово устойчивые алгоритмы, в первую очередь постквантовые схемы асимметричного шифрования (Public-Key Encryption) и электронной подписи (Digital Signatures)».

Так, в мае 2022 г. администрация Президента США Джо Байдена выпустила две новые директивы о подготовке государства и бизнеса к будущим квантовым кибератакам (quantum.gov; whitehouse.gov/briefing-room/statements-releases/2022/05/04/fact-sheet-president-biden-announces-two-presidential-directives-advancing-quantum-technologies). А в отчёте аналитической компании PreScouter, опубликованном в 2022 г., хоть и отмечено, что у злоумышленников сегодня вряд ли есть ресурсы для разработки атакующих систем на основе квантовых компьютеров, подчёркивается, что появление и широкое распространение облачных квантовых вычислений общего назначения (IaaS, PaaS) позволит сделать квантовые атаки доступными для широкого круга пользователей.

Поэтому в начале 2022 г. администрация Джо Байдена поручила NIST, АНБ и Агентству по кибербезопасности и защите инфраструктуры (Cybersecurity and Infrastructure Security Agency, CISA) в срок от 90 дней до 1 года выполнить все необходимые мероприятия по защите критической инфраструктуры США и их союзников по НАТО.

На примере алгоритмов — финалистов конкурса NIST можно видеть, как современные концепции синтеза схем постквантовой криптографии нашли применение в конкретных примерах и решениях, в том числе для создания



Сергей ПЕТРЕНКО
руководитель
направления ИБ
«Академии АйТи»

квантово устойчивых блокчейн-экосистем и платформ. Так, задачи теории решёток лежат в основе алгоритмов — финалистов конкурса NIST (CRYSTALS-Kyber, NTRU, SABER, CRYSTALS-Dilithium и FALCON), а также альтернативных алгоритмов-финалистов FrodoKEM и NTRU Prime. Задачи теории кодирования обеспечивают стойкость таких алгоритмов — финалистов конкурса NIST, как Classic McEliece, и альтернативных алгоритмов — финалистов BIKE, HQC. На основе многочленов от многих переменных строится решение финалистов конкурса NIST Rainbow и альтернативный алгоритм-финалист GeMSS. Большое внимание уделяется криптографическим алгоритмам на основе хеш-функций, в частности, финалистом конкурса NIST стал XMSS, а альтернативным является алгоритм-финалист SPHINCS+.

Таким образом, в современных условиях актуальность создания отечественных криптосистем «квантового» и «постквантового» шифрования подтверждается следующим.

- ◆ Нарастание рядом зарубежных стран потенциала возможностей квантовых технологий для проведения информационно-технических воздействий на КИИ Российской Федерации в военно-политических целях. Одновременно с этим усиление деятельности иностранных технических разведок, использующих возможности квантового криптоанализа асимметричных и симметричных схем шифрования на основе квантовых алгоритмов Шора, Гровера и других для проведения технической разведки в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса.

- ◆ Стремление отдельных государств использовать технологическое превосходство в квантовых технологиях для доминирования в информационном пространстве. Применение квантовых технологий в военно-политических целях, в том числе для осуществления действий, противоречащих международному праву, направленных на подрыв суверенитета, политической и социальной стабильности, территориальной целостности Российской Федерации и её союзников и представляющих угрозу международному миру, глобальной и региональной безопасности.

- ◆ Рост квантовых криптоатак на объекты КИИ, усиление разведывательной деятельности иностранных государств в отношении Российской Федерации, а также нарастание угроз применения квантовых технологий для нанесения ущерба суверенитету, территориальной целостности, политической и социальной стабильности Российской Федерации.

- ◆ Рост числа криптоатак на блокчейн-экосистемы и платформы Цифровой экономики Российской Федерации, использующих криптографические алгоритмы для создания пары «открытый — закрытый ключ» и адреса, получаемого с использованием операций хеширования и контрольной суммы открытого ключа. Если раскрытие одного адреса не является большим риском, то раскрытие адреса и открытого ключа, применяемого при транзакции, несёт потенциальную опасность, поскольку в случае достижения достаточного прогресса в области квантовых вычислений это даст возможность получить закрытый ключ.

ПРОТИВОСТОЯНИЕ «ЩИТА И МЕЧА» В КВАНТОВЫХ РЕШЕНИЯХ

В начале марта стало известно, что учёные из Королевского института КТН в Швеции обнаружили уязвимость в квантово безопасном алгоритме CRYSTALS-Kyber — одном из тех, которые NIST выбрал в качестве стандарта для будущих криптографических систем. Да, 100% безопасности не бывает, всегда существуют остаточные риски, которыми нужно научиться управлять (принимать или уклоняться, снижать или передавать на сторону). Обнаружение уязвимости в постквантовой криптосхеме CRYSTALS-Kyber — тому наглядное подтверждение.

Сегодня не только в США и ЕС, но и в России активно проводятся поисковые исследования, направленные на получение ряда прорывных научных и практических результатов:

- ◆ квантовые ускорения для предлагаемых улучшений комбинаторных атак на постквантовые криптосистемы на решётках, например для ряда известных систем блокчейн: «Мастерчейн 2.0» (финансово-кредитные организации), Enterprise Ethereum Alliance («Эфириум 2.0»), Waves Enterprise (Waves, Vostok), Hyperledger Fabric (Linux, IBM), Corda Enterprise, Bitfury Exonum, Blockchain Industrial Alliance, Exonum (Bitfury CIS), NodesPlus (b41), Microsoft Azure Blockchain и др.;

- ◆ оценки теоретической и практической стойкости известных постквантовых криптосистем на решётках, например, для упомянутых блокчейн-систем;

- ◆ примеры возможных открытых квантовых атак на постквантовые криптосистемы на основе решёток и др.

Здесь ключевой особенностью уязвимости современных криптопримитивов является необходимость экспоненциально повышать параметры протоколов каждые n лет в ответ на

Вид списка	Уровень зашиф.	NTRU		SABER		CRYSTALS-Kyber	
		Кубиты	Глубина	Кубиты	Глубина	Кубиты	Глубина
Квантовый	1	$2^{227,48}$	$2^{340,19}$	$2^{228,95}$	$2^{343,36}$	$2^{228,85}$	$2^{343,36}$
	3	$2^{298,45}$	$2^{452,72}$	$2^{337,06}$	$2^{512,95}$	$2^{336,96}$	$2^{512,95}$
	5	$2^{359,31}$	$2^{547,82}$	$2^{444,99}$	$2^{684,12}$	$2^{444,89}$	$2^{684,12}$
Классический	1	$2^{19,4}$	$2^{219,91}$	$2^{19,77}$	$2^{221,91}$	$2^{19,6}$	$2^{221,91}$
	3	$2^{19,81}$	2^{291}	$2^{20,36}$	2^{329}	$2^{20,18}$	2^{329}
	5	$2^{20,28}$	2^{351}	$2^{20,77}$	2^{437}	$2^{20,6}$	2^{437}

Рисунок 1. Реализация квантовых оракулов. Источник: Квантово-устойчивый блокчейн: Как обеспечить безопасность блокчейн-экосистем и платформ в условиях атак с использованием квантового компьютера (научно-популярная монография). Алексей Петренко. ISBN978–5–4461–2357–5. Издательский дом «Питер», 2023

растущую квантовую мощность передовых квантовых компьютеров. Частично эта проблема была решена в отобранных NIST алгоритмах, использующих решётки. Однако данные протоколы, в частности NTRU, оказались уязвимы к атакам с использованием квантового компьютера иного рода. Таким образом, используя алгоритм Гровера, были получены результаты количества кубит и глубины схемы, достаточные для реализации квантовых оракулов (модели генерации псевдослучайных чисел) с различными видами списка при атаке на постквантовые криптосистемы (рис. 1).

В таблице приведены количество кубит и глубина схемы, достаточные для реализации квантовых оракулов с различными видами списка при атаке на постквантовые криптосистемы. Здесь NTRU, SABER и CRYSTALS-Kyber — постквантовые криптосистемы на основе решёток, которые прошли в финальный раунд конкурса NIST.

Как видно из таблицы, экспоненциальная длина списка L накладывает ограничения на возможность реализации гибридных атак на полноразмерные постквантовые криптосистемы. Однако стоит заметить, что для атак на NTRU используются циклические решётки, исследование которых может помочь уменьшить длину списка L , что приведёт к меньшим верхним оценкам сложности в части реализации квантового оракула.

Замечу, что проблема нахождения SVP может быть разрешена с определёнными параметрами с помощью алгоритма Гровера. Она также является одной из важнейших проблем, лежащих в основе постквантовой криптографии, реализованной на решётках. С помощью уже известных алгоритмов криптоанализа и модификаций для использования алгоритма Гровера можно получить весомое квантовое ускорение в решении данной задачи.

КАК РАЗВИВАЕТСЯ СИТУАЦИЯ У НАС?

Для своевременного предупреждения вышеназванных угроз безопасности в 2019 г. в России утвердили «Дорожную карту по развитию квантовых технологий», рассчитанную до 2024 г. В качестве её основной цели заявлено достижение в среднесрочной и долгосрочной перспективе практически значимых научно-технических и практических результатов мирового уровня в области квантовых технологий, в том числе «квантовой» и «постквантовой» криптографии.

В середине 2022 года отечественная компания «Криптонит» (<https://kryptonite.ru>) предоставила Техническому комитету по стандартизации «Криптографическая защита информации» (ТК26) Росстандарта пакет документов по постквантовой электронной подписи (ЭП) «Шиповник». Стойкость этой криптосхемы базируется на задаче декодирования случайного линейного кода, которая является вычислительно сложной. В основу упомянутой криптосхемы легли коды, исправляющие ошибки, математические свойства которых хорошо изучены. В пакет документов вошло описание криптосхемы электронной подписи (ЭП) «Шиповник», теоретическое обоснование её стойкости, обоснование выбора параметров, а также модельная реализация.

Рабочая группа РГ 2.5 «Постквантовые криптографические механизмы» технического комитета ТК26 «Криптографическая защита информации» также проводит работу по стандартизации отечественного алгоритма «Форзизия», основанного на изогениях суперсингулярных эллиптических кривых и соответствующих вычислительно сложных задачах.

В настоящее время, по моему мнению, рыночная популярность систем квантового и постквантового шифрования для обеспечения надлежащей защиты объектов критической информационной инфраструктуры РФ достаточно

высока. К концу 2023 г. исследовательские проекты, развиваемые сегодня различными российскими научными школами совместно с ведущими отечественными производителями средств криптографической защиты информации, могут выйти из состояния единичных уникальных пилотов и перейти в более зрелую фазу так называемых коммерческих и промышленных прототипов новых уникальных средств и систем криптографической защиты информации.

Так, система квантового распределения ключей ViPNet QSS компании «ИнфоТеКс», которая имеет сертификат ФСБ России, открыла новые возможности для внедрения комплексов квантово-криптографической связи на инфраструктуре ведущих российских предприятий. Например, так называемые квантовые телефоны как раз построены на системе квантового распределения ключей ViPNet QSS. Это значит, устройство работает в качестве IP-телефона, подключённого к клиенту квантового распределения ключей и серверу. За счёт протокола квантового шифрования трафик шифруется таким образом, что к нему нельзя получить доступ со стороны.

Инновационная российская компания QArp вывела на отечественный рынок ряд уникальных решений «квантовой» и «постквантовой» криптографии:

- ◆ PQLR SDK — интегрированная с OpenSSL библиотека квантово устойчивых алгоритмов;
- ◆ Qtunnel — квантово устойчивое соединение в незащищённой сети;
- ◆ PQStor — end-to-end-шифрование файлов и папок;
- ◆ TAF — фреймворк для детектирования атак по времени.

А совместное решение университета «Иннополис» и «Академии АйТи» представляет собой исследовательский проект и одноимённую программную платформу «Квант-К», которая предназначена для проведения квантового криптоанализа большинства известных криптопримитивов блокчейн. Результаты упомянутого криптоанализа позволяют существенно улучшать теоретическую и практическую криптостойкость исследуемых криптопримитивов.

Для оценивания квантовой устойчивости известных блокчейн-платформ был впервые предложен и обоснован новый вид квантового криптоанализа схем асимметричного шифрования (RSA, Эль-Гамала) и цифровой подписи (DSA, ECDSA или RSA-PSS) на основе модифицированного авторами алгоритма факторизации Шора. При этом доля квантовых алгоритмов криптоанализа в арсенале инструментальных

средств криптоанализа схем асимметричного шифрования (RSA, Эль-Гамала) и электронной подписи (DSA, ECDSA или RSA-PSS) была увеличена до 17%, а оперативность исследования криптостойкости схем асимметричного шифрования (RSA, Эль-Гамала) и цифровой подписи (DSA, ECDSA или RSA-PSS) изученных блокчейн-платформ была повышена на 20–30% за счёт автоматизации первой и второй части модифицированного (квантового) алгоритма факторизации Шора в гибридной среде IBM Q (16, 20, 100 и 1000 кубитов) и на суперЭВМ пятого поколения.

В состав «Квант-К» вошли следующие программные модули:

- ◆ первичного анализа криптосистемы, предназначенного для определения криптографического шифра и сведения задачи вскрытия к задаче факторизации;
 - ◆ поиска периода неопределённой функции, предназначенной для реализации факторизации на квантовой вычислительной системе;
 - ◆ расчёта секретного ключа (предназначен для обработки полученного в результате функционирования предыдущего модуля итога факторизации для последующего вскрытия криптосистемы);
 - ◆ представления результатов и их анализа (предназначен для отображения полученного итога и анализа характеристик его получения).
- В ходе дальнейшего развития платформы «Квант-К» предполагается добавление в библиотеку платформы других квантовых и постквантовых алгоритмов: Гровера, Саймона, Экера, Берштейна — Вазираниа, Харроу, Хассилима, Ллойда и др.

Заметной конкуренции между российскими разработчиками, работающими над созданием систем квантового шифрования, пока не наблюдается: рынок только формируется, большинство проектов находятся на этапе стартапов. По этой причине место на рынке найдётся всем игрокам. При этом возникает интересный практический вопрос, лежащий в плоскости системной интеграции, — плавный переход от традиционных коммуникаций к квантовой защите.

Полагаю, что квантовая модель вычислений ещё недостаточно зрелая. Иными словами, отказаться от классической архитектуры фон Неймана и полностью перейти на квантовую модель вычислений сегодня не получится. Экосистема квантовых технологий только формируется. Поэтому, скорее всего, ожидается вкрапление Q-технологий в существующую инфраструктуру для решения узких и специфичных задач.

При этом на системном уровне следует отметить недостаточный уровень развития конкурентоспособных отечественных квантовых технологий и их использования для производства продукции и оказания услуг. Это объясняется, в частности, высокой степенью зависимости отечественной промышленности от зарубежных информационных технологий в части, касающейся электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи. Такая ситуация, в свою очередь, обуславливает зависимость социально-экономического развития Российской Федерации от геополитических интересов зарубежных стран и, как следствие,

недостаточную эффективность научных исследований в области квантовых технологий, направленных на создание перспективных квантовых компьютеров. По всей видимости, в 2023 году потребуются существенно скорректировать национальную программу развития квантовых технологий, в том числе принять ряд новых отечественных стандартов квантового и постквантового шифрования. И такая работа уже начата. Например, на конференции «РУСКРИПТО'2023», которая прошла 21–24 марта, целая секция была посвящена актуальным вопросам стандартизации перспективных отечественных криптосхем квантовой и постквантовой криптографии.

«ТЕХНОЛОГИЯ КВАНТОВОГО ШИФРОВАНИЯ НАХОДИТСЯ В САМОЙ НАЧАЛЬНОЙ СТАДИИ СВОЕГО РАЗВИТИЯ»

На восприятие рынком технологий квантового шифрования влияет несколько факторов. Во-первых, угроза квантового взлома алгоритмов асимметричного шифрования пока воспринимается как некая абстракция, хотя уязвимость асимметричных алгоритмов шифрования перед квантовыми вычислителями была продемонстрирована на практике уже более 20 лет назад. Во многом такое отношение вызвано отсутствием практически применимых квантовых вычислителей. Но здесь важно заметить, что увеличение числа кубитов, которое ежегодно демонстрируют исследовательские группы, например IBM, отражает не только рост вычислительных возможностей, но и серьёзный прогресс в решении инженерных задач, связанных с реализацией квантового компьютера как физического устройства, пригодного к эксплуатации. Именно от решения этих задач напрямую зависит, насколько быстро квантовые компьютеры «пойдут в массы», а значит, смогут быть использованы и для взлома ключей тоже.

Во-вторых, сама технология квантового шифрования находится в самой начальной стадии своего развития. Самые «старые» игроки на рынке квантовой криптографии, поставляющие решения квантового распределения ключей для оптоволоконных сетей, существуют около 20 лет, но их производственная и коммерческая история куда меньше.

Спутниковые системы квантового распределения ключей (КРК), разработкой которых занимается наша компания, только-только подходят к стадии прототипов. Другими словами, если следовать логике кривой диффузии инноваций, сейчас квантовой криптографией интересуются клиенты-инноваторы. Ещё не набрана достаточная положительная история, чтобы убедить большинство потенциальных заказчиков в состоятельности технологии. Однако полагаю, что в ближайшие годы возможен рост пилотных проектов и промышленных внедрений систем квантового шифрования. Об этом говорит пусть умеренный, но всё же растущий интерес к разработкам в этой области со стороны венчурных фондов, государственных структур, а также крупных технологических игроков рынка связи, финансового сектора.

Нельзя также забывать, что для широкого внедрения какой-либо новой технологии требуется время с целью решения чисто технических задач — на отладку взаимодействия с существующей информационной инфраструктурой, стандартизацию алгоритмов и процессов, разработку и отработку компонентов. В частности, по мере подтверждения интереса от рынка у производителей появятся дополнительные стимулы для активизации разработки специализированной компонентной базы, её адаптации к серийному производству. Это в конечном счёте может привести к уменьшению стоимости устройств, потенциально улучшить технические характеристики.



Дмитрий ПЛОХОВ
менеджер
проектов QSpace
Technologies



Василий ПИСКАРЕВ
председатель Комитета
Государственной Думы
по безопасности
и противодействию коррупции

«У ХАКЕРОВ, ПРИЧИНИВШИХ УЩЕРБ ГРАЖДАНАМ И БАНКАМ, НЕОБХОДИМО ИЗЫМАТЬ ДЕНЬГИ И ЦЕННОСТИ, ПОЛУЧЕННЫЕ ПРЕСТУПНЫМ ПУТЁМ»

Доступ к компьютерной информации всё чаще становится не способом получения новых знаний, а средством обогащения и даже военных действий в киберпространстве. А это значит, что мы должны обеспечить надёжную защиту государственных секретов, банковских данных и личной информации граждан. В последнее время Государственная Дума сделала ряд важных шагов в части пресечения преступных действий в сфере компьютерной информации, обеспечения безопасности данных о госрегистрации недвижимости, а также для объединения усилий стран ОДКБ с целью создать общую систему защиты критической информационной инфраструктуры.

ЗАСТАВИТЬ ХАКЕРОВ ВЕРНУТЬ НАГРАБЛЕННОЕ

Статистика Министерства внутренних дел РФ показывает: в настоящее время в нашей стране каждое четвёртое преступление совершается с использованием информационно-коммуникационных технологий или в сфере компьютерной информации. При этом большинство таких преступлений совершено с использованием сети Интернет, средств мобильной связи, компьютерной техники и программных средств.

По данным МВД России, в 2022 году совершено 12 006 преступлений в сфере компьютерной информации, что почти на 44% больше, чем за аналогичный период прошлого года (в 2021 году — 8 360), из них:

- ♦ неправомерный доступ к компьютерной информации — 10 891 (в 2021 году — 7 530);
- ♦ создание, использование и распространение вредоносных компьютерных программ — 518 (в 2021 году — 656);
- ♦ нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей — 1 (в 2021 году — 1);
- ♦ неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации — 596 (в 2021 году — 173).

Чтобы повысить эффективность противодействий такой преступной деятельности, вместе с коллегами мы внесли в Государственную думу проект поправок в Уголовный кодекс РФ, которыми вводится конфискация имущества, полученного в результате совершения преступлений в сфере компьютерной информации. Для этого предлагаем внести в пункт «а» части 1 статьи 1041 Уголовного кодекса Российской Федерации изменения, дополнив его статьями 272–274.2.

Ни для кого не секрет, что ущерб, нанесённый гражданам и банковскому сектору в результате компьютерных преступлений, исчисляется многими миллионами рублей. Конфискация денег, ценностей и иного имущества преступников не только станет справедливым наказанием за такого рода преступления, но и поможет восстановить справедливость — направить эти средства на возмещение ущерба потерпевшим гражданам.

23 января законопроект принят в первом чтении. Работа над ним продолжается.

ДАнные О НЕДВИЖИМОСТИ ЗАЩИТИМ ОТ ХАКЕРОВ

Также в этом году Госдума поддержала в первом чтении ещё одну нашу законодательную инициативу, которой предложены дополнительные меры для обеспечения безопасности критической информационной инфраструктуры в сфере госрегистрации недвижимости.

Речь идёт о том, чтобы защитить от хакерских атак и хищения регистрационные данные. Предложенные нами поправки позволят распространить на эту сферу комплекс мероприятий, которые применяются государством для защиты критической информационной инфраструктуры РФ.

Развитие современных технологий, которые быстро осваивают сетевые пираты, требует и совершенствования мер защиты критически важных данных. Этому и посвящён наш законопроект. Можно только предполагать, к каким последствиям приведут попытки хакеров взломать базы данных и, например, изменить данные о собственниках недвижимого



имущества или просто похитить этих сведения в мошеннических целях.

В данном случае, на наш взгляд, не нужно изобретать велосипед. Вступивший в силу 5 лет назад Федеральный закон «О безопасности критической информационной инфраструктуры» позволил построить надёжную систему защиты данных и доказал свою эффективность при проведении выборов, когда на серверы ЦИК Российской Федерации велись непрерывные хакерские атаки, но сорвать голосование злоумышленникам не удалось. Целесообразно распространить эту систему государственной защиты и на другие данные, которые имеют важнейшее значение для наших граждан. В данном случае — на данные о недвижимости.

ОБЪЕДИНИТЬ УСИЛИЯ СТРАН ОДКБ В ПРОТИВОДЕЙСТВИИ КИБЕРПРЕСТУПЛЕНИЯМ

29 марта на заседании Постоянной комиссии Парламентской Ассамблеи ОДКБ по обороне и безопасности обсуждался ряд вопросов, связанных с гармонизацией законодательства.

В центре внимания был, в частности, модельный законопроект «О защите информации и кибербезопасности», разработанный по предложению Белоруссии. В него включены нормы, которые позволят выстроить защиту от хакерских атак на государственные органы и компании, на информационные ресурсы.

Мы видим, как против стран ОДКБ ведётся необъявленная кибервойна — на это указывают массированные вбросы фейков в соцсетях, атаки на сайты государственных органов и критически важных объектов, массовое лженирование социальных объектов. Сегодня в этой сфере возникает всё больше новых угроз, и для нас важно задействовать опыт и возможности стран, которые входят в ОДКБ, чтобы выработать совместимый понятийный аппарат, создать общую систему защиты критической информационной инфраструктуры.

Разработка модельных законодательных актов — важное направление деятельности Парламентской ассамблеи ОДКБ. Эти законы не являются обязательными для стран-участниц, но служат примером для создания национальных законов и таким образом позволяют сблизить законодательство наших стран.



Заседание Комитета Государственной Думы по безопасности и противодействию коррупции с участием министра МЧС России Александра Куренкова

СИЛОВИКИ СМОГУТ ПРЕСЕКАТЬ ПЕРЕДВИЖЕНИЕ БЕСПИЛОТНИКОВ В ВОЗДУХЕ, НА ЗЕМЛЕ И НА ВОДЕ

Ещё одна важная инициатива последних дней — разработанный мною с коллегами по Комитету по безопасности и противодействию коррупции законопроект «О внесении изменений в отдельные законодательные акты Российской Федерации», в соответствии с которым силовым ведомствам предоставляется право останавливать движение любых беспилотных аппаратов в зоне своей ответственности.

Законопроект затрагивает передвижения робототехнических комплексов, включая беспилотные воздушные, подводные, надводные суда и наземные аппараты, — иными словами, все существующие виды беспилотников.

Напомню, в 2019 году мы разработали и приняли закон, который позволяет пресекать представляющие угрозу полёты беспилотных летательных аппаратов над объектами критической инфраструктуры, важными государственными объектами и в местах массового скопления людей. И закон показал свою эффективность.

Однако техника развивается, появились другие виды беспилотных аппаратов, которые действуют не только в воздухе. Анализ современной ситуации, в том числе международный опыт, свидетельствует об активном использовании наземных и морских (надводных, подводных) беспилотных аппаратов в террористических и военных целях. Случаи их

противоправного применения уже зафиксированы и на территории Российской Федерации, что обусловлено диверсионно-террористическими устремлениями властей Украины.

По имеющимся данным, с начала специальной военной операции только в зоне её проведения подразделениями Росгвардии было обнаружено 2585 БПЛА, и посредством подавления сигналов дистанционного управления пресечено перемещение значительной их части.

При этом, по данным Росгвардии, при охране Запорожской и Курской АЭС ежедневно фиксируется и подавляется от 5 до 9 сигналов дистанционного управления БПЛА. И на новые угрозы необходимо реагировать.

В этой связи законопроектом предлагается расширить существующие полномочия Росгвардии, МВД, ФСБ, ФСО, СВР, ФСИН России, а также Главного управления специальных программ и ведомственной охраны по пресечению использования всех видов беспилотных аппаратов на земле, в воздухе и на воде. Такое пресечение будет осуществляться, в том числе посредством их уничтожения или повреждения, а также подавления или преобразования сигналов дистанционного управления.

Принятие закона обеспечит уполномоченные органы, а также организации ведомственной охраны правовыми основаниями для противодействия террористическим, диверсионным и иным преступным посягательствам. Наши граждане и объекты критической инфраструктуры должны быть под надёжной защитой.



Оксана ДЯЧЕНКО
обозреватель BIS Journal

ПОДРОБНЕЕ, ПОЖАЛУЙСТА!

НОВЫЕ ТРЕБОВАНИЯ ЦБ ВСТУПАЮТ В СИЛУ С 1 ОКТЯБРЯ

Банк России обязал кредитные организации с 1 октября 2023 года передавать в ФинЦЕРТ развёрнутую информацию о подозрительных транзакциях, чтобы регулятор получал сведения обо всех участниках мошеннических переводов, а не только о конечном получателе, как это происходит сейчас.

С октября текущего года в АСОИ ФинЦЕРТ будет стекаться подробная информация о подозрительных транзакциях. Например, сведения о гаджете, с которого совершена операция, номер SIM-карты, геолокация человека, который проводит операцию, и т.д.

«Новая редакция правил, которые впервые появились в 2018 году, подготовлена с учётом актуальных приёмов кибермошенников, формы запросов адаптированы под предстоящий информационный обмен между Банком России и МВД России по фактам хищений денежных средств при переводах. За счёт увеличения состава и повышения качества поступающих в нашу автоматизированную систему сведений банки смогут лучше бороться с мошенническими переводами», — отметил директор Департамента информационной безопасности Банка России Вадим Уваров.

Мы попросили экспертов оценить, в какой степени такие меры повысят уровень информационной безопасности и каковы будут последствия введения таких мер для банков.

«СЕРВИСЫ БОЛЬШИНСТВА БАНКОВ НЕ ГОТОВЫ К ДОПОЛНИТЕЛЬНОЙ НАГРУЗКЕ»

Концепция данной инициативы хорошая, она обязет аккумулировать и обращать внимание на данные об атаках более чем по 50 признакам, отмечает генеральный директор ITGLOBAL.COM Security Александр Зубриков. Так, под подозрение попадают, например, случаи одновременной работы интернет-банкинга в разных географических местах, оформление предодобренного кредита сразу после снятия блокировки онлайн-банкинга из-за неверного ввода логина, пароля или номера телефона.

«Это не только поможет пресекать мошеннические и подозрительные операции, но и будет полезно органам внутренних дел в расследовании финансовых преступлений. Однако могут возникнуть сложности — неясно, все ли банки успеют за полгода подготовиться и модифицировать архитектуру и бизнес-процессы должным образом. Также есть большая вероятность, что банки не будут в полной мере исполнять эти требования, так как государством не устанавливается ответственность или вообще какие-то санкции при неисполнении», — считает эксперт.

По его словам, главное последствие этой инициативы — дополнительная нагрузка на банки, которым придётся в кратчайшие сроки закупать новые или расширять и перенастраивать текущие системы, сервисы и СЗИ. Сервисы большинства банков были не готовы собирать и анализировать такие объёмы данных, подчёркивает он. Также могут потребоваться дополнительные вложения в кадровом направлении. Может оказаться так, что придётся в кратчайшие сроки нанимать новых специалистов или обучать текущих под новые реалии и новые требования.

«Судя по опыту, многие банки постараются отсрочить выполнения данных мер, по крайней мере, пока за их невыполнение не будет контроля и административной ответственности — это поможет выиграть время и подготовиться более качественно», — добавляет Зубриков.

«ДЛЯ ИНДУСТРИИ ПОЛЕЗНО, НО ОТДЕЛЬНО ВЗЯТОМУ ЧЕЛОВЕКУ ВРЯД ЛИ ПОМОЖЕТ»

В теории введённые меры могут повысить общий уровень безопасности в том смысле, что несколько проще станет выявлять мошеннические схемы и оперативно на них реагировать, считает руководитель группы защиты инфраструктуры ИТ компании «Газинформсервис» Сергей Полунин.

«Отдельно взятому обманутому человеку это не особо поможет, но потенциально со временем потребует от злоумышленников как-то менять свои мошеннические схемы,



подстраиваться под новые условия, а это может вызвать определённые сложности у аферистов. Кроме этого, конечно, всей индустрии будет очень полезно, если финансовые учреждения не будут замалчивать проблемы в сфере информационной безопасности. Борьба с хакерами, особенно в сфере финансов, — это общее дело, в этом смысле мы в одной лодке», — высказывает своё мнение эксперт.

При этом нагрузка на информационные системы банков возрастёт чисто технически — каждое событие или каждый инцидент должен теперь будут дополняться всеми этими сведениями о геолокации или данными сим-карты. Это очень небольшой объём данных, но, учитывая количество событий в целом, объёмы хранения могут заметно возрасти, отмечает Полунин. Ведь, кроме того, чтобы сгенерировать инцидент, его нужно как-то корректно хранить и передавать.

«Кроме того, чтобы эти данные попали в инцидент, сведения нужно начать собирать, в том числе от пользователей. Это вполне решаемая инженерная задача, которая просто потребует доработки информационных систем банков и, например, клиентских приложений», — добавляет эксперт.

«СЛИШКОМ МАЛО ВРЕМЕНИ, ЧТОБЫ БАНКИ УСПЕЛИ СЕРЬЁЗНО ПОДГОТОВИТЬСЯ»

Закон вступит в силу в октябре, у банков есть полгода, чтобы подготовиться и разработать сервисы для мониторинга, нотификаций и ответов.

«Не думаю, что этого времени хватит, чтобы каждая кредитная организация России успела разработать полный набор сервисов для взаимодействия с ЦБ», — высказывает свою точку зрения технический директор ИТ-компании HFLabs Никита Назаров.

По его словам, также есть вопросы к способности банков заполнить все требуемые поля: если документ, удостоверяющий личность плательщика, у банка быть обязан (хотя на практике они бывают и неактуальными), то СНИЛС есть редко, а уж про ДУЛ, СНИЛС и ИНН получателя говорить не приходится.

«Регулятор также предполагает сбор массы информации об устройствах, с которых выполняются операции: IP и MAC-адреса, ICCID и IMSI-коды телефонов — всё это не является обязательным, но без передачи такой информации процесс расследований вряд ли упростится. А банкам придётся более серьёзно относиться к сбору информации и её структурированию», — уверен эксперт.

«ЦБ ГОТОВИТ БАНКИ К НОВЫМ ЗАКОНОДАТЕЛЬНЫМ ПОПРАВКАМ»

«На наш взгляд, само по себе требование о сборе и передаче такого рода информации является позитивным фактом как минимум потому, что обяжет банки собирать информацию такого рода. Мы предполагаем, что в дальнейшем

ЦБ так или иначе будет эту информацию агрегировать и использовать для оценки текущей ситуации, а в идеальном варианте — приведёт к принятию в отрасли новых стандартов», — делится своей точкой зрения эксперт по информационной безопасности, директор технологического стартапа «Третья сторона» (3side.org) Антон Бочкарев.

По его словам, уже сейчас многие банки имеют собственные алгоритмы выявления подозрительных транзакций, которые активно используются и позволяют предотвратить значительную часть мошеннических операций.

«Не исключено, что ЦБ готовит банки к поправкам в законодательстве, которые переложат на них потенциальные убытки по мошенническим транзакциям, даже если они были совершены самим клиентом, — предполагает эксперт. — Предусматривающий это закон был принят Госдумой в первом чтении 15 марта 2023 года».

Безусловно, вместе с применением других систем, таких как разрабатываемая ЕИС ПСА (система проверки сведений об абоненте), может существенно повысить уровень безопасности, сократить для банка операционные риски и снизить возможный ущерб от действий мошенников, но это будет

зависеть от конкретной реализации требований ЦБ и возможных изменений в законодательстве, отмечает Бочкарев.

Безусловно, необходимость внедрения подобных изменений увеличит для банков операционные расходы, потребует найма дополнительных специалистов и, вероятно, инвестиций в инфраструктуру, считает он. С другой стороны, получение доступа к новой информации может улучшить качество внутрибанковских моделей предотвращения мошенничества и в конце концов как сократить ущерб, наносимый клиентам банка, так и снизить собственно банковские оперриски, подчёркивает эксперт.

«Очень многое зависит от того, кто в конце концов, по мнению ЦБ, должен будет платить за фактически понесённый от действий мошенников ущерб — в случае с российской банковской системой речь идёт о 14,2 млрд рублей за прошлый год, и количестве незаконных операций, которое составило порядка 900 тысяч. Поэтому в краткосрочной перспективе мы видим необходимость инвестирования как в инфраструктуру, так и в сотрудников. В долгосрочной — возможное сокращение числа мошеннических транзакций», — считает Бочкарев.

«ГОВОРИТЬ ОБ ОПЕРЕЖЕНИИ МОШЕННИКОВ ПОКА НЕВОЗМОЖНО»

Расширение критериев информационного обмена коммерческих банков, мегарегулятора и силовых структур относительно киберинцидентов вполне логично и высоковероятно повысит уровень кибербезопасности, но говорить об опережении мошенников вряд ли возможно, высказывает своё мнение кандидат экономических наук, декан факультета «Цифровая экономика и массовые коммуникации» МТУСИ **Сергей Гатауллин**.

«Всё расширение полей сбора информации продолжает носить характер анализа данных постфактум и не гарантирует защиту от фрода, который постоянно меняет своё цифровое обличье. Сложность борьбы с фродом заключается именно в том, что киберпреступники постоянно меняют свои бизнес-модели, оперативно подстраиваясь под технологический стек силовых структур, находя уязвимости. При этом бизнес-модели фрода усложняются и помимо новых информационных технологий активно используют и социальную инженерию, от которой обмен самой полной информацией о киберинцидентах не спасает», — объясняет эксперт.

Однако борьбу с фродом необходимо продолжать, и затраты на обеспечение кибербезопасности будут увеличиваться, говорит Гатауллин. Мошенники зачастую используют самые современные технологии, в том числе искусственного интеллекта, для осуществления киберпреступлений, и противостоять им должны сотрудники соответствующего уровня подготовки, подчёркивает он. При этом нельзя допустить создания условий, в которых финансовые учреждения вынуждены будут скрывать киберинциденты.

ЭФФЕКТИВНАЯ РАБОТА ФИНЦЕРТ

По мнению руководителя направления аудитов и соответствия требованиям ИБ компании УЦСБ (Екатеринбург) **Евгения Баклушина**, сейчас сложно говорить о каких-то конкретных цифрах, но уровень информационной безопасности в результате принимаемых ЦБ мер точно возрастет.

«В России Центробанк — один из локомотивов в вопросе обеспечения кибербезопасности, поэтому здесь однозначно стоит ожидать от коллег из ФинЦЕРТ дальнейшего улучшения своей деятельности, своих процессов», — отмечает эксперт.

Он считает, что возможно активное включение ФинЦЕРТ в международное сотрудничество по противодействию мошенническим операциям. Например, с Национальным центром мониторинга кибербезопасности Республики Беларусь в рамках Союзного государства.

«Здесь уже ведётся работа с коллегами по многим направлениям, финансовые мошеннические операции не будут исключением. Также в рамках наверняка будет взаимодействие с аналогичными центрами стран-участников ШОС и БРИКС», — отмечает Баклушин.

Директор по продуктам компании «Гарда Технологии» **Павел Кузнецов** говорит, что в целом деятельность по предотвращению мошеннических операций ведётся Центральным банком уже далеко не первый год.

«Наибольшую эффективность ФинЦЕРТ продемонстрировал в первые три года после своего создания. Текущие нововведения просто расширяют перечень данных, предоставляемых участниками финансового рынка регулятору в целях более эффективной координации борьбы с мошенничеством с участием правоохранительных органов», — отмечает эксперт.

ПОСЛЕСЛОВИЕ. СРАБОТАЕТ ЛИ ПРАВИЛО: ЧЕМ БОЛЬШЕ ИНФОРМАЦИИ, ТЕМ БОЛЬШЕ ЗАЩИТЫ?

Таким образом, можно констатировать, что у банков есть почти полгода для того, чтобы подготовиться к выполнению требований ЦБ, предусмотренных новой редакцией стандарта правил информационного обмена о кибератаках и инцидентах информационной безопасности в финансовой сфере (СТО БР БФБО-1.5–2023). По мнению регулятора, эти нововведения необходимы для исполнения закона об информационном обмене между регулятором и МВД России.

Сбор информации обо всех участниках переводов и её детализация по более чем 50 уникальным признакам — это дополнительная нагрузка на банки, которым придётся перенастраивать текущие СЗИ. С другой стороны, пока непонятно, какое наказание последует, если требования не будут выполнены. Только после того как новая редакция стандарта заработает, можно будет оценить, насколько это полезно для конечного пользователя — клиента кредитной организации. Потому что количество собираемой информации растёт из года в год, а вот киберпреступность от этого не падает, скорее наоборот, она увеличивается по мере роста тех данных, которые собирают о гражданах не только банки, но и многие другие учреждения, включая государственные.

При этом стоит отметить, что банки не впервые выполняют новые требования регулятора и расширяют свои системы и сервисы. Возможно, в ближайшем будущем им это будет очень даже полезно, учитывая то, что регулятор может рано или поздно принять решение о том, чтобы возложить на кредитные организации убытки по мошенническим транзакциям, даже если они были совершены самим клиентом.



Александр БАБКИН
вице-президент —
начальник
Департамента
информационной
безопасности,
Газпромбанк

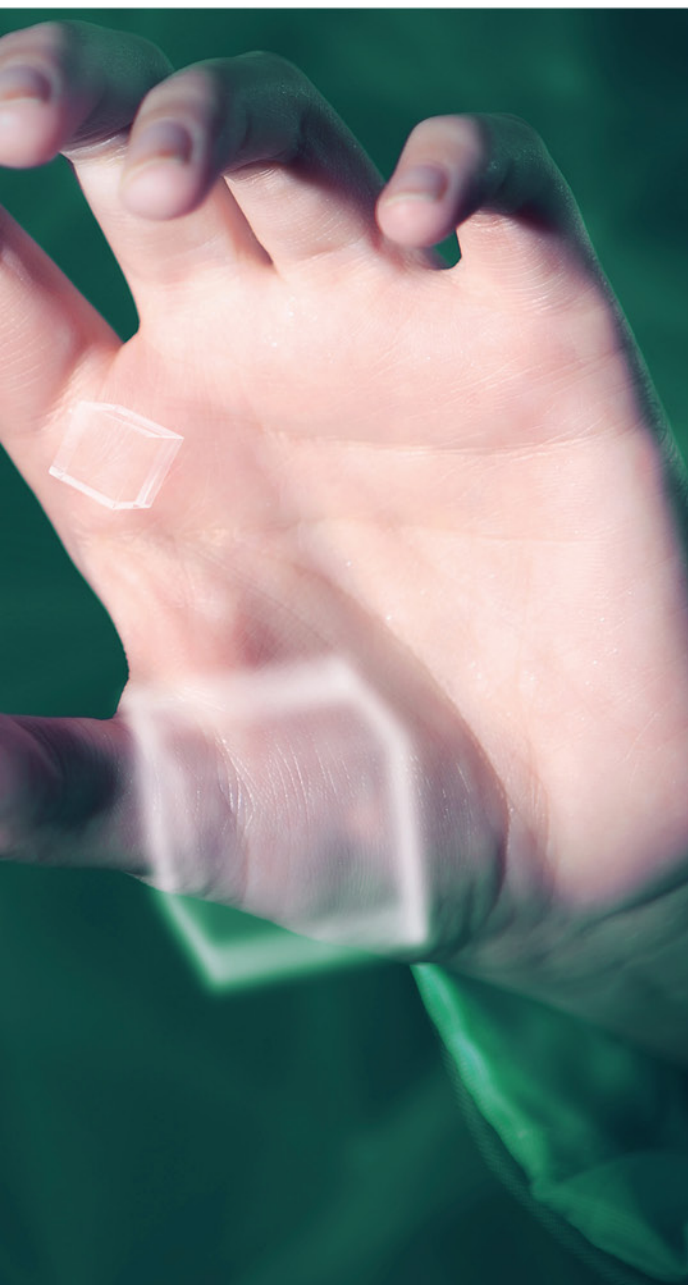
«ИНТЕГРАЦИЮ НОВЫХ РЕШЕНИЙ В ИБ МОЖНО СРАВНИТЬ С РЕМОНТОМ АВТОМОБИЛЯ НА СКОРОСТИ 150 КМ/Ч»

Газпромбанк в прошлом году столкнулся с большим количеством вызовов, среди которых необходимость внедрять новые решения для обеспечения информбезопасности и отражение хакерских атак. О том, как банк справился с этими задачами и какие ИБ-технологии сейчас в тренде, рассказал вице-президент — начальник Департамента информационной безопасности Александр Бабкин.

Немного предыстории. Традиционно банк выстраивал информационную защиту, используя проверенные зарубежные Enterprise-решения. Мы выбирали самые лучшие и функциональные разработки из всех доступных на мировом рынке для того, чтобы обеспечить максимально

высокий уровень информбезопасности. В ряде сфер лидерами были российские компании, например разработчики антивирусных программ, и в таком случае мы, конечно, использовали наше ПО. С 2014 года мы стали целенаправленно мигрировать на российские решения, выбирая те, что по своим параметрам не уступали зарубежным. Это была плановая работа, которая велась в соответствии с принятой стратегией.

В прошлом году нам, как и всем, пришлось ускориться. Некоторые западные вендоры ушли, передав свой бизнес, а некоторые просто отключили свои сервисы. Негативных последствий удалось избежать благодаря тому, что у нас была выстроена многоуровневая система защиты. И когда, к примеру, один из



спам-фильтров превратился в «кирпич», мы переключились на другой и не допустили возникновения угрозы.

Весь прошлый год, помимо того, что приходилось отбиваться от постоянных кибератак, мы активно занимались импортозамещением. Мы выбирали производителей, проводили исследования и запускали «пилоты», сравнивали результаты и делали выбор. Было понятно, что волшебной таблетки не существует, поэтому выбирали тех производителей, которые были готовы учитывать наши замечания и оперативно дорабатывать продукт. Сейчас у нас замещено 70% всех решений в информбезопасности.

В этом году продолжаем внедрять уже выбранные решения, следим за их развитием

и строим полностью импортозамещённую среду. У информбезопасности своя специфика, в частности, надо обеспечить переход так, чтобы все сервисы банка продолжали работать с тем же уровнем защиты. Можно это сравнить с необходимостью поменять деталь автомобиля, когда тот мчится на скорости 150 км в час.

Самая сложная часть с точки зрения замещения — это программно-аппаратные комплексы. Так, есть потребность в межсетевых экранах, которые бы выдерживали значительные нагрузки. Для межсетевой безопасности необходимо обеспечить большую скорость обмена информацией, а для этого нужно соответствующее оборудование, и в этом пока слабое место отечественных производителей. Ждём в этой области решений от российских вендоров.

Ещё одна особенность нашей работы в том, чтобы всё время быть на шаг впереди, а для этого надо постоянно развивать действующие системы и внедрять новые. Если говорить о современных трендах, то это, конечно, использование Machine Learning и математического моделирования (в том числе искусственного интеллекта). Ещё один тренд в информбезопасности — системы аналитики поведения пользователей — User Behavior Analytics. Система определяет шаблоны в типичном поведении пользователей, а затем детектирует аномальные действия, которые не соответствуют этим шаблонам и могут представлять проблемы с безопасностью. Аналогично можно настроить выявление нетипичных событий в различных процессах, ПО, системах хранения данных и т.п.

Мы также видим перспективы в развитии Threat intelligence platform — платформ для киберразведки, которые позволяют быстро обмениваться информацией. Если вернуться к событиям прошлого года, то эффективно отражать атаки удавалось в том числе за счёт взаимодействия между участниками рынка, регулятором и отраслями. Так, если компания из другого сектора или финансовая организация сталкивалась с мощной DDoS-атакой, мы получали предупреждение и оперативно донстраивали свои системы. На мой взгляд, консолидация усилий позволяет эффективно реагировать на возникающие вызовы.

Актуальный для банка тренд — построение единой системы информационной безопасности для того, чтобы обеспечить защиту не только своего контура, но и тех организаций, с которыми происходит взаимодействие. В прошлом году мы столкнулись с атаками не только на банк, но и на дочерние компании. Сейчас занимаемся созданием единого центра, который разработает стандарты ИБ для всех этих компаний и обеспечит их внедрение.



Александр ВИНОГРАДОВ
старший научный сотрудник
ФГУП «ЦНИИХМ»



Вадим АНДРЕЕВ
заместитель начальника
СИБ ООО КБ «АРЕСБАНК»



Анастасия НИКОЛАЕВА
эксперт BIS Journal

ГОТОВЬСЯ, ТОВАРИЩ!

НЕ НАДО БОЯТЬСЯ ПРОВЕРКИ ЦБ, ЕСЛИ ТЫ ВО ВСЕОРУЖИИ

Проверки ЦБ — вопрос не новый, он знаком всем специалистам ИБ банка, так как, наверное, каждый из них хоть раз в жизни такую проверку проходил. Описывать порядок проведения проверки не стоит. Процесс понятный и страшный одновременно, вызывающий стресс и ведущий к дурным воспоминаниям. Вечером — ожидаемый, но всегда внезапный — запрос от проверяющих, и ты, «вырывая на себе волосы», «в холодном поту», пытаешься закрыть все пункты в этом запросе. Что-то уже есть, а чего-то нет, и это что-то придётся сделать до утра.

ЭТО НЕ НАШ МЕТОД!

И многие, заранее предвкушая такое «счастье», пытаются уволиться во время проверки, сразу после осознания реальных масштабов постигшего их бедствия. А дальше — хоть «травка не расти». «Пусть банк сам решает свои проблемы. Я просил руководство. Мне не дали. Ну вот и всё. Пока!» — такой монолог в момент стресса возникает в голове практически каждого ИБэшника.

НО. Товарищи, это не наш метод! Зачем портить себе карьеру на пустом месте? Ведь в банке работают люди, которые не виноваты, что руководитель службы ИБ не смог донести до руководства размеры бедствия и объёмы предстоящих штрафов. Поэтому будем спасать себя и выращивать хороших людей!

ЧТО ДЕЛАТЬ?

Первое, что необходимо сделать, когда узнал о проведении проверки ЦБ:

1. Понять, на какой стадии находится ИБ банка.
2. Заранее собрать все документы и перевести их в электронный вид. Всё общение с проверяющими будет проходить через портал ЦБ.

3. Если время ещё есть, то актуализировать приказы (может, люди уже уволены), списки ответственных и допущенных, разместить их в нужных местах.

4. Максимально устранить недостатки, которые легко проверяются и на устранение которых требуется минимум усилий. Например, заблокировать учётные записи уволенных сотрудников, отобрать лишние администраторские права у секретаря, опломбировать и закрыть на замки серверные шкафы.

5. Не лишним будет напомнить пользователям об их обязанностях по хранению ключей, носителей информации, паролей.

6. Провести запланированные (но отложенные) работы и контрольные мероприятия (например: отчёт на регулярной основе, акт по проверке Плана ОНВД и др.).

7. Если ещё осталось и после выполнения всех выше пунктов время, то заняться, уже глубоко, устранением более серьёзных косяков. (Например: закупить недостающие СЗИ, донастроить («убрать временные костыли») систему и др.).

ЧЕГО ОНИ ХОТЯТ?

И главное, надо понимать, что проверяющие из ЦБ хотят написать красивый отчёт со стандартными нарушениями, без колоссальных усилий и копаний в инфраструктуру банка, а не наказать вас по всей строгости закона за невыполнение всех нормативных документов.

НА ЧТО ОБРАТИТЬ ВНИМАНИЕ

Кредитно-финансовая сфера — самая зарегулированная в области информационной безопасности. Основные действующие положения по защите информации для банков на сегодняшний день — 683-П, 719-П, 802-П. Положения новые,

недостаточно проработанные и изученные со стороны специалистов ИБ банков.

Как же провести самооценку выполнения требований положений, на что необходимо обратить внимание, чтобы соответствовать многочисленным требованиям ЦБ.

Рассмотрим требования по Положениям.

ПОЛОЖЕНИЕ № 683-П

Положение от 17 апреля 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»

В данном положении устанавливаются требования к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента, применяются для обеспечения защиты информации, подготавливаемой, обрабатываемой и хранимой в автоматизированных системах, входящих в состав объектов информационной инфраструктуры и используемых для осуществления банковских операций, связанных с осуществлением перевода денежных средств:

- ♦ информации, содержащейся в документах, составленных при осуществлении банковских операций в электронном виде (электронные сообщения), формируемых работниками кредитных организаций и (или) клиентами кредитных организаций;

- ♦ информации, необходимой для авторизации клиентов при совершении действий в целях осуществления банковских операций и удостоверения права клиентов распоряжаться денежными средствами;

- ♦ информации об осуществлённых банковских операциях;

- ♦ ключевой информации средств криптографической защиты информации (СКЗИ), используемой при осуществлении банковских операций (криптографические ключи);

- ♦ а также к персональным данным субъекта РФ.

Требуется обратить пристальное внимание на выполнение пункта 5.2683-П, а именно: регламентацию, реализацию, контроль (мониторинг) технологии обработки защищаемой информации, указанной выше, при совершении следующих действий:

- ♦ идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций;

- ♦ формирование (подготовка), передача и приём электронных сообщений;

- ♦ удостоверение права клиентов распоряжаться денежными средствами;

- ♦ осуществление банковской операции, учёт результатов её осуществления;

- ♦ хранение электронных сообщений и информации об осуществлённых банковских операциях.

Кредитно-финансовые организации должны определить объекты информационной безопасности, которые задействованы на каждом технологическом участке. Обеспечить фиксацию указанных действий (событий) и хранение. А также обеспечить способ оперативного предоставления указанных данных в случае требования регулятора, обеспечив наличие следующих обязательных полей:

1. дата (день, месяц, год) и время (часы, минуты, секунды) осуществления банковской операции;

2. присвоенный работнику идентификатор, позволяющий установить работника в автоматизированной системе, программном обеспечении;

3. код, соответствующий технологическому участку;

4. результат осуществления банковской операции (успешная или неуспешная);

5. идентификационная информация, используемая для адресации устройства, с использованием которого и в отношении которого осуществлён доступ к автоматизированной системе, программному обеспечению с целью осуществления банковских операций (сетевой адрес компьютера и (или) коммуникационного устройства (маршрутизатора).

ПОЛОЖЕНИЕ № 719-П

Положение от 4 июня 2020 г. № 719-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»

Особое внимание необходимо обратить при прочтении пункта 2.8 на конструкцию «и (или)»:

При осуществлении переводов денежных средств с использованием сети Интернет и размещении программного обеспечения, используемого клиентами операторов по переводу денежных средств при осуществлении переводов денежных средств, на средствах вычислительной техники, для которых операторами по переводу денежных средств не обеспечивается непосредственный контроль защиты информации от воздействия вредоносного кода, операторы по переводу денежных средств должны обеспечить реализацию технологических мер и (или) реализовать ограничения по параметрам операций

по осуществлению переводов денежных средств, определяемые договорами операторов по переводу денежных средств с клиентами.

Кредитно-финансовая организация в своих бизнес-процессах, в которых осуществляются переводы денежных средств, должна реализовать и регламентировать реализацию технологических мер. Или вместо этого установить и прописать во внутренних документах лимиты по параметрам операций.

ПОЛОЖЕНИЕ № 787-П

Положение от 12 января 2022 г. № 787-П «Об обязательных для кредитных организаций требованиях к операционной надёжности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг»

Рассмотрим пункт 6.1 «Кредитные организации должны обеспечивать организацию учёта и контроля состава следующих элементов»:

- ◆ технологических процессов, реализуемых непосредственно кредитной организацией;
- ◆ подразделений (работников) кредитной организации, ответственных за разработку технологических процессов, поддержание их выполнения, реализацию технологических процессов;
- ◆ объектов информационной инфраструктуры кредитной организации, задействованных при выполнении каждого технологического процесса;
- ◆ технологических участков технологических процессов, установленных в 683-П;
- ◆ технологических процессов, технологических участков технологических процессов, реализуемых поставщиками услуг в сфере информационных технологий;
- ◆ работников кредитных организаций или иных лиц, осуществляющих физический и (или) логический доступ, или программных сервисов, осуществляющих логический доступ к объектам информационной инфраструктуры, задействованных при выполнении каждого технологического процесса;
- ◆ взаимосвязей и взаимозависимостей кредитной организации с иными кредитными организациями, некредитными финансовыми организациями, поставщиками услуг в сфере информационных технологий в рамках выполнения технологических процессов;
- ◆ каналов передачи защищаемой информации, установленной в 683-П, обрабатываемой и передаваемой в рамках технологического процесса.

Кредитно-финансовая организация должна организовать учёт, производить актуализацию и назначать ответственных сотрудников (пример: служба ИБ, служба автоматизации или оба эти подразделения).

ПОЛОЖЕНИЕ № 802-П

Положение от 25 июля 2022 г. № 802-П «О требованиях к защите информации в платёжной системе Банка России»

В данном положении следует быть внимательным к пункту 1.2 Приложения:

«Участник ССНП должен разместить объекты информационной инфраструктуры контура формирования электронных сообщений и контура контроля реквизитов электронных сообщений в информационной инфраструктуре участника ССНП в разных сегментах вычислительных сетей, в том числе реализованных с использованием технологии виртуализации. Способ допустимого информационного взаимодействия между указанными сегментами вычислительных сетей оформляется документально и согласовывается со службой информационной безопасности участников ССНП».

Именно предоставление фактов согласования со службой информационной безопасности и утверждения требуется Регулятором. По этой причине следует заранее продумать, как правильно оформить и утвердить:

Схемы сетевого взаимодействия объектов информационной инфраструктуры, задействованных при переводах денежных средств через платёжную систему Банка России;

Правила и ограничения сетевого взаимодействия между объектами, обеспечивающие их изоляцию в разных сегментах вычислительных сетей;

Состав эксплуатационного персонала, ответственного за разные сегменты вычислительной сети.

При выполнении требований к защите информации в платёжной системе Банка России следует помнить о необходимости выполнения требований эксплуатационной (технической документации) СКЗИ, программного обеспечения и иных требований.

Так, для СКЗИ СИГНАТУРА формуляр ВАМБ.00107–06 93 01 рекомендуется выполнение 25 пунктов настроек, которые легко забыть реализовать в полном объёме и так же легко проверить регулятору.

Выше представлены только основные требования, которые были выставлены кредитно-финансовым организациям при проведении проверок ЦБ. Будем держать руку на пульсе и собирать в дальнейшем требования при проверке, освещать их на конференциях и в статьях.



Kaspersky Unified Monitoring and Analysis Platform

Центральный элемент единой платформы безопасности

- Мониторинг и анализ инцидентов ИБ
- Поточковая корреляция в режиме реального времени
- Автоматическое обогащение данными об угрозах
- Масштабируемая архитектура и низкие системные требования
- Тесная интеграция с решениями «Лаборатории Касперского» и сторонних производителей
- Обеспечение соответствия законодательству в сфере безопасности объектов КИИ

kaspersky АКТИВИРУЙ
БУДУЩЕЕ

kaspersky.ru/enterprise

ДиалОгНаука

СИСТЕМНАЯ ИНТЕГРАЦИЯ В ОБЛАСТИ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

dialognauka.ru



**Александр
ТОВСТОЛИП**
руководитель
управления
информационной
безопасности
Ассоциации ФинТех

ОТКРЫТЫЙ КОД В ФИНСЕКТОРЕ

МОЖЕТ ЛИ ФИНАНСОВЫЙ РЫНОК ДОВЕРИТЬСЯ OPENSOURCE-РЕШЕНИЯМ?

Российский финансовый рынок стремительно развивается: банки в последние годы стали одними из крупнейших разработчиков и заказчиков специализированного ПО. Некоторыми из своих наработок они готовы поделиться с коллегами, но пока на рынке нет эффективно работающего механизма для этого. Поэтому участники рынка решают типовые задачи независимо друг от друга, нередко используя для этого одни и те же OpenSource-инструменты. О том, как объединить усилия финансовых организаций и зачем банкам единое хранилище отраслевых решений, рассказывает руководитель Управления информационной безопасности Ассоциации ФинТех Александр Товстолип.

По данным [опроса](#), проведённого компанией Accenture при поддержке Фонда «Сколково», в 2021 году OpenSource-решения применяли все компании-разработчики, а также 79% компаний-потребителей. Прогнозируется, что к концу

2026 года решения с открытым кодом будут применять до 92% российских компаний. Причём многие из них сами разрабатывают прикладное ПО и инструменты разработки.

КАЖДЫЙ САМ ЗА СЕБЯ?

За относительно короткое время финансовый рынок в РФ прошёл путь от одного из самых медленных и забюрократизированных сегментов экономики до лидера инноваций. Активную роль в этом процессе сыграли крупнейшие игроки и Банк России, взявший в 2015 году курс на развитие финансовых технологий на российском рынке. В результате уже в 2019 году Россия вошла в тройку лидеров по проникновению финтех-услуг: 82% граждан использовали их в своей обычной жизни. А по данным исследования BusinesStat, за пять лет (с 2017 года по 2021 год) рынок вырос более чем в 2 раза: с 31,7 млрд рублей до 67,1 млрд рублей. И этот процесс продолжается. Люди всё реже

БАНК РОССИИ ВКЛЮЧИЛ «МАСТЕРЧЕЙН» В РЕЕСТР ОПЕРАТОРОВ ИНФОРМАЦИОННЫХ СИСТЕМ

Компания «Мастерчейн»¹ (ООО «Системы распределённого реестра») получила статус оператора информационной системы, в которой осуществляется выпуск цифровых финансовых активов (ЦФА) на собственной блокчейн-платформе, входящей в реестр отечественного ПО. Компания предоставит рынку площадку для выпуска ЦФА, а также лицензионное ПО для

организации работы будущих операторов информационной системы.

В ближайшее время «Мастерчейн» допустит к своей платформе клиентов для выпуска и торговли ЦФА. Компания также рассматривает возможность подключения внешних агентов и брокеров для привлечения ещё большего числа эмитентов и инвесторов.

На первом этапе компания будет выпускать цифровые финансовые активы на право денежного требования, которые могут структурироваться либо как облигации (без привязки к активам), либо как структурные инструменты с привязкой к любым видам активов. В последующих релизах будут выпущены остальные виды ЦФА: гибридные, на долю

¹ Компания «Мастерчейн» — ведущий эксперт в области разработки и развития блокчейн-решений. Специализируется на создании, внедрении и сопровождении сервисов и программных продуктов на собственной блокчейн-платформе «Мастерчейн». Учреждена в 2021 г. ведущими участниками финансового рынка РФ: ВТБ, Газпромбанк, ПСБ, Московская биржа, НСПК, Ассоциация ФинТех.

посещают отделения банков, а если и посещают, то проводят там гораздо меньше времени, чем раньше. Современный банкинг становится всё более цифровым: практически все необходимые операции — от платежей и переводов до получения кредитов — можно совершить удалённо в интернет-банке или мобильном приложении.

Чтобы сделать финансовые продукты удобнее и технологичнее, участники рынка применяют технологии big data, используют разнообразные движки, библиотеки, инструменты разработки. Причём разные участники рынка, имеющие сходные продукты и сервисы, вынуждены фактически изобретать велосипед, разрабатывая одни и те же решения параллельно. Для этого компании чаще всего используют OpenSource, что предполагает создание или аренду хранилищ, тестирование и отладку софта.

Крупные банки на всех этапах стараются использовать «своё» — дата-центры, разработчиков, инструменты и среду разработки. Более того, под некоторые задачи крупнейшие участники рынка готовы запустить отдельные проекты по созданию специализированных решений. У них достаточно ресурсов для тестирования ПО — они используют собственных сотрудников или привлекают сторонние компании, расходуя на это сотни миллионов и даже миллиарды рублей. В то же время небольшие компании не могут себе позволить таких бюджетов.

Бурный рост и развитие финтеха сформировали потребность в создании экспертного отраслевого сообщества, в рамках которого можно было бы эффективно обмениваться информацией, тестировать и дорабатывать готовые решения, делиться опытом. Особенно важно, чтобы это была независимая площадка с равным доступом для всех участников. А это значит, что на базе одного из игроков, например банка или ИТ-компании, создать такое сообщество не получится.

ОДИН ЗА ВСЕХ И ВСЕ ЗА ОДНОГО

Финтех-сообщество уже не первый год говорит о необходимости создания отраслевого хранилища решений, а также экспертного сообщества на его базе. Реализация этих планов позволит крупным игрокам оптимизировать ИТ-расходы, безопасно хранить свои разработки, привлекать к их тестированию и доработке других участников рынка. Для небольших компаний создание финтех-сообщества и репозитория отраслевого ПО — возможность нарастить свои компетенции и получить доступ к доверенному ПО и инструментам разработки отраслевых решений. Такой подход позволит распределить ресурсы среди участников сообщества, привлечь другие компании для решения текущих задач, откроет равный доступ всем участникам рынка к актуальному ПО.

От создания отраслевого финтех-сообщества выиграют не только финтех-компании.

в непубличном акционерном обществе и права требования по эмиссионным ценным бумагам.

«Мастерчейн» уже имеет ряд договорённостей о выпуске ЦФА с ведущими российскими компаниями. Среди них — «ВТБ Факторинг», где базовым активом для ЦФА выступит портфель обязательств, уступленных в адрес фактора, и девелопер «Джи-групп», который планирует выпустить на платформе «Мастерчейн» ЦФА с привязкой к стоимости квадратного метра строящегося жилья.

«Мы давно обсуждали с коллегами из „Мастерчейн“ возможность выпуска ЦФА с привязкой к рыночной стоимости квадратного метра в жилых комплексах компании или рентного дохода с коммерческой площади наших торговых центров. Считаем, что этот продукт востребован на рынке. С помощью площадки „Мастерчейн“ мы сможем предложить российским инвесторам совершенно новый инвестиционный продукт, соединяющий инновационный финансовый инструмент ЦФА с real estate», — отмечает директор по ЦФА АО «Джи-групп» Алексей Фатхудинов.

«Отличительная черта „Мастерчейн“ в том, что мы единственный оператор информационной системы, который

разрабатывает информационные системы ЦФА для других участников рынка. Собственная экспертиза в ЦФА позволяет также осуществлять консалтинг в процессе создания оператора ЦФА», — комментирует Иван Оперчук, генеральный директор компании «Мастерчейн».

«Банк России включил в реестр операторов информационных систем компанию „Мастерчейн“. Это должно создать дополнительный стимул для развития рынка цифровых финансовых активов в России. На наш взгляд, компания „Мастерчейн“ обладает компетенциями, необходимыми для того, чтобы предложить рынку оригинальную блокчейн-платформу для широкого круга эмитентов ЦФА и расширить продуктовую линейку базовых активов для цифровизации», — отмечает заместитель генерального директора Ассоциации ФинТех, член совета директоров ООО «Системы распределённого реестра» (бренд «Мастерчейн») Дмитрий Ищенко.

Платформа ЦФА, с которой компания прошла аудит в Банке России, доступна будущим операторам информационной системы в качестве лицензионного программного обеспечения. «Мастерчейн» уже заключила первые сделки по продаже платформы, ведутся переговоры с другими игроками рынка.



Положительным эффектом для потребителей станет рост безопасности финансовых продуктов, а также, потенциально, выход на рынок новых решений за счёт роста скорости разработки и тестирования ПО. Кроме того, использование отраслевого репозитория открытого ПО будет способствовать росту конкуренции на рынке, так как участники рынка смогут перераспределить ресурсы, сосредоточившись на разработке продуктов и услуг.

РЕПОЗИТОРИЙ ИТ-РЕШЕНИЙ НА ПОДХОДЕ

В декабре 2022 года Ассоциация ФинТех (АФТ) провела круглый стол с представителями финансовой отрасли, участники которого обозначили необходимость создания доверенного репозитория и профессионального комьюнити на независимой, равноудалённой от всех участников площадке. Такой площадкой и стала АФТ.

Планируется придать этому репозиторию статус доверенного, чтобы к нему могли обращаться участники финансовой отрасли, в том числе и для выполнения требований и соблюдения стандартов Банка России. Требования к репозиторию разработаны на площадке АФТ, в рамках пилотов и рабочих групп, в которые входили ведущие представители финансовой отрасли.

Участники АФТ, у которых выстроен процесс безопасной разработки ПО, поделились опытом. Выработанные требования согласовываются со всеми регуляторами, идут обсуждения с Банком России.

На первом этапе драйвером развития репозитория станет Мосбиржа, которая уже готова передать ряд своих разработок, в том числе инструменты разработки, созданные на базе OpenSource. В ближайшее время к процессу подключатся и другие участники Ассоциации ФинТех. Инфраструктура и финансирование проекта — на стороне АФТ. На первом этапе использовать возможности репозитория смогут участники АФТ, выразившие такое желание, в дальнейшем — все участники финтех-сообщества.

Запуск репозитория и создание отраслевого экспертного сообщества будет стимулировать развитие финтех-рынка, появление новых продуктов и услуг, что положительно скажется на финансовом секторе и экономике в целом. Кроме того, рынок получит доверенное ПО, использование которого снизит потенциальные риски.

ОПАСНОСТИ ДИРЕКТИВНОЙ ЦЕНТРАЛИЗАЦИИ

О ЧЁМ СЛЕДУЕТ ПОМНИТЬ, РАЗВИВАЯ ОТРАСЛЕВЫЕ ЦЕНТРЫ ПРОТИВОДЕЙСТВИЯ КИБЕРУГРОЗАМ (ЦПК)

С прошлого года на страницах BIS Journal (№ 4/2022, № 1/2023) развивается дискуссия об аутсорсинге в сфере ИБ. На примере создания Центра противодействия киберугрозам (ЦПК) рассматриваются невероятные перспективы централизации ИБ-компетенций, столь востребованных в сфере финансов. Из более чем 15 000 субъектов этого рынка многие организации не в состоянии позволить себе собственную службу ИБ, а риски безопасности, в том числе правовые, непрерывно растут. В такой парадигме преимущества централизации у многих не вызывают сомнений. Но так ли это на самом деле? Нет ли у централизации оборотной стороны и нужно ли вообще сводить дискуссию к выбору между «чёрным» и «белым», утверждая вслед за древними *tertium non datur*? Может быть, существует «третий путь», который позволяет сочетать все плюсы концепции ЦПК с альтернативными подходами? На фоне высказываемых ФСТЭК России мыслей о необходимости переноса опыта ЦБ в другие сферы и создания отраслевых регуляторов ИБ¹ в других сферах экономики этот вопрос из «местечкового» приобретает межотраслевое значение.

ОБЩИЕ СООБРАЖЕНИЯ В ПОЛЬЗУ СМЕШАННЫХ СИСТЕМ

Читатели статьи имеют право знать о предвзятости автора. Не являясь идейным противником централизации, автор не относит себя и к анархистам, предпочитая смешанные системы. Смешанные не в том смысле, в каком это может представляться любителям коктейлей и «свободного рынка», но системы, которые целенаправленно спроектированы для сочетания преимуществ обоих подходов. То есть системы, построенные таким образом, чтобы элементы централизации (иерархии) и децентрализации (горизонтальности) обеспечивали максимальную степень устойчивости и адаптивности целого. В полном соответствии с

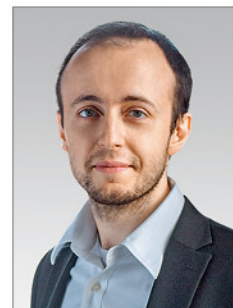
заветами кибернетики или, если хотите, эволюционной биологии. Да-да, именно эволюционной биологии, ведь именно природа на примере экосистем выработала принципы обеспечения равновесия. Равновесия, в котором есть место и «вертикальной интеграции», и «тысячам горизонтальных связей». Равновесия, в котором остаётся пространство для маневра, обеспеченного сочетанием избыточного разнообразия с вертикальными цепочками связей, во главе которых располагаются доминирующие виды.

Избыточное разнообразие означает, что число видов живых существ и количество связей между ними сильно больше, чем нужно для поддержания существования экосистемы с точки зрения её краткосрочной «эффективности». При этом в конкретных нишах или цепочках связей могут возникать доминирующие виды, но их доминирование не обусловлено каким-то вечным законом и является ситуативным. Такой подход позволяет системе не разваливаться как карточный домик под влиянием новых обстоятельств, но более миллиарда лет осуществлять пересборку на фоне происходящих изменений среды и катастроф. Желая глубже порефлексировать социальный, исторический и менеджерский аспект проблемы можно отослать к специальному исследованию автора², ну а мы спустимся с небес абстрактного мышления на грешную землю конкретных проблем сферы ИБ и посмотрим, как эту оптику можно применить к нашей внутренней кухне.

АРГУМЕНТАЦИЯ ЗА ЦЕНТРЫ ПРОТИВОДЕЙСТВИЯ КИБЕРУГРОЗАМ (ЦПК) И ЦЕНТРАЛИЗАЦИЮ АУТСОРСИНГА ИБ

Аргументы в пользу ЦПК сводимы к следующему набору:

1. В условиях дефицита кадров в ИБ целесообразно создавать подобные органы, которые предоставят качественную экспертизу всем страждущим и решат проблемы небольших организаций, не способных позволить себе



Рустам ГУСЕЙНОВ
председатель
кооператива «Рад
Коп» (radcop.online),
эксперт АРБ

¹ См. выступление представителя ФСТЭК России на SOC-Forum 2022: <https://youtu.be/kBRf6CGU41I>.

² См. видеодоклад автора в «Точке кипения» от 20.08.2022: https://youtu.be/Ntd_UnljGSg.

собственных квалифицированных специалистов в силу ряда причин (прежде всего финансовых ограничений);

2. Опыт подобных структур не нов, и мы хорошо понимаем, как системы SOC и CERT функционируют за рубежом, а кроме того, имеем собственный опыт аутсорсинга, регулирования зон ответственности между заказчиком работ (ответственным за ИБ) и поставщиком услуг (ответственным за сервис MSSP), контроля SLA и даже управления соответствующими рисками (СТО БР ИББС-1.4-2018, требования положений Банка России об операционных рисках и опернадёжности, новые части стандартов серии 57580).

И алгоритм решения выглядит достаточно простым: давайте создавать единые отраслевые центры, которые будут централизованно закрывать потребности если не всей экономики, то целых отраслей. Пусть будет свой ЦПК для финансовой сферы, свой ЦПК для здравоохранения, свой ЦПК для транспорта и энергетики, свои ЦПК... Радужные картины киберустойчивой России будущего начинают омрачаться, как только мы начинаем задумываться о конкретных опытах подобной централизации и спецификации работы в ИТ и ИБ. Ниже представлены лишь наброски размышлений, которые, конечно, не заменят полноценного моделирования с использованием математических моделей и аппарата теории игр, но в нашем случае будут достаточны для популярного разбора ключевых проблем централизации на конкретных примерах.

ПРОБЛЕМА № 1

Неустойчивость централизации и полезность избыточности. В своё время автора поразила красота и простота аргументации необходимости избыточности ресурсов в любой сфере, приведённая Томом Демарко в не переведённой на русский язык книге Slack, Getting Past Burnout, Busywork, and the Myth of Total Efficiency. В ней на конкретных примерах, со ссылками на различные исследования и эмпирический опыт Демарко и его коллег, приводилась важность проектирования таких систем управления и такой организации процессов, которые обладают «избыточным» запасом прочности и не стремятся к 100% эффективности, а наоборот, содержат в себе «лишних» специалистов, «избыточные» компетенции и «неэффективные» каналы связи. И это оказывается оправдано, потому что, как только мы начинаем смотреть на динамику устойчивости системы «вдолгую», оказывается, что именно избыточность позволяет системе быть по-настоящему эффективной.

Почему? Это можно понять, изучая международный опыт реагирования системы здравоохранения на вызовы, брошенные COVID-19, когда оказалось, что после реинжиниринга и сокращения неэффективных мощностей эта достаточно централизованная система не вполне способна справиться с пиковыми нагрузками и нуждается в перестройке, кадрах и дополнительных ресурсах, до этого сокращённых и укрупнённых. Оказалось, что идея концентрировать все необходимые компетенции и технологии в незначительном количестве критичных узлов — областных или региональных больниц — снижает системную устойчивость здравоохранения, и если происходит маловероятное, но неизбежное в долгосрочной перспективе событие, то система встаёт на дыбы (специалистов и оборудования не хватает, возникают накладочки с логистикой...) и формируется кризисная ситуация. Не произойдёт ли подобное с ИБ? И уверены ли мы, что готовы жить с подобными рисками в областях, связанных с КИИ?

С другой стороны, ЦПК действительно мог бы быть полезным тем, у кого сейчас нет ресурсов, чтобы полноценно заниматься ИБ и для кого хоть какое-то ИБ лучше, чем его полное отсутствие. Но эта полезность могла бы проявляться в том числе и в том, что внутри ЦПК существовала бы подсистема обучения внутренних специалистов «подшефных» организаций, которая работала бы на «доращивание» зрелости собственных процессов «клиентов» ЦПК. Если фантазировать дальше, то такая подсистема могла бы помогать с подбором штатных специалистов за счёт контактов в профильных вузах, предоставлять доступы к базе знаний, организовывать профильные конференции и в целом стремиться «не дать человеку рыбу», а «научить человека ловить рыбу». Естественно, что в такой парадигме речь идёт не о коммерческой активности, а о совершенно некоммерческом инфраструктурном проекте, который приносит не прямые финансовые выгоды и является чем-то вроде долгосрочных инвестиций в качество общественно необходимой среды.

ПРОБЛЕМА № 2

Мотивация и вовлечённость участников, а также уровень качества сервисов (SLA). Мы все пользуемся централизованными сервисами, и такие проекты, как, например, «Госуслуги», сэкономили миллионы человеко-часов, которые раньше тратились на стояния в очередях, заполнение тысяч непонятных бумажек и фрустрацию от того, что ты не знаешь, что делать, куда идти и кого спросить. Подобные системы — безусловное благо и большое

достижение нашего государства. Но бывают у них и оборотные стороны. Порой качество сервиса оставляет желать лучшего, обратная связь собирается с ошибками, а для того чтобы предложить или внести какие-то изменения, необходимо пройти тысячи согласований, зачастую безрезультатно. В результате адаптивность системы к потребностям пользователей снижается, что приводит к негативным последствиям в областях, где требуется повышенная скорость реагирования и возможность относительно быстро скорректировать принципы работы или какие-то отдельные элементы системы. Отсюда важность проектирования такого органа управления ЦПК, который позволял бы непосредственным пользователям (или клиентам) давать обратную связь, которую невозможно проигнорировать.

Каким образом можно организовать подобные механики управления? Например, через создание ассоциации или СРО, контролирующей деятельность ЦПК. Механизмы подобного контроля могут быть аналогичны предложениям экспертной группы Ассоциации российских банков³ в части регулирования аутсорсинга, сформированных по мотивам соответствующего доклада Банка России от декабря 2022 года. Если не сделать чего-то подобного, то высока вероятность снижения качества работы ЦПК, а главное — его немотивированность в получении и обработке обратной связи от собственных пользователей, что, согласитесь, неприемлемо и негативно повлияет на пресловутый SLA. Подобный механизм вкупе с предложенным выше механизмом «подсистемы обучения» внутренних специалистов подключаемых организаций позволит в полной мере реализовать исходную цель проекта — дать подключаемым к ЦПК организациям возможность по-настоящему повысить уровень ИБ. А регулярная отчетность, прозрачность процессов, возможность организаций-участников по достижении нужного уровня зрелости отключиться от ЦПК, перейдя на самообеспечение, — защиту системы от вырождения и бюрократизации, а главное — повысит вовлеченность и мотивированность организаций-участников, без активной позиции которых в процессе ни одна самая квалифицированная ЦПК не достигнет поставленной перед ней цели. Ведь любой аутсорсинг всё равно упирается во внутреннюю мотивацию пользователя этого аутсорсинга, и против воли пользователя его не спасёшь. А какая будет воля и мотивация у участников, если ЦПК окажется добровольно-принудительным,

полностью директивным упражнением? Вопрос риторический.

РЕЗЮМЕ

Идея ЦПК и проблема аутсорсинга ИБ становятся всё более актуальными, но вместе с тем мы не должны забывать про наш исторический опыт, про общие соображения теории управления и про нашу главную цель — повышение реального уровня ИБ финансовой (и не только финансовой!) отрасли. Кажется, что с высоты наших знаний и опыта спор сторонников и противников централизации утрачивает свою остроту и выбор должен быть сделан в пользу смешанной системы. Некоторые контуры этой системы можно обрисовать уже сейчас:

1. На вершине государственные органы, которые создают инфраструктуру требований и формируют «центр управления полетами» в масштабах страны, — ФСБ и НКЦКИ;

2. На следующем уровне отраслевые ЦПК, управляемые коллегиально с помощью ассоциаций и СРО, при ресурсной поддержке государства, и коммуницирующие с НКЦКИ;

3. И в самом низу — собственные службы ИБ организаций⁴, которых становится не меньше, а больше и которые при поддержке ЦПК стремятся ко всё более высокому уровню зрелости и автономности, чтобы по возможности из состояния полного аутсорсинга ИБ перейти в состояние хотя бы частичной полноты внутренних компетенций и симбиоза с ЦПК.

И хотя такая система может показаться кому-то «избыточной» и «неэффективной», именно она наилучшим образом обеспечивает достижение главной цели — устойчивости и надёжности функционирования всей системы, сочетая в себе все преимущества «централизации» и «децентрализации» и нивелируя их недостатки. Да, построить и поддерживать такую систему сложнее и дольше, чем уходить в одну из крайностей, но именно это, по мнению автора, и является показателем зрелости процессов управления. И именно этот, смешанный, паттерн мы видим в наиболее устойчивых системах — природных экосистемах — эталонных с точки зрения красоты и целесообразности.

⁴ Любопытно, но похожий тренд мы можем увидеть на примере вооружённых сил, которые несмотря на ассоциации с централизацией и иерархией многократно прибегали к смешанным формам — партизанским отрядам времен Великой Отечественной войны; группам казаков, занимавшихся колонизацией Сибири и Дальнего Востока; доктрине сетцентрической войны — в которых элементы централизации соседствуют с автономными или полуавтономными элементами, при чем баланс между ними может динамически изменяться, в зависимости от обстоятельств.

³ <https://disk.yandex.ru/i/qa6w7MPUYenz2w>

**Павел ЛУЦИК**директор по развитию бизнеса
и работе с партнерами,
КриптоПро

ПОЛНОЦЕННАЯ ЗАМЕНА

В КРИПТОПРО РАЗРАБОТАЛИ ОТЕЧЕСТВЕННЫЙ HSM-МОДУЛЬ

В части импортозамещения в банковской сфере крайне важным и актуальным сегодня является вопрос импортозамещения аппаратных модулей безопасности платежных систем (HSM-модулей), предназначенных для обеспечения криптографической защиты чувствительной информации, обрабатываемой в платежных системах, и безопасного хранения криптографических ключей. HSM-модуль является ключевым и одним из самых сложных элементов платежных систем, в том числе Национальной Системы Платежных Карт (НСПК). Поэтому создание и импортозамещение этих модулей является фундаментальным элементом нашей национальной технологической независимости и бесперебойности функционирования финансовой системы. И после ухода из России компании Thales — крупнейшего производителя платежных HSM, с помощью HSM-модулей которого осуществляется более 80% мирового объема транзакций по платежным картам, в том числе крупнейшими российскими банками, — требование импортозамещения данных модулей стало объективной реальностью, подкрепленной требованиями отечественных регуляторов.

Ещё до ухода Thales из России, в Положении Банка России от 4 июня 2020 г. N719-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты

информации при осуществлении переводов денежных средств» было закреплено требование о том, что с 1 января 2024 года в национально значимых платёжных системах должны использоваться только HSM-модули, реализующие иностранные, либо российские и иностранные криптографические алгоритмы, и имеющие подтверждение соответствия требованиям, установленным ФСБ России. Поддержка иностранной криптографии в данном случае обусловлена необходимостью обеспечения совместимости при обслуживании платежных карт международных платежных систем, в первую очередь Visa и MasterCard, которые, однако, в прошлом году также покинули российский рынок.

Во исполнение 719-П ФСБ России и Банком России совместно разработаны и опубликованы на официальных сайтах соответствующие требования к HSM-модулям и иным элементам платежной системы, функционирующим совместно с ними — банкоматам, платежным терминалам и т.д. (утв. ФСБ России 24.01.2020, 28.02.2020 N ФТ-56-3/32).

Как указано выше, данные требования регуляторов появились заблаговременно, еще до ухода Thales из России. И, как показали события прошлого года, это был оправданный, стратегически продуманный шаг со стороны регуляторов, позволивший финансовым организациям и отечественным производителям HSM-модулей подготовиться к возможным негативным сценариям, некоторые из которых мы как раз сейчас наблюдаем.

Еще один важный момент — со своим уходом компания Thales полностью прекратила поставки оборудования и техническую поддержку HSM-модулей, которые были поставлены в Россию. И в ближайшие несколько лет это может привести к тому, что устройства начнут выходить из строя без возможности их ремонта внутри страны, из-за того, что они конструктивно являются неразборными. По сути, отсутствие технической поддержки и прекращение поставок приводит к тому, что отдельные кредитные организации уже сейчас начинают испытывать серьезные трудности в этом вопросе. Поэтому вопрос замены HSM-модулей на российские становится еще более актуальным.

Для разрешения сложившейся ситуации создана и функционирует рабочая группа в составе Банка России, НСПК, основных банков РФ, компаний-разработчиков процессингового ПО и HSM-модулей, идет активное тестирование модулей, большинством банков проведено тестирование на программных эмуляторах, наращивает обороты тестирование аппаратных модулей, после которого можно будет уже приступить к промышленной эксплуатации. И мы надеемся, что к 1 января 2024 года российские аппаратные модули займут свое достойное место в Национальной платежной системе.

Уже сейчас технически все для этого готово. В частности, специалистами КриптоПро разработан HSM-модуль, который предоставляет возможность полноценной замены (как по функционалу, так и по производительности) соответствующих модулей

иностранный производства (в том числе HSM-модулей Thales) в действующих схемах подключения в рамках функционирования информационных систем участников финансового рынка:

- ♦ банков — эмитентов платёжных карт;

- ♦ банков, осуществляющих эквайринг платёжных карт;

- ♦ процессинговых центров операторов платёжных систем.

HSM-модуль от КриптоПро разработан на основе программно-аппаратного криптографического модуля

«КриптоПро HSM» версии 2.0, который был дополнен программным модулем безопасности для систем платёжных карт, разработанным в соответствии с Положением Банка России от 4 июня 2020 г. N719-П и PCI PTS HSM Modular Security Requirements.



Платёжный HSM реализует программно-аппаратный интерфейс поддержки операций системы платёжных карт, позволяя решать следующие задачи:

- ♦ Инициализация и эмиссия платёжных карт с магнитной полосой, бесконтактных и смарт-карт, включая генерацию PIN/CVC/CVP и печать PIN-конвертов, смену и проверку PIN и прочее.

- ♦ Управление ключами (и обеспечение безопасности ключей) на всех этапах жизненного цикла (включая генерацию, печать ключевых компонент, формирование ключей из компонент, диверсификацию ключей, импорт/экспорт и трансляцию).

- ♦ Обработка платёжных транзакций, банковских транзакций от платёжных устройств.

ПОДДЕРЖИВАЕМЫЕ АЛГОРИТМЫ

- ♦ Шифрование: 2DES, 3DES, AES
- ♦ Электронная подпись: RSA, ECDSA
- ♦ Хэш-функции: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, MD5, ISO 10118-2
- ♦ MAC: ISO 9797-1 MAC algorithm 1, ISO 9797-1 MAC algorithm 3, ANSI X9.19, CBC-MAC, CMAC
- ♦ Согласование ключей: ECDH

ФОРМАТЫ КЛЮЧЕЙ

- ♦ Key Block (в том числе ANSI X9 TR-31)
- ♦ ANSI X9.17
- ♦ Variant

ФОРМАТЫ PIN-БЛОКОВ

- ♦ ISO 9564-1 & ANSI X9.8 Format 0
ISO Format: 0, алгоритм: 2DES, 3DES
- ♦ ISO 9564-1 Format 1
ISO Format: 1, алгоритм: 2DES, 3DES

♦ Standard EMV 1996

ISO Format: 2, алгоритм: 2DES, 3DES

♦ Mastercard Pay Now & Pay Later

Алгоритм: 2DES, 3DES

♦ Visa/Amex new PIN only

Алгоритм: 2DES, 3DES

♦ Visa/Amex new & old PIN

Алгоритм: 2DES, 3DES

♦ ISO 9564-1 & ANSI X9.8 Format 3

ISO Format: 3, алгоритм: 2DES, 3DES

♦ ISO 9564-1 Format 4

ISO Format: 4, алгоритм: AES

ПРОИЗВОДИТЕЛЬНОСТЬ (НА ПРИМЕРЕ ОПЕРАЦИИ ТРАНСЛЯЦИИ PIN-БЛОКОВ)

- ♦ 10 000 tps на AES
- ♦ 20 000 tps на 3DES

ПОДДЕРЖИВАЕМЫЕ ТЕХНОЛОГИИ

- ♦ МИР
- ♦ Visa VIS, Visa VCP, Mastercard M/Chip, Mastercard MCBP, American Express AEIPS, JCB, Union Pay
- ♦ EMV 3.1.1, EMV 4.1, EMV 4.3
- ♦ Visa CVV, iCVV, CAVV; Mastercard CVC, Chip CVC, AAV
- ♦ IBM 3624 (IBM Offset)
- ♦ ABA PVV
- ♦ Mastercard CAP, Visa DPA
- ♦ Global Platform Secure Channel Protocol 2 (SCP02), Secure Channel Protocol 3 (SCP03); EMV Common Personalization Specification (EMV CPS)
- ♦ DUKPT (X9.24)



Алексей ПАРФЕНТЬЕВ
руководитель отдела
аналитики «СёрчИнформ»

«ЗАГЛЯНУТЬ ПОД КАЖДЫЙ КАМЕНЬ»

5 ПРИЧИН ИСПОЛЬЗОВАТЬ DLP ВМЕСТЕ С DСАР

Основная задача DLP-систем — борьба с утечками информации и защита от других внутренних инцидентов. Но, выстраивая защиту данных в компании, в первую очередь нужно понимать, как устроены бизнес-процессы и какая информация представляет ценность. Второй шаг — разобраться, где хранится эта информация и откуда может утечь. И только третий шаг — непосредственно защита.

Инструмент, который поможет на первых двух этапах, проанализирует информацию и категоризирует ее — это решение класса DСАР (Data-Centric Audit and Protection). Расскажу, почему DLP и систему для файлового аудита (DСАР) стоит использовать вместе.

ПРИЧИНА 1: БЫСТРЫЙ ПОИСК

DСАР-системы классифицируют все документы в компании по контенту. Они сканируют хранилища и вычитывают файлы, затем относят их к разным категориям: персональные данные, финансовая информация, договоры и т.д. Каждой

категории присваивается метка, она ставится на файл с заданным содержанием на уровне характеристик в файловой системе (т.е. вручную такую метку не удалить). Метка становится как бы «обложкой» для файла, которая сообщает DLP об уязвимом контенте.

DLP «СёрчИнформ КИБ» бесшовно интегрируется с нашей же DСАР «СёрчИнформ FileAuditor». В одном интерфейсе можно настроить правила классификации, по которым DСАР разметит документы, а затем политики безопасности в DLP на основе этих меток.

Метки заменяют длинные «поисковые запросы» внутри политик и ускоряют быстрое действие DLP, потому что ей не приходится самостоятельно «сканировать» каждый файл. Настройка сводится к двум кликам: например, оповещать об инциденте, если в канале «мессенджеры» пересылают файл с меткой «ПДн».

ПРИЧИНА 2: ПРОФИЛАКТИКА СЛУЧАЙНЫХ ИНЦИДЕНТОВ

Если конфиденциальные документы хранятся хаотично, доступны тем, кому

не нужны по прямым обязанностям — это риск, что кто-то прочтет их из любопытства или «расшарит» по незнанию. DСАР позволяет контролировать, чтобы данные хранились «как надо»: показывает, где лежат самые уязвимые данные, и кто имеет к ним доступ. Так ИБ-специалисту проще скорректировать пользовательские права доступа и убрать лишнее из общих папок.

DLP в свою очередь ищет кто и как нарушает или пытается нарушить правила. Таким образом, DСАР-система сужает для DLP фронт работ.

ПРИЧИНА 3: ВЫЯВЛЕНИЕ ОРГАНИЗАЦИОННЫХ ПРОБЛЕМ

DСАР дополняет картину инцидента тем, что невозможно отследить с DLP. Представим ситуацию, что у сотрудника нашелся не предназначенный ему документ, но DLP не увидела передачу файла. Как документ к нему попал, прояснит DСАР: покажет, что файл лежал в общей папке, а пользователь скопировал его к себе на ПК. В FileAuditor за это отвечают аудит прав доступа и журнал операций с файлами.

Файловый аудит выявляет организационные проблемы и нарушения правил работы с информацией. Людям всегда удобнее сделать копию грифованного документа, чтобы потом использовать как шаблон, хранить ее у себя на ПК, а не в специальной папке на сервере, чтобы была под рукой.

DСАР позволяет контролировать, чтобы данные хранились «как надо»: показывает, где лежат самые уязвимые данные, и кто имеет к ним доступ. Так ИБ-специалисту проще скорректировать пользовательские права доступа

Понимание таких «коротких путей», которыми идут сотрудники в обход регламентов, помогает эффективнее настроить контроль с DLP.

ПРИЧИНА 4: УПРАВЛЕНИЕ ДОСТУПОМ К КОНТЕНТУ

Почти в любых DLP есть механизм eDiscovery для работы с данными в покое. Он хорош для простого поиска файлов, но не чтобы разобраться с правами доступа или действиями пользователей с информацией.

DCAP-решения разрешают/запрещают операции с файлами и доступ к местам их хранения. Это можно сделать вручную средствами ОС, но удобнее — в одном интерфейсе, а не в каждой директории отдельно. «СёрчИнформ FileAuditor» идет еще дальше и регулирует способы работы с данными. Например, для организаций из финансового сектора с 2023 года ввели ограничения: платежную информацию и персональные данные клиентов им нельзя передавать в мессенджерах даже для рабочих нужд. В FileAuditor можно настроить запрет на пересылку файлов с метками — в данном случае «ПДн» и «Платежная информация» (эти правила классификации преднастроены) — через выбранные мессенджеры и в любом другом приложении. Программы просто не смогут вычитать такие документы из файловой системы, это уникальный функционал FileAuditor.

DLP в этом случае выявляет более сложные схемы инсайдеров. Когда FileAuditor запретит пересылку конфиденциального документа, КИБ подстрахует от «расшаривания» пользователем отдельных критичных отрывков из него где-нибудь в соцсети. Нестандартные каналы утечки тоже будут под контролем. Например, КИБ распознает наведение смартфона с камерой на экран ПК. Для этого система задействует веб-камеру на ПК сотрудника, съемку можно включать принудительно, когда запускается критичный процесс (например, CRM) или открывается конфиденциальный документ.

То есть связка DLP+DCAP дает комплексный контроль и позволяет настраивать запреты максимально гибко. К тому же в обеих программах есть аудит блокировок — ИБ-служба всегда будет знать, кто пытался обойти ограничения.

В FileAuditor можно настроить запрет на пересылку файлов с метками через выбранные мессенджеры и в любом другом приложении. Программы просто не смогут вычитать такие документы из файловой системы

ПРИЧИНА 5: РАЗВИТИЕ КУЛЬТУРЫ ИБ

Возможности DCAP и DLP помогают дисциплинировать коллектив. В «СёрчИнформ КИБ» можно информировать пользователя о правилах ИБ с помощью специального интерфейса. Он уведомляет о блокировках и дает сотруднику возможность запросить доступ к необходимым ему устройствам и документам. DCAP, в свою очередь, подсказывает пользователю, насколько информация в документе конфиденциальна.

Мы внедрили видимые метки указанием уровня доступа, которые сотрудники могут самостоятельно расставлять на документы. Например, руководство готовит новые регламенты работы с поставщиками — и может поставить на инструкцию метку «Для служебного пользования». FileAuditor автоматически контролирует, что «ручные» метки расставлены правильно (скажем, что договоры с клиентами имеют гриф «Конфиденциально»). Постановку этих

меток можно сделать обязательной: без них документ не получится отправить или сохранить.

В результате системы приучают пользователей анализировать контент и самим делать выводы, что он требует защиты. Сотрудники в курсе, что ведется контроль, это тоже дисциплинирующий фактор. Это страховка от инцидентов «по незнанию», а если пользователь проигнорировал предупреждения системы — подтверждение, что нарушение было намеренным.

ИТОГО

DLP и DCAP дополняют и усиливают друг друга. Со связкой систем критичные нарушения станут реже, ведь ИБ-специалистам не придется разбираться с хаосом: неправильным хранением данных, избыточными правами доступа, нежелательными операциями с файлами. Значит, станет меньше пользовательских ошибок и лазеек для инсайдеров, эффективность защитыкратно вырастет.

Попробуйте решения «СёрчИнформ» для комплексной защиты конфиденциальных данных. Это бесплатно на 30 дней.



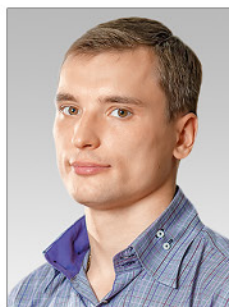
DLP «СёрчИнформ КИБ»



DCAP «СёрчИнформ FileAuditor»



Иван ЧЕРНОВ
менеджер по развитию
UserGate



Артём ТУРЕНОК
руководитель отдела
технических решений
АО «ДиалогНаука»

КОНКУРЕНТ ЗАРУБЕЖНЫМ АНАЛОГАМ

КАК ЗАЩИТИТЬ ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ
С ПОМОЩЬЮ РОССИЙСКОГО МЕЖСЕТЕВОГО ЭКРАНА
НОВОГО ПОКОЛЕНИЯ

N GFW (Next Generation Firewall) изменили парадигму оперативного контроля внешнего сетевого трафика, предоставив компаниям возможность отсекаать пакеты данных из определённых источников, а также анализировать сами передаваемые данные, проверять их на наличие вредоносных сигнатур и ограничивать работу с нежелательными ресурсами. Рассмотрим функции современного межсетевого экрана на примере отечественного представителя систем этого класса UserGate Next Generation Firewall.

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ USERGATE NEXT GENERATION FIREWALL

Набор функциональных возможностей UserGate Next Generation Firewall охватывает разнообразные потребности в сфере защиты трафика и фильтрации контента. Гибкие механизмы настройки межсетевого экрана позволяют выстраивать сложные логические схемы обработки данных и в автоматическом режиме реагировать на потенциально опасные или нелегитимные действия.

Кратко остановимся на наиболее важных аспектах работы UserGate Next Generation Firewall.

ФИЛЬТРАЦИЯ КОНТЕНТА ПО ПРАВИЛАМ

Фильтрация трафика в UserGate Next Generation Firewall основывается на механизме правил — по сути, политик безопасности, описывающих действия системы при наступлении тех или иных заданных условий. Правила фильтрации могут блокировать или, наоборот, разрешать движение данных в зависимости от их типа, источника, получателя, приложения, категории и других параметров. Правила могут применяться к одному или нескольким пользователям и выполняются последовательно, что даёт возможность строить гибкую систему обеспечения кибербезопасности и осуществлять контроль работы сотрудников.

При помощи правил можно не только создавать белые и чёрные списки ресурсов, но и контролировать множество параметров передаваемых пакетов, например тип используемого браузера, наличие определённых словосочетаний или

типов информации. Правила используются не только для фильтрации контента, но и в других функциональных блоках системы — межсетевом экране, подсистеме ограничения пропускной способности и пр. Пример настройки правил контентной фильтрации представлен на рисунке 1.

АНАЛИЗ ТРАФИКА

Глубокий разбор трафика является ключевой функцией NGFW и основным источником данных для других подсистем. UserGate Next Generation Firewall способен детально исследовать нагрузку каждого передаваемого пакета, на лету определяя потенциально небезопасное содержимое, а также триггеры, по которым активируются заранее заданные правила и сценарии. Помимо обычного трафика, система расшифровывает и защищённые SSL-пакеты (рис. 2), работая с протоколами HTTPS, SMTPS и POP3S. При этом сервер NGFW осуществляет подмену оригинального сертификата на собственный, отдавая на сторону пользователя по-прежнему защищённый контент.

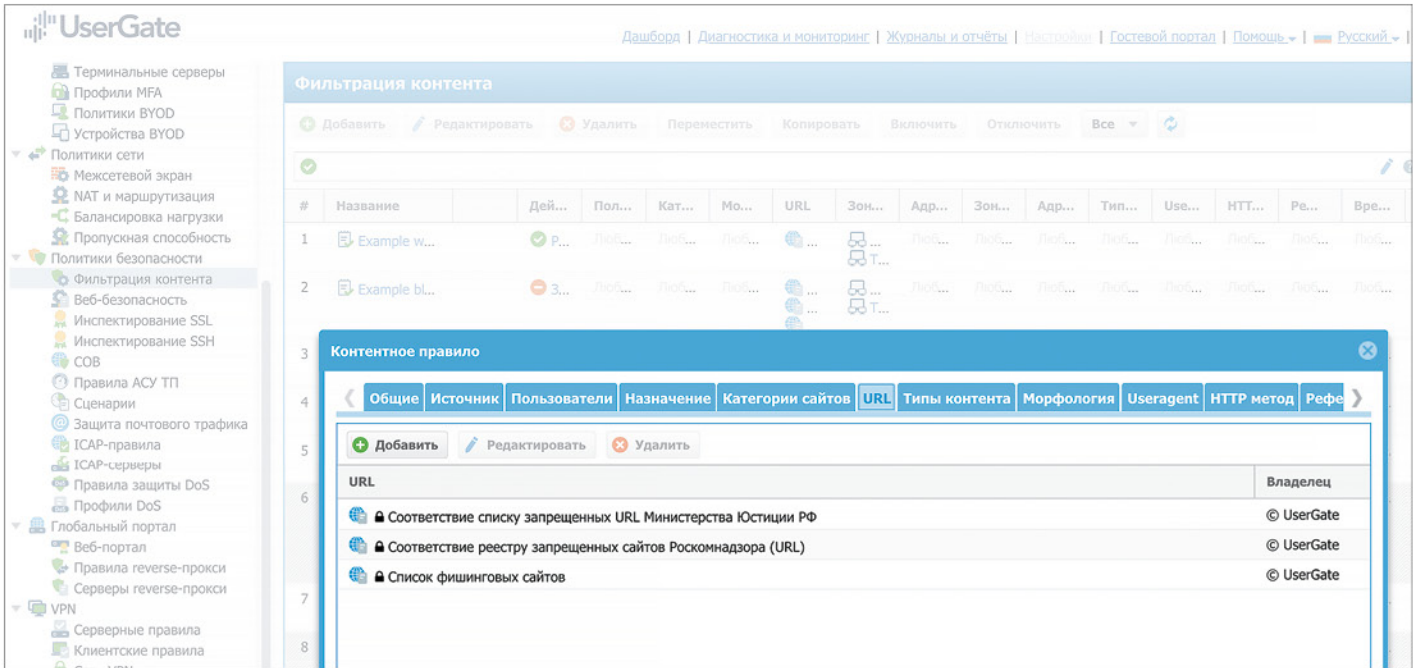


Рисунок 1. Пример настройки правила контентной фильтрации

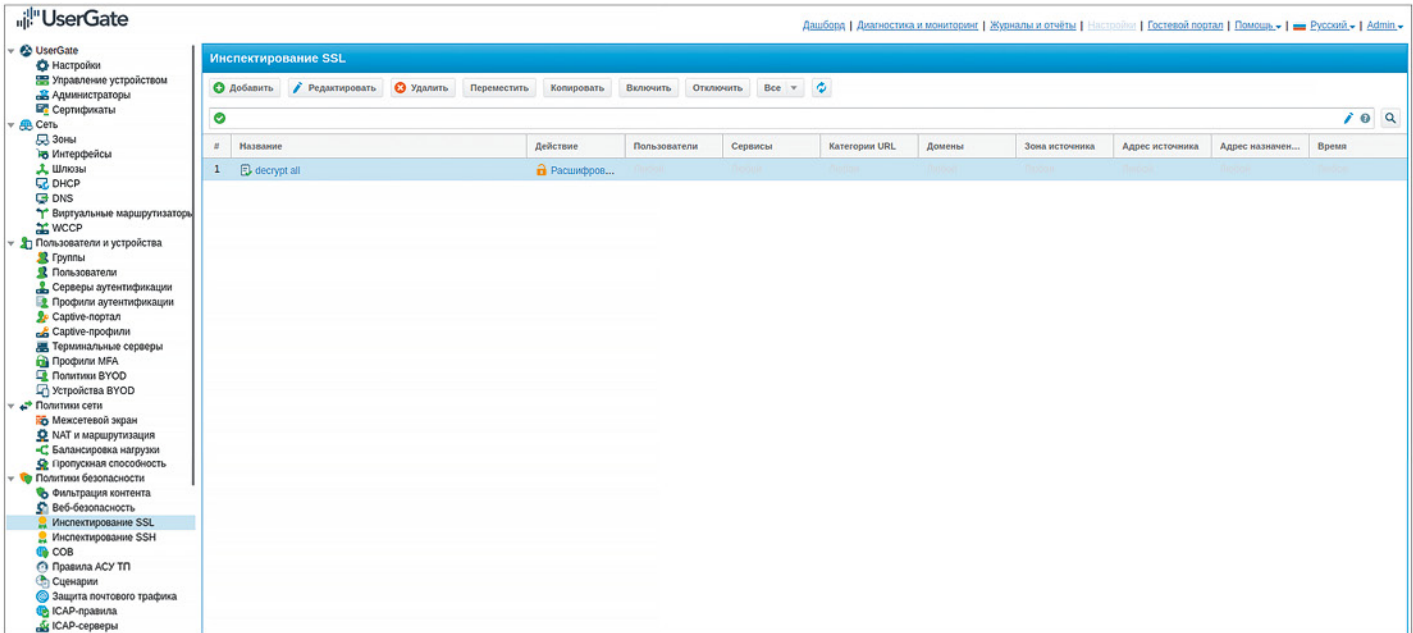


Рисунок 2. Раздел настройки «вскрытия SSL-трафика»

ЗАЩИТА ОТ DOS

Одним из механизмов безопасности в UserGate Next Generation Firewall является функция ограничения числа соединений, открытых одним пользователем. Так же, как и многие другие элементы NGFW, она реализована при помощи механизма правил и сценариев, что позволяет гибко настраивать чувствительность системы в соответствии с особенностями конкретной компании. Ограничение на

количество одновременно открытых пользователем сеансов обеспечивает эффективное противостояние возможным DoS-атакам (Denial of Service) через пользовательские или гостевые учётные записи.

КОНТРОЛЬ ИНТЕРНЕТ-ПРИЛОЖЕНИЙ

UserGate Next Generation Firewall работает с приложениями на седьмом уровне сетевого взаимодействия модели

OSI. Система идентифицирует более 1000 приложений (рис. 3) и даёт администратору возможность ограничивать их использование. Например, NGFW способен полностью заблокировать работу мессенджеров, торрент-клиентов (рис. 3) и других нежелательных программ. Собственная база обновляемых сигнатур позволяет, помимо этого, защищать локальную сеть от угроз, связанных с теми программами, которые работают с интернетом.

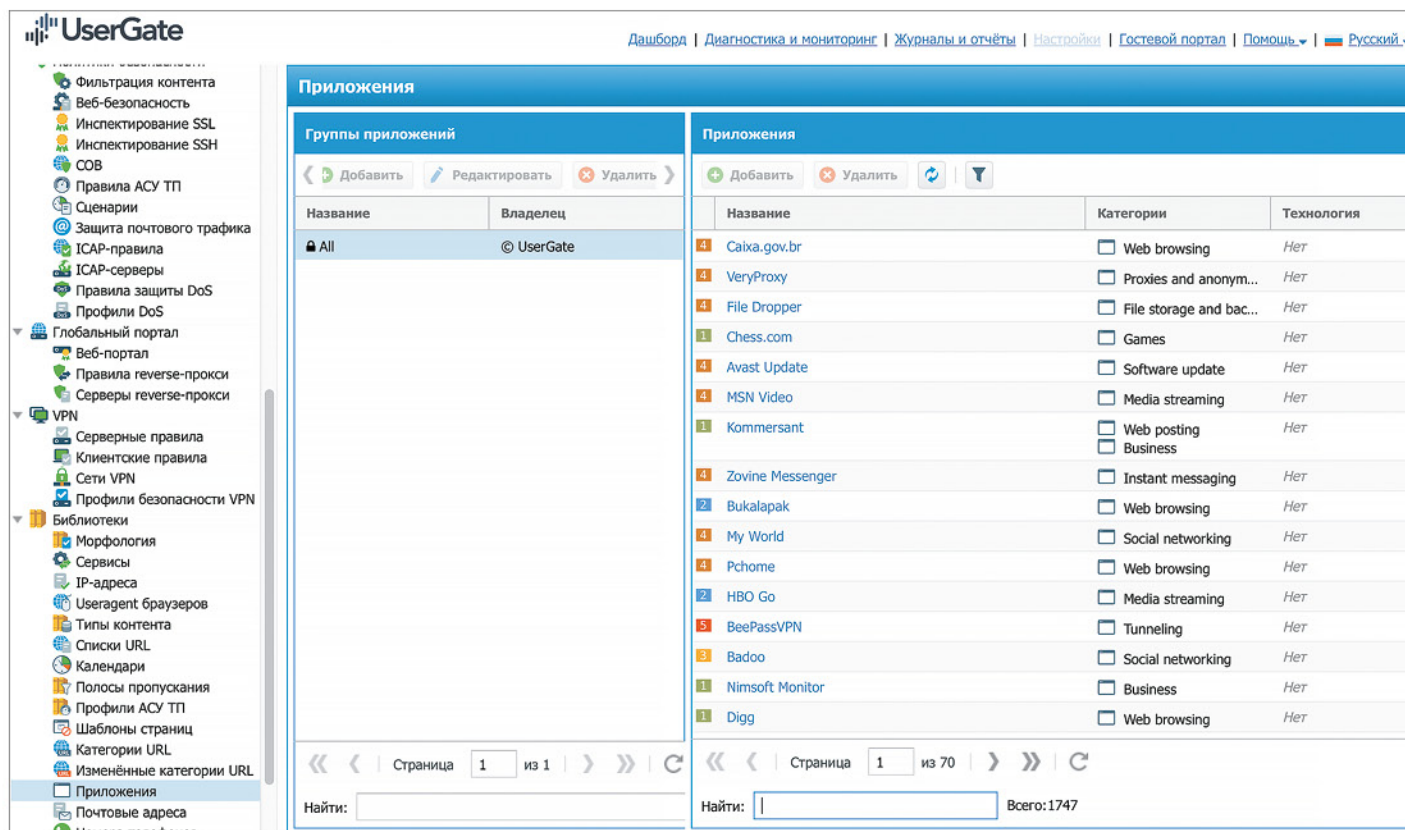


Рисунок 3. Список доступных приложений

АНТИВИРУС

В состав UserGate Next Generation Firewall входит потоковый антивирус, который может проверять внешний трафик на наличие вредоносных программ. Анализ ведётся при помощи собственной базы сигнатур, что обеспечивает достаточную надёжность и блокировку основных угроз до того, как данные пересекут контур безопасности. С другой стороны, использование лёгкого сигнатурного антивирусного ядра минимально нагружает систему, что даёт возможность при необходимости проверять весь трафик полностью. Антивирусная защита использует механизм правил безопасности NGFW.

РЕАГИРОВАНИЕ

В UserGate Next Generation Firewall встроена система предотвращения вторжений, которая способна в настоящее время реагировать на атаки киберпреступников, эксплуатирующих известные уязвимости. UserGate Next Generation Firewall даёт администратору возможность создавать различные наборы сигнатур для защиты

различных сервисов, а также формировать на базе универсального механизма правил собственные сценарии для каждого типа трафика. Это позволяет не только формировать реакции на кибератаки, но и контролировать вредоносную активность внутри сети.

СОБСТВЕННАЯ ОС

В основе UserGate Next Generation Firewall лежит оригинальная операционная система UGOS, оптимизированная для задач быстрой и эффективной обработки трафика. Платформа создана на базе дистрибутива Linux и не использует готовых комплексных модулей: все подсистемы безопасности разработаны программистами UserGate и не содержат стороннего кода. С одной стороны, это позволяет быстро адаптировать её под требования заказчика, а с другой — существенно снижает вероятность атак на систему с использованием общеизвестных уязвимостей.

ВАРИАНТЫ ПОСТАВКИ

UserGate Next Generation Firewall может поставляться как в виде виртуального межсетевого экрана, развёрнуто-

го на одном из гипервизоров (VMware, Hyper-V, Xen, KVM, OpenStack, VirtualBox, отечественные разработки), так и в виде программно-аппаратного комплекса, созданного UserGate. Производитель предлагает несколько вариантов исполнения таких NGFW, предназначенных для организаций разного масштаба — от компаний сегмента СМБ до крупных предприятий и дата-центров.

ВЫВОДЫ

UserGate Next Generation Firewall занимает передовые позиции в секторе NGFW российского рынка информационной безопасности и может конкурировать с ведущими зарубежными аналогами. Компетенции компании UserGate в сфере анализа сетевого трафика позволили ей создать зрелый продукт, способный стать существенным препятствием для кибератак, универсальным инструментом первой необходимости, который сможет обезопасить компанию от большого числа инцидентов даже при частичной недоступности других инструментов информационной безопасности.



Лев ЯКУБОВИЧ
эксперт в области
информационной
безопасности,
коммерческий
директор ГК «ЦИБИТ»

ОСТОРОЖНО, МОШЕННИКИ!

ПРИНЦИПЫ ДЕЙСТВИЯ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ И МЕТОДЫ ЗАЩИТЫ

По данным комитета Госдумы РФ по финансовому рынку, в 2022 году в России на 40% увеличилось количество мошеннических действий с использованием методов социальной инженерии (в сравнении с 2021 годом). Эксперты Группы компаний «ЦИБИТ» отмечают: чаще всего злоумышленники получают доступ к информации из-за низкой грамотности сотрудников компаний в области кибербезопасности — работники сами передают свои и клиентские персональные данные хакерам. В этой статье расскажем об основных типах атак с использованием методов социальной инженерии и о том, как от них защититься.

ТИПОЛОГИЯ АТАК

Социальная инженерия — это вид атаки с применением механизмов психологического манипулирования, влияния или обмана жертвы с целью получения контроля над компьютером либо кражи личной и финансовой информации. В процессе такой атаки злоумышленники используют «слабые места» человеческой психологии, заставляя жертву выполнить нужное действие или раскрыть секретные данные.

С примерами социальной инженерии сталкивался каждый из нас: это и электронные письма с вредоносными вложениями или всевозможными

ссылками (на веб-ресурсы, на скачивание различных приложений или на фотографии), и «звонки из банка» с требованием предоставить информацию.

В арсенале кибермошенников сегодня огромное количество самых разных техник социальной инженерии. ГК «ЦИБИТ» обладает экспертизой в области информационной безопасности: уже более 13 лет мы работаем в отрасли, в том числе проводим социотехнические тестирования (пентесты) для клиентов. Специалисты «ЦИБИТ» констатируют: основными схемами социальной инженерии являются фишинг, вишинг и байтинг. Поговорим о каждом подробнее.

Фишинг. Фишинг (от англ. fishing «рыбная ловля») — это рассылка мошеннических электронных писем со ссылками или вложенными файлами, которые создают впечатление, что они направлены из надёжного источника. Такие сообщения, как правило, содержат ссылки, ведущие на поддельные сайты или устанавливающие вредоносное программное обеспечение.

Основная цель фишинговых писем — обман пользователя с целью получения доступа к его учётным данным, личной или финансовой информации. Другой задачей такого сообщения может быть установка на компьютер сотрудника вредоносного ПО для последующей эксплуатации этого компьютера.

Отметим, что чаще всего жертвами фишинга становятся менее подготовленные в области информационной безопасности службы и сотрудники организации. В первую очередь, это бухгалтерия, кадровый отдел, финансовые и юридические подразделения компаний.

Вишинг. Ещё один популярный вид социальной инженерии — вишинг (от англ. vishing, от voice fishing — голосовой фишинг). В этой технике злоумышленник звонит жертве и разговаривает с ней по телефону от имени сотрудника компании (например, банка). Чаще всего такие звонки замаскированы под звонки от специалистов службы безопасности, системных администраторов и т.п.

В основе этого типа атаки лежит доверие людей к финансовым организациям, силовым структурам и государственным учреждениям (таким как банки, МВД, налоговая служба и т.п.).

Байтинг. Байтинг (от англ. bait — наживка) — это техника социальной инженерии, в которой используются различные «приманки», например, USB-устройство с вредоносным содержанием. В основе механики атаки лежит любопытство пользователя или мотив жадности.

Стоит отметить, что такой вид атаки не всегда приносит желаемый успех мошенникам — нет никаких гарантий, что USB-устройство достанется жертве и будет запущено на рабочем компьютере.

Изучая статистику совершения атак методами социальной инженерии, а также опираясь на практику социотехнических тестирований, которые проводят эксперты ГК «ЦИБИТ» для компаний-клиентов, мы видим, что главным фактором успешности таких мошеннических действий является недостаточная грамотность пользователей в области защиты информации, доверчивость сотрудников организаций. Примерно каждый десятый работник переходит по ссылкам из фишинговых писем, в результате чего открывается несанкционированный доступ к учётным данным и появляется возможность воспользоваться корпоративными ресурсами, содержащими конфиденциальную информацию.

МЕТОДЫ ЗАЩИТЫ

Специалисты «ЦИБИТ» комментируют: не существует единого механизма безопасности, который мог бы защитить организацию от методов социальной инженерии. С каждым днём хакеры придумывают новые уловки, с помощью которых осуществляется воздействие на людей.

Мы подготовили несколько рекомендаций для компаний, которые могут быть использованы для предупреждения и предотвращения атак с использованием механик социальной инженерии:

- ♦ Регулярное проведение тестирования на проникновение с использованием методов социальной инженерии. Это поможет службе безопасности компании узнать, какие типы пользователей представляют наибольший риск для конкретных типов атак, а также определить, какие сотрудники нуждаются в дополнительном обучении.

- ♦ Обучение сотрудников и повышение осведомлённости персонала в области информационной безопасности. Если пользователи знают, как выглядят атаки социальной инженерии, они с меньшей вероятностью попадутся на уловки мошенников.

- ♦ Проведение учений на предприятии с имитацией различных ситуаций атак. В процессе таких учений сотрудники компании отрабатывают модели поведения в той или иной рискованной ситуации и учатся на практике применять знания, полученные во время обучения.

- ♦ Внедрение почтовых и веб-шлюзов для сканирования электронной почты на наличие вредоносных ссылок и их фильтрации — такая мера снижает вероятность того, что сотрудник осуществит переход по ссылке.

- ♦ Поддержание антивирусного ПО в актуальном состоянии для предотвращения установки вредоносных программ в фишинговых письмах.

- ♦ Регулярное обновление ПО.

ГК «ЦИБИТ»: ПРОФЕССИОНАЛЬНЫЕ РЕШЕНИЯ В ОБЛАСТИ ИБ

Работая в сфере защиты информации уже более 13 лет, мы убеждаемся: самым эффективным решением для предупреждения атак с использованием методов социальной инженерии является постоянное повышение грамотности в области информационной безопасности, обучение сотрудников тому, как распознавать инциденты и реагировать на них, а также проведение на предприятии учений и социотехнических тестирований.

Специалисты «ЦИБИТ» готовят высококвалифицированные кадры в области защиты информации в собственном учебном центре «ЦИБИТ», проводят аудиты информационной безопасности и тестирования на проникновение, реализуют полный комплекс услуг по проектированию, поставке и пуско-наладке различных средств и систем защиты информации.

Департамент проектов ГК «ЦИБИТ» оказывает услуги по проведению тестирований на проникновение (оценка защищенности ИТ-инфраструктуры), в том числе с использованием методов социальной инженерии.

Тестирование на проникновение (пентест) — это имитация действий злоумышленников, направленная на получение доступа к конкретным конфиденциальным данным через обнару-

жение и последовательную эксплуатацию цепочки уязвимостей.

Пентест является наиболее реалистичным методом, показывающим на практике, насколько эффективны внедренные системы и меры безопасности. В отличие от реальной хакерской атаки, целью такого тестирования не является нанесение ущерба компании, все действия находятся под контролем специалистов.

Учебный центр «ЦИБИТ» предлагает большой спектр обучающих курсов в области защиты информации, в том числе для общего повышения грамотности в сфере кибербезопасности и цифровых технологий.

Основные направления Учебного центра «ЦИБИТ»:

- ♦ Профессиональная переподготовка в области информационной безопасности;

- ♦ Повышение квалификации в области информационной безопасности;

- ♦ Бесконтактное обучение;

- ♦ Электронные курсы;

- ♦ Открытые вебинары.

Профессиональная цель ГК «ЦИБИТ» — совершенствование профессиональной среды и стремление задавать вектор развития для структур, работающих в сфере информационной безопасности.

Глобальная цель ГК «ЦИБИТ» — через формирование понимания необходимости защиты информации в современном мире делать жизнь общества более безопасной и комфортной, делиться своими знаниями и опытом для развития способности общества более гибко, оперативно и безболезненно реагировать на вызовы времени и справляться с ними.



ГРУППА КОМПАНИЙ
ЦИБИТ

**МЫ ПОМОГАЕМ
СООТВЕТСТВОВАТЬ
ТРЕБОВАНИЯМ!**

Телефон: +7 (495) 792-80-80

E-mail: info@cibit.ru

Сайт: www.cibit.ru



«МАГНИТКА»-2023

В этом году форум «Цифровая устойчивость и информационная безопасность России» — «Магнитка» — был посвящён технологической независимости и ИБ промышленных предприятий.

АНТИПЛЕНАРКА

«Почему мы до сих пор смотрим в рот регулятору, пытаюсь понять, что же он имел в виду в очередном приказе, положении, указании или стандарте? Почему мы, занимающиеся ИБ на практике, ждём, что регулятор лучше нас знает, как нам защищать наши активы?» — так анонсировали «Антиплениарку» организаторы и автор её концепции Алексей Лукацкий.

Предполагалось, что участники дискуссии покажут регуляторам кузькину мать, но эксперты не стали рвать на себе рубахи и разговор о регуляторной политике

в области ИБ прошёл достаточно конструктивно. В ходе дискуссии участники вспомнили, что существуют 180 требований ФСТЭК России и 400 — Банка России, часть из них избыточна и дублирует друг друга. И вопрос стоит не в количестве требований, а в их толковании и здравом смысле. Нужны отраслевые нормативы и простая форма подачи материала, исключающая двойную трактовку документа. К завершению «Антиплениарки» спор всё же вспыхнул. Зажжённой спичкой стала тема «Регуляторика или самоответственность?», которая так и не была погашена и периодически вспыхивала на других сессиях «Магнитки».

Подводя итоги, Алексей Лукацкий отметил единогласие экспертов в вопросах выполнения требований базовой ИБ, прописанной регуляторами, а также в политике нулевой толерантности, необходимости пентестов и программ Bug Bounty.

НЕ ПРО ПОЛИМЕРЫ

— Технологическая независимость лучше отражает суть явления импортозамещения, — заметил Рустэм Марданов, начальник Уральского главного управления Банка России, модератор панельной дискуссии «Технологическая независимость как основа информационной безопасности, или „Не про полимеры“». Он заявил о важности рассматриваемых вопросов: проблем, связанных с обеспечением технологической независимости в отношении средств и инструментов, позволяющих обеспечивать ИБ на предприятиях разного профиля; качества ПО, которое приходит на смену иностранному; сложностей, с которыми сталкиваются разработчики, вендоры и потребители. Отметил модератор и значительную роль вопросов государственного регулирования и поддержки.



— Процесс перехода на отечественные решения идёт полным ходом, внедряются решения, которые были разработаны до всех событий, и функционально многие из них даже совершеннее инструментов, предлагаемых на западном рынке, — считает начальник Уральского главного управления Банка России.

Однако, по мнению представителей промышленности, ситуация с технологической независимостью не столь радужная. Михаил Ермолаев, генеральный директор АО «Гринатом», и Виталий Александров, директор по цифровой трансформации АО «НПП «Исток» им. Шокина», отметили, что начали переход на отечественные решения задолго до 2022 г. И в большинстве случаев не нашли равноценной замены западному ПО. В результате чего специалисты «Гринатома» занимаются собственными разработками с учётом принципа *Secure by design*, «Росатом» создал полигоны и ведёт тестирование ПО и оборудования, чтобы понять, как интегрировать программные и аппаратные решения.

Будет сложно в срок — к 2025 году — перевести все объекты на отечественные системы, и предстоящие два года придётся жить в режиме постоянного тестирования и разработки, считает и Виталий Александров. Выпускающее электронику предприятие НПП «Исток» тестирует отечественные решения и не всегда может найти аналоги западным продуктам.

«Если какие-то решения и представлены, то некоторых функций у них нет или они находятся в процессе разработки, — отметил он. — Даже вендоры не могут дать дорожную карту, что

эти функции появятся, например, в 2024 году».

Виталий Александров положительно оценил инициативу правительства по созданию промышленных центров компетенции, где предполагается систематизация российского софта под разные отрасли и направления.

В промышленных центрах компетенции с лета 2022 года идут активные дискуссии по импортозамещению ERP-систем, отметил Вадим Феоктистов, директор «ММК-Информсервис». Крупные металлургические предприятия пока не видят возможности полноценного перехода на отечественные ERP-решения. По словам эксперта, такое готовое решение либо будет «длинным и дорогим», либо «оно будет содержать в себе одни кастомизации».

«Мы сейчас находимся в стадии стабилизации, т.е. нам нужно обеспечить ровную работу нашей ERP-системы на протяжении нескольких лет. При этом мы выстроили для себя дорожную карту по всем ключевым бизнес-системам, в соответствии с которой будет осуществлён плавный переход через стабилизацию к внедрению новых решений», — рассказал В. Феоктистов. В западные решения были вложены большие средства, и они отлично показали себя с точки зрения отказоустойчивости и продолжают работу.

Отказоустойчивость — это важный параметр для предприятий металлургии, поскольку все системы предприятия работают в режиме 24/7 без возможности остановки производства. Поэтому столь пристальное внимание уделяется архитектуре решений.

С мнением металлургов по поводу отсутствия готовых отечественных

решений для замены ERP-систем тяжёлого класса согласился и представитель «Гринатома». Он отметил, что «Росатом», РЖД и другие крупные корпорации не нашли пока выхода из ситуации. Представленные на рынке системы не ориентированы на промышленные предприятия непрерывного цикла и требуют долгого процесса доработки и затрат. Многие компании занимаются собственными разработками, чтобы перейти на отечественные решения к 2025 г.

По мнению Эльмана Бейбутова (Positive Technologies), отрасль ИБ оказалась лучше других готова к процессам импортозамещения. Это стало возможным по ряду причин, в том числе связано с требованиями регуляторов и наличием нормативных документов, в которых ставится вопрос сертификации и оценки соответствия. Компании-разработчики уже несколько лет используют решения из реестра российского ПО. В других отраслях запросы к российским разработчикам появились недавно, задачи обеспечения ИБ на крупных промышленных предприятиях ранее не ставились. «Незакрытые ниши и области — это сегменты, где исторически сильны западные вендоры», — отметил эксперт.

«Мы не можем остановиться вообще, у нас очень короткие технологические окна, а поменять СУБД — это означает десятки тысяч часов работы, — сказал Алексей Юдин, директор по ИБ компании QIWI. Он также отметил сложности с переносом данных и донстройкой решений. Ещё одна проблема — параллельное функционирование двух систем в момент перехода, их нужно

одновременно обслуживать, обучать людей, всё это требует дополнительных финансовых вложений. Юдин отметил, что на отечественном рынке СЗИ не всегда есть нужные решения, что-то приходится писать самостоятельно. По его словам, существует и проблема с программно-аппаратными комплексами: «Российских решений нет. Мы обошли всех по три раза — никто ничего не обещает. Поэтому пока не очень понятно, на какие решения мы можем перейти».

«Существуют контрольные сроки, есть несколько указов Президента РФ, есть одна единая дата — 1 января 2025 года, и в целом мы положительно на всё это смотрим. Но при этом мы понимаем, что это очень сложный процесс, есть огромное количество проблем», — сказал Владимир Бенгин, подводя итоги сессии. Представитель Минцифры рассказал о проектах по стимулированию процессов импортонезависимости (льготы, субсидии, гранты и т.д.), куда входят и проекты по ИБ. И в целом, по словам Владимира Бенгина, в отрасли дела обстоят неплохо, но есть и проблемы. Сложные направления — файрволы, межсетевые экраны следующего поколения... Ещё одна проблема, которую можно решить только через открытый диалог сообщества, — качество отечественных разработок, их надёжность и технологические возможности. Минцифры призывает производителей прислушаться к мнению заказчиков, которые, в свою очередь, должны понимать, что в любом случае придётся существенно менять внутренние процессы.

БЕЗОПАСНАЯ ЦИФРОВИЗАЦИЯ

Открывший ключевую дискуссию «Безопасная цифровизация» заместитель министра цифрового развития, связи и массовых коммуникаций РФ Александр Шойтов подвёл итоги 2022 г. По его словам, сейчас уже надо от первоочередных шагов переходить к системным и перспективным мерам. Он отметил, что руководители компаний переходят к практическим вопросам — как и что надо делать.

Хорошая регуляторика позволила прожить прошлый год без катастроф,



считает Владимир Бенгин. Минцифры видит новые типы угроз, предстоит много работы. Важно, что после выхода Указа Президента России от 1 мая 2022 г. № 250 проблема кибербезопасности из глубин отделов ИБ поднята на уровень персональной ответственности руководителей компаний. Для организаций, которые профессионально занимаются кибербезопасностью и у которых уровень ИБ высок, вообще нет никаких проблем, но для всех остальных, для десятков тысяч организаций, это будет непросто, подчеркнул Владимир Бенгин.

Представитель Национального координационного центра по компьютерным инцидентам (НКЦКИ) Сергей Корелов также отметил, что до выхода нормативно-правовых актов в области ИБ, в частности Указов президента России № 166 и 250, Приказа ФСБ России № 77, многие организации не задумывались о кибербезопасности. Кто-то занимался «бумажной» ИБ, кто-то считал, что их организация неинтересна хакерам, кто-то не подпадал под действия требований регуляторов. Однако практика показала, что любая организация может оказаться интересной для взлома.

Отвечая на вопрос модератора дискуссии Алексея Бобровского о влиянии процессов цифровизации на уровень защищённости КИИ, представитель регулятора отметил, что «цифровизация нужна конкретной отрасли. ИБ нужна при цифровизации».

«Внедряя цифровые процессы в бизнес, надо задумываться, к чему они

могут привести с точки зрения безопасности данных. Надо в обязательном порядке рассматривать угрозы и то, как их нивелировать», — отметил представитель НКЦКИ. — Техническая плоскость проблем компьютерных инцидентов — это отражение более глубоких причин».

«Не всякая цифровизация несёт угрозы, — считает и Владимир Бенгин. — Но если вдруг вы занялись цифровизацией, то обязаны заниматься ИБ», — подчеркнул он, сосредоточив внимание собравшихся на принципе Secure by design.

«Любая цифровизация порождает иные виды угроз, которых не было раньше. Задача и вопрос к безопасности — готов ли он перейти к тому, чего не было раньше, — поделился практическим опытом цифровизации финансовой сферы Артём Сычёв (Positive Technologies). — Любая цифровизация даёт новый вид угроз и требует перестройки мозгов — как парировать риски на уровне процессов и технологий. ...Абсолютной безопасности нет и не будет. Важно видеть, как тебя атакуют, нейтрализовать это и устранить последствия».

Как компании понимают текущие вызовы, рассказал на примере ОАО «РЖД» Юрий Ногинов, начальник департамента управления ИБ. Он отметил, что РЖД — крупная компания с огромной структурой, информационные системы которой должны функционировать в режиме онлайн с учётом территориально-распределённой схемы.



ОАО «РЖД» — это много компаний со своей сложной инфраструктурой и зависимостями бизнес-процессов. Цифровизация несёт новые вызовы и угрозы такой корпорации, отметил докладчик. И хотя документы и требования регуляторов значительно облегчают работу, многие задачи в классическом понимании нереализуемы, учитывая непрерывность бизнес-процессов. В РЖД понимают всю ответственность за безопасность и ведут работу по категорированию объектов КИИ, планируют создание киберлаборатории для прогнозирования угроз с учётом развития технологий.

В рамках 250-го Указа предстоит ещё многое сделать для повышения ИБ, отметил представитель НКЦКИ Сергей Корелов. В частности, вопросы аккредитации центров ГосСОПКА находятся в стадии проработки. Приказом ФСБ России от 1 ноября 2022 г. № 543 установлен трёхлетний переходный период. Заинтересованные в получении аккредитации компании должны набраться терпения и ждать проектов «Положения об аккредитации центров ГосСОПКА» и «Требования к центрам ГосСОПКА». Работа над этими документами ведётся, о чём подробно рассказывалось на «Регуляторном треке» Форума.

250-й Указ не обошёлся без принуждения исполнения мероприятий по ИБ, отметили все эксперты. Однако практика показывает, что организации приходится принуждать к исполнению требований по кибербезопасности, поскольку не все захотели реализовывать их в добровольном порядке.

«Вопрос самомотивации в виде штрафов и мониторинга гораздо сложнее», — считает Артём Сычёв. Ситуация начнёт меняться при появлении экономических механизмов, отраслевых регламентов, лицензий и требований по ИБ. В качестве примера эксперт привёл Банк России и финансовую отрасль, где экономические рычаги оказались надёжнее требований регулятора устранить недостатки.

КИБЕРБЕЗОПАСНОСТЬ АСУ ТП, ОБЛАЧНЫХ СЕРВИСОВ. SOC

Практическая часть Форума была посвящена вопросам Центров по обеспечению безопасности (SOC), практике построения корпоративных облачных сервисов с учётом их операционной надёжности и отказоустойчивости. Большой блок мероприятий был посвящён вопросам защищённости автоматизированных систем управления технологическими процессами (АСУ ТП), которые ранее выпадали из поля зрения инфобеза, однако оказались в числе критической информационной инфраструктуры (КИИ), которая требует защиты.

«Если есть силы, время и возможность, стройте SOC самостоятельно. Если нет — приглашайте MSSP-провайдера, у него есть опыт, средства и специалисты по всем направлениям, от программистов до узких специалистов в области ИБ», — говорили эксперты отрасли на сессии, посвящённой построению SOC.

Опытом построения SOC на крупном промышленном предприятии, в

работе которого сложно разобраться любому MSSP-провайдеру, поделился Алексей Мартынец, генеральный директор компании «НорникельСфера». Для промышленного предприятия типа «Норникеля» услуги внешнего SOC не подошли по ряду причин, среди которых недостаточный уровень компетенций сторонних специалистов, необходимость частого изменения бизнес-процессов, которые сказываются на работе SOC, недостаточный контроль за действиями подрядчика и доступ его к КИИ предприятия. Поэтому в «Норникеле» SOC является частью организационной структуры, подчиняется всем правилам внутреннего распорядка и его руководители несут полную ответственность.

«Процесс управления инцидентами ИБ в технологической сети не может быть реализован без комплексного проекта», — отметил Алексей Мартынец. Для обеспечения принципа Security by design необходимо вовлечение архитекторов безопасности АСУП на этапах построения и модернизации производственных процессов и систем управления, которые станут связующим звеном между командами автоматизации и ИБ.

При этом для управления инцидентами ИБ необходимо наличие зрелого ландшафта СЗИ для сбора данных о событиях безопасности. Все процессы кибербезопасности в технологической сети передачи данных взаимосвязаны с существующими бизнес-процессами, включая АСУП и АСУ ТП. Так, критичное повышение температуры, которое относится к процессам АСУ ТП, контролируется системами SOC в числе недопустимых ИБ-событий.

Согласился с подходом коллеги к построению внутреннего SOC и управляющий директор Центра информационной безопасности дочерних и зависимых обществ Газпромбанка Артём Калашников. Он отметил, что в презентации коллеги термин АСУ ТП можно легко заменить банковскими процессами и применить решения к финансовой сфере. Схожесть процессов финансовой ИБ и ИБ АСУ ТП подчеркнул и Алексей Мартынец, который ранее не был знаком с банковской безопасностью. Он отметил полезность межотраслевых встреч и мероприятий.

«КИБЕРБЕЗОПАСНОСТЬ В ФИНАНСАХ» — 2023

ЧТО МЕШАЕТ ПЕРЕЛОМИТЬ СИТУАЦИЮ В БОРЬБЕ С СОЦИАЛЬНОЙ ИНЖЕНЕРИЕЙ

На форуме «Кибербезопасность в финансах», который прошёл в феврале 2023 года в Екатеринбурге, участники обсудили методы борьбы с кибермошенниками, вопросы защиты интересов потребителей, законодательные инициативы. Панельная дискуссия «Противодействие мошенничеству и социальной инженерии» с участием Эльвиры Набиуллиной была посвящена итогам борьбы с таким злом, как социальная инженерия. Эксперты попытались понять, что всё-таки мешает всем участникам рынка во главе с регулятором переломить ситуацию в этой области мошенничества.

По данным регулятора, в 2022 году больше половины случаев кражи средств граждан было совершено именно с помощью социальной инженерии. Размер ущерба от действий злоумышленников вырос на 4,29%, до 14,2 млрд рублей.

В целом рост киберпреступности в 2022 году на 80% превысил статистику 2021 года, сообщил председатель комитета Госдумы по финансовому рынку Анатолий Аксаков, который выступил модератором панельной дискуссии.

По его словам, основная причина, конечно, геополитическая. Однако тот факт, что Россия стала продвинутой цифровой страной, также повлиял на количество атак.

Понятно, что компании стремятся как можно с меньшими затратами предоставлять как можно больше финансовых услуг и при этом с точки зрения бизнес-интересов немного тратить на защиту цифровых процессов. Налицо явный конфликт интересов.

Аксаков предложил участникам дискуссии обсудить ряд законодательных инициатив и тех шагов, которые необходимо предпринять, чтобы свести к минимуму киберпреступность. Первый

вопрос, который он предложил для обсуждения, — каковы итоги борьбы с социальной инженерией и что мешает добиться перелома ситуации.

КУЗНЕЦОВ ПОВЕДАЛ О ХОРОШИХ И ПЛОХИХ НОВОСТЯХ

В телефонном мошенничестве произошли коренные изменения и по направлению противодействия, и по направлению исследования новых инструментов действий наших противников, рассказал зампред правления Сбербанка Станислав Кузнецов.

«Звонки с Украины не прекратились — это плохая новость, — сказал он. — Хорошая новость в том, что почти прекратились звонки из пенитенциарных учреждений (тюрьма, колония, лагерь или иное закрытое учреждение, предназначенное для отбывания уголовного наказания, — прим. ред.).

Сегодня около 92–95% всех звонков в формате телефонного мошенничества совершается с территории Украины. Столицей телефонного мошенничества по-прежнему остаётся город Днепр, где в пике было около 1100 кол-центров, сейчас работает около 150. Всего на всей территории Украины Сбербанк фиксирует 800–900 кол-центров. При этом хорошая новость, по словам Кузнецова, в том, что в банке стали в десятки раз больше знать о работе этих кол-центров.

Зампред Сбербанка рассказал о том, что четыре телекоммуникационных оператора полностью соблюдают недавно внесённые поправки в закон, однако остальные несколько сотен, особенно региональных телекомов, к сожалению, допускают нарушения и продолжают незаконно торговать телефонными номерами, часть которых вообще предоставляется бесплатно. Это, конечно, нарушение закона, Роскомнадзор знает об этих фактах и уже начал штрафовать

подобных телеком-операторов. Но эта проблема сохраняет свою актуальность на региональном уровне.

«На повестке дня остро стоит вопрос о том, как объединить усилия, чтобы не допустить перетекания мошенников из одного банка в другой. В этом смысле у нас есть несколько предложений вместе с коллегами из других банков, как это сделать и объединить усилия, — рассказал представитель Сбербанка. — Мы готовы инвестировать и ресурсы, и силы, чтобы создать единый автоматизированный подход, который могли бы использовать все банки. Думаем, что его надо делать на безвозмездной основе, и лучше, если эту работу возглавит Центробанк».

КУЛИК СЧИТАЕТ, ЧТО ПРОТИБОБОРСТВУЮЩИЕ СТОРОНЫ ЭВОЛЮЦИОНИРУЮТ И ТАК БУДЕТ ВСЕГДА

«Есть такое представление, что надо что-то переломать и всем сразу станет лучше. Мне кажется, что это иллюзия, потому что это то же самое, что человечество и болезни — обе стороны эволюционируют всё время», — высказал свою мысль заместитель президента — председателя правления ВТБ Вадим Кулик.

По его словам, есть некоторые задачи, которые надо решить, и это может произойти уже в ближайшее время.

Первое — это создание между участниками взаимодействия — физическим лицом и организацией — доверия. Что имеется в виду? «Иванов должен быть уверен, что он общается с банком ВТБ, а ВТБ должен быть уверен, что общается с Ивановым», — подчеркнул Кулик.

В пандемию многие организации переходили на электронные каналы взаимодействия. Как результат появилась масса способов выудить информацию о физическом лице, в том числе с помощью фальшивых сайтов.

Для того чтобы было понимание, с кем человек общается, нужно доработать систему уже имеющихся государственных сервисов (например, Госуслуги, ЕБС) и донести до физического лица безопасный способ такого общения, сказал представитель ВТБ. Необходимо также составить базу, из которой будет понятна принадлежность телефонных номеров той или иной организации. Кроме того, должна быть решена проблема доставки значимой информации. Сейчас ответственность операторов за защищённость СМС одинаковая, независимо от содержания. Они в принципе не несут ответственности в этом плане, а наверное, должны бы, считает Кулик.

Вторая задача — это онлайн-обмен данными, при котором возможна блокировка подозрительных действий. Для того чтобы блокировка окончательно отработала, нужны будут точечные изменения в законодательстве, чтобы у банков появились права блокировать все подозрительные операции, подчёркивает эксперт ВТБ.

Наконец, «как бы мы ни защищались, если человек после многочисленных хищений опять попадает на уловки мошенников, то без третьей компоненты — образования людей и выстраивания у них определённой формы недоверия к таким способам воздействия на них — не обойтись, этим нужно обязательно заниматься», — говорит Кулик.

Заместитель президента — председателя правления ВТБ рассказал о том, что есть определённый процент клиентов, пусть и небольшой, которые готовы прийти в отделение банка и обливать сотрудников зелёной, наслушавшись разговоров о том, что они участники спецоперации по задержанию «ужасных банкиров», которые занимаются коррупционной деятельностью прямо в отделении кредитной организации.

КОМЛЕВ ЗАЯВИЛ О ВАЖНОСТИ МЕЖБАНКОВСКОЙ СВЯЗАННОСТИ ОПЕРАЦИЙ

«Мы как оператор платёжной системы видим другие аспекты проблемы, в отличие от банков. Важный



момент — межбанковская связанность операций, которая не всегда видна кредитным организациям, потому что она очень часто разрывается на уровне снятия наличных и переноса их руками в другой банкомат другого банка. Эти наличные деньги просто не видны», — объясняет своё видение вопроса генеральный директор Национальной системы платёжных карт (НСПК) Владимир Комлев.

Сейчас в НСПК идёт работа над тем, как за счёт машинного обучения, искусственного интеллекта, больших данных связать в одну транзакцию операции, которые на первый взгляд кажутся абсолютно разными (речь идёт о том, когда деньги снимаются со счёта в одном банке и затем кладутся на счёт в другом банке физическим способом, не через электронные каналы). И это составит весомый вклад в борьбу с социальной инженерией, подчёркивает Комлев.

«Я не хочу сказать, что мы научились отслеживать все транзакции, но среди тех, которые мы научились видеть, вероятность попадания близка почти к 100%», — отметил он.

Мошенничество никуда не денется, уверен эксперт. «И пока есть мошенники, они будут совершенствовать свои средства, а мы будем придумывать всё более искусные методы противостояния», — сказал Комлев.

По его мнению, сейчас рынок начинает консолидироваться вокруг понимания того, что проблема не может

быть решена отдельно Сбером, ВТБ, НСПК или ФинЦЕРТ. Должна быть единая консолидированная структура, которая максимально технологична, автоматизирована и в состоянии с такими вызовами бороться, резюмировал эксперт.

ПОЧЕМУ МЫ НЕ МОЖЕМ ПЕРЕЛОМИТЬ СИТУАЦИЮ С СОЦИАЛЬНОЙ ИНЖЕНЕРИЕЙ

Аксаков поддержал мысль Комлева о том, что надо объединять усилия по борьбе с социальной инженерией, поскольку одному банку с этим не справиться. При этом он обратился к прошлому опыту, когда банки старались замалчивать эту проблему, меньше говорить о том, что воруют деньги, потому что боялись испугать клиентов, опасались, что те уйдут из банковской сферы в наличные.

«Сейчас во весь голос все кредитные организации говорят об этой проблеме, но при этом социальная инженерия растёт, — подчеркнул Аксаков. — По данным Лаборатории Касперского, в прошлом году полтора миллиарда данных из различных крупных компаний утекло на рынок, что говорит об объёме проблемы, которую необходимо решать».

Депутат задал прямой вопрос главе Банка России Эльвире Набиуллиной: почему нам не удастся переломить ситуацию?

**СИТУАЦИЯ НЕИДЕАЛЬНАЯ,
НО РЕЗУЛЬТАТ ЕСТЬ**

«Мы обсуждаем это на разных форумах, боремся и боремся, каждая финансовая организация предпринимает усилия, мы предпринимаем усилия как регулятор. Где же мы всё-таки находимся? Я тоже посмотрела всю статистику, цифры. Такой общий ответ: результат есть, неидеально, но при этом не удалось достичь взрывного роста мошеннических атак, хотя такой риск был», — отметила председатель Центробанка.

По её мнению, в нынешней дискуссии речь идёт о банальной вещи — стакан наполовину пуст или полон. «Анатолий Геннадьевич утверждает, что он наполовину пустой, а коллеги с финансового сектора говорят, что они борются и говорят, что наполовину полный», — подметила Набиуллина.

Что можно увидеть по цифрам? Количество атак растёт, и эта тенденция будет продолжаться. Объём ущерба растёт, но не такими темпами, как количество атак. Успешность атак падает. Потому что если посмотреть удельный вес мошеннических атак к безналичному товарообороту, то он снизился на 25% в этом году.

Среди технологий социальная инженерия продолжает доминировать, хотя её вес несколько снизился: раньше речь шла о двух третях, сейчас они составляют примерно 50% из общего объёма мошеннических операций.

«На мой взгляд, перелома, к сожалению, не произошло, — констатировала глава регулятора. — Но я с Вадимом (Куликом — прим. ред.) не согласна, что это иллюзия, что будет когда-то переломный момент, мы должны его добиться. Приведу пример фальшивомонетчества. В своё время страна почувствовала, что это угроза, применили жесточайшее наказание, все органы власти боролись. Да, оно и сейчас есть, но не является социально распространённым явлением. И мне бы очень не хотелось, чтобы получение финансовых сервисов у людей в голове всё время ассоциировалось с риском мошенничества. Любой звонок может рассматриваться как звонок от мошенников. А у нас сейчас, к сожалению, появилась такая тенденция. И мы обязаны её переломить, и я считаю, что мы можем

этого добиться», — высказала своё мнение Набиуллина.

**НЕ ХВАТАЕТ СКОРОСТИ
И ВЫСОЧАЙШЕГО УРОВНЯ
КООРДИНАЦИИ ДЕЙСТВИЙ**

Возникает закономерный вопрос: что необходимо, чтобы ситуацию переломить?

«Мошенники, как всегда, креативны и очень сфокусированы. А мы действуем разрозненно и медленно, потому что в этой борьбе участвуют все: законодатель с законодательной базой, мы с регуляторными и надзорными практиками, банки, операторы связи, правоохранительные органы. Мы научились многие вещи делать быстрее, но всё равно мошенники будут быстрее нас. Поэтому нужна скорость и беспрецедентный уровень координации», — высказала своё мнение председатель Центробанка.

Она выразила удовлетворение тем, что коллеги поддержали идею обмена информацией и что крупные участники рынка готовы в это инвестировать, потому что не все кредитные организации могут создать на своей базе данных модели с ИИ.

«Если вы готовы делиться данными и отработкой моделей — это прекрасно, и мы как регулятор к этому готовы. Потому что критически важны и скорость обмена, и скорость принятия решений. Всё-таки многие атаки идут на крупных участников рынка, но дойдёт до всех, и все должны быть к этому готовы».

**КТО ЗАПЛАТИТ
ЗА МОШЕННИЧЕСТВО?**

Модератор панельной дискуссии обрисовал её участникам следующую проблему: «Я перевёл деньги в другой банк, а это оказались воры (операция была мошеннической — прим. ред.). Возникает вопрос о возмещении ущерба. Как вы относитесь к тому, чтобы возместить ущерб или часть ущерба, который понёс ваш клиент, и потом уже самому разбираться с тем, кто украл деньги, — с дроппером».

Владимир Комлев считает, что этот вопрос является болезненным для банков. По его мнению, важность тезиса о том, что должна быть собственная

ответственность людей и осознанность в совершении действий, не вызывает сомнений. Финансовая грамотность и понимание того, что ты делаешь, — ключевые вещи. При этом Комлев считает, что не должна возникнуть ситуация, при которой снизится «градус нормальной здоровой ответственности среди граждан». Если человек будет знать, что, сколько бы денег он ни перевёл мошенникам, ему всё равно всё возместят, это навредит.

Кулик, сам определивший свою роль в данной дискуссии как роль «асоциального пессимиста», указал на риск превращения банков в «странные социальные организации».

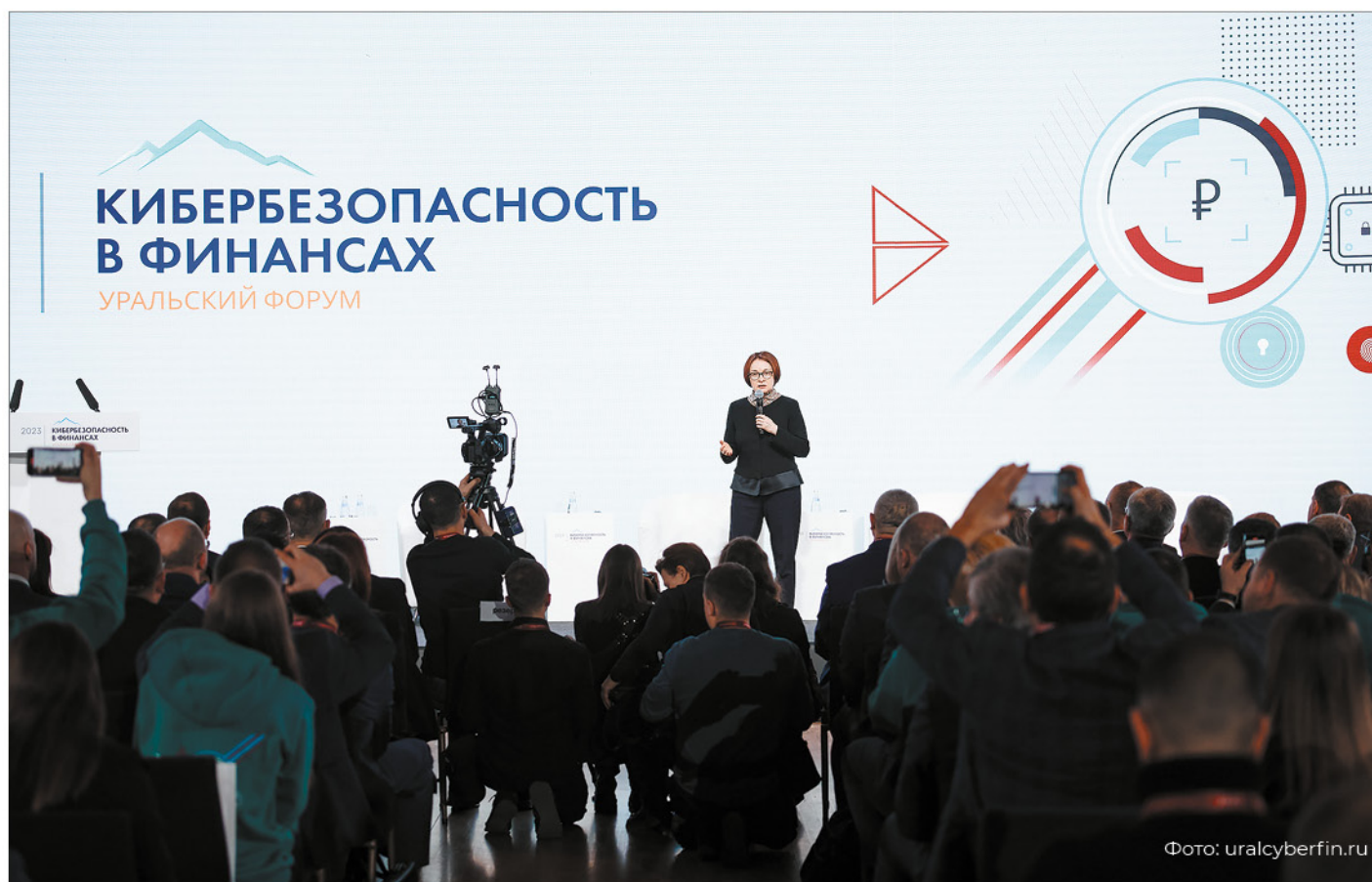
«Представьте, вы выдали ипотеку, и клиент приходит и говорит: я под социальным давлением взял у вас кредит и возвращать не буду. Мы рискуем превратиться в какие-то странные социальные организации, поэтому правильнее было бы иметь водораздел. Если технологии отработали правильно и у организации есть все следы того, что клиент был многократно предупреждён и отвергал эту помощь в разных формах, тогда я не понимаю справедливости этого возмещения», — объяснил позицию представитель банка ВТБ.

«Если банк виноват в том, что не защитил клиента, банк должен вернуть деньги. Если клиент после всех предупреждений снял деньги и по ведомой только ему логике отнёс их мошеннику самостоятельно, банк не должен нести ответственность», — высказал своё мнение Кузнецов.

**НАБИУЛЛИНА РЕШИЛА
НЕ РАДОВАТЬ БАНКИ,
НО ПОРАДОВАТЬ ИХ
КЛИЕНТОВ**

Глава Центробанка чётко обозначила позицию регулятора: «Я не порадою банки. Я считаю, что банки должны отвечать перед клиентами. Банки у нас такие продвинутые, с моделями, с системами антифрод-защиты. Человек более незащищён перед мошенниками, чем финансовая организация с её мощью».

Кстати, когда человек подпадает под влияние мошенников, это не только вопрос знаний, но и некоторой психологической готовности, человек может



быть психологически уязвим в какие-то моменты своей жизни, и не всегда знания спасают, считает Набиуллина.

«Мы с вами знаем немало примеров, когда даже менеджеры продвинутых финансовых организаций попадали на утку мошенников, — подчеркнула она. — Поэтому, помимо финансовой грамотности, необходимо создавать системы специальной защиты, а это могут делать только финансовые институты».

Глава Центробанка уверена, что необходимо принимать соответствующий закон. Он позволит, используя базу данных ЦБ о мошеннических счетах, во-первых, быстрее такой счёт блокировать. Во-вторых, у человека будет два дня, чтобы подумать, переводить деньги на счёт или нет.

«Знаю такие случаи, когда человека ушествовают, просят не переводить деньги, а он настаивает. Что в этой ситуации делать? Я считаю, что мы должны думать об этих решениях. Например, если мы знаем, что это сайт мошенников, надо блокировать поступление на него средств. И второе, я знаю, что обсуждаются вопросы страхования

киберрисков — это сложный вопрос, сложно оценить риски, но об этом можно думать. Особенно если система антитрода будет создана, страховщикам будет легче оценивать риски», — отметила Набиуллина.

По её мнению, перелома, о котором говорилось ранее, не произойдёт, если не будет достигнут перелом в вопросе по возмещению ущерба клиентам.

«Всё-таки возмещение ущерба банками стимулирует банки более активно заниматься антитродом», — констатировала председатель ЦБ.

В данном случае логика главы регулятора вполне понятна и заслуживает одобрения, на наш взгляд. Потому что банк — это огромная, сильная организация, особенно если речь идёт о тех финансовых учреждениях, которые принимали участие в пленарной дискуссии. Один из них монополист рынка, другой недалеко ушёл от этого. И они имеют огромный потенциал для защиты клиентских средств.

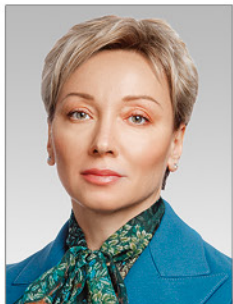
Логика «сам перевёл мошеннику — сам виноват» справедлива только отчасти. Безусловно, нужно думать головой,

когда ты совершаешь те или иные операции со своими деньгами, и быть предельно осторожным. Финансовая грамотность нам всем в помощь. Но Набиуллина абсолютно права в рассуждениях о «психологической уязвимости» каждого из нас в некоторые моменты жизни.

Люди доверяют банкам деньги, которые те с готовностью принимают. В таком случае они обязаны выстраивать эффективные системы защиты клиентских средств или признать свою несостоятельность и рекомендовать уходить в кеш.

Возмещение ущерба — это единственный способ стимулировать кредитные организации «заниматься антитродом», здесь регулятор также прав. Только материальный стимул является для банкиров действенным.

Правда, если банки получают право блокировать сомнительные, по их мнению, операции клиентов, есть риск того, что финансовые учреждения начнут усердствовать и заблокируют всё что надо и что не надо, дабы избежать проблем на своей стороне.



Ольга СКОРОБОГАТОВА
первый заместитель
председателя Банка России

ТЕХНОЛОГИИ: ЧТО В ФОКУСЕ ВНИМАНИЯ ЦБ?

СБП, ЕБС, ЦИФРОВОЙ РУБЛЬ, ТРАНСГРАНИЧНЫЕ РАСЧЁТЫ

Первый заместитель председателя Банка России Ольга Скоробогатова выступила с презентацией о результатах и перспективах развития национальной платёжной системы (НПС) и цифровых технологий на Ежегодной встрече кредитных организаций с руководством ЦБ РФ. Она рассказала о результатах работы в 2022 году и поделилась планами регулятора на 2023 год.

Регулятор чётко обозначил свои приоритеты в плане развития технологий на текущий год. При этом нельзя сказать, что они сильно изменились. По-прежнему пристальное внимание уделяется развитию цифровых сервисов. СБП будет в центре внимания, у системы появятся программы лояльности, которых станут хорошим стимулом для роста её популярности среди населения.

Важный пункт повестки ЦБ — развитие трансграничных платежей. Правда, здесь многое зависит не только от российского регулятора, но и от его партнёров за рубежом.

Есть надежда на то, что заработает единая биометрическая система, в том числе во многом благодаря запуску специального мобильного приложения, которое призвано решить проблему безопасности передачи клиентских данных.

КАЖДЫЙ ВТОРОЙ

Главным результатом работы НПС в 2022 году стала бесперебойность её

функционирования, несмотря на все сложности и большое количество платежей, отметила Скоробогатова.

Она озвучила некоторые цифры по картам «Мир» и СБП. Так, на сегодняшний день выпущено 182 миллиона карт НПС. «Это был органический рост, — подчеркнула первый зампред ЦБ. — Мы сохранили обработку карт международных платёжных систем в стране, чтобы у клиентов не было шока в связи с резким переходом на НПС».

Каждый второй гражданин РФ уже воспользовался сервисом СБП по переводу от физлица физлицу. «В 2,8 раза у нас вырос за прошлый год объём платежей двух видов (от физлица физлицу и оплата в торгово-сервисных предприятиях)».

Система передачи финансовых сообщений, которая изначально была создана как резервная, в прошлом году заработала в качестве основной там, где это возможно. Сейчас это 106 нерезидентов из дружественных стран, с которыми ЦБ активно продолжает работу.

По итогам 2022 года доля безналичных платежей в общем розничном обороте составила 78,1%, при этом прогноза на 2023 год был повышен до 80%, рассказала Скоробогатова.

ПЕРВОПРОХОДЦЫ

С точки зрения выстраивания стратегии платёжного рынка ЦБ видит СБП как основную. Это не значит, что система «Мир» прекратит своё развитие,

однако в контексте снижения издержек для граждан и для бизнеса, а также формирования конкурентной среды СБП будет в центре внимания.

Будут создаваться программы лояльности для СБП. Они обычно существуют для карт, но тем не менее регулятор считает, что для удобства и выгоды пользователей кешбэк и баллы по лояльности должны присутствовать и в СБП.

«Тема сложная, и в международной практике нет успешных примеров. Наша страна будет одной из первых в этом отношении», — подчеркнула Скоробогатова.

ТРАНСГРАНИЧНЫЕ РАСЧЁТЫ

Часть банков стали предлагать СБП для трансграничных расчётов через косвенное участие, и такие проекты успешно себя показывают с дружественными странами, рассказала первый зампред ЦБ.

«Если мы решим вопрос трансграничных расчётов, в том числе через СБП, это даст возможность нашим людям переводить деньги, оплачивать товары и услуги, находясь за рубежом, особенно в тех странах, которые готовы принимать российских туристов и хотели бы сохранить уровень безналичного обслуживания внутри их стран».

ЦИФРОВОЙ РУБЛЬ

Скоробогатова напомнила, что цифровой рубль рассматривается регулятором

**Национальная платежная система. Планы на 2023 год.****Система быстрых платежей (СБП)**

- > внедрение банками С2В сценариев оплаты, в т.ч. по NFC в одно касание и «подписок»
- > реализация программы лояльности
- > внедрение банками платежей в бюджет (С2G)

**Трансграничные расчеты**

- > увеличение участников СПФС
- > расширение участников СБП
- > прием карты МИР в дружественных странах

**Цифровой рубль (ЦР)**

- > принятие законодательства о Цифровом рубле
- > с апреля пилот С2С, С2В, В2С на ограниченном круге участников
- > интероперабельность ЦРЦБ с другими странами

**Цифровые технологии. Планы на 2023 год.****Единая биометрическая система (ЕБС)**

- > совершенствование процесса сбора биометрических образцов в банках
- > мобильное приложение для сдачи биометрии
- > развитие новых сервисов:
 - * дополнительный фактор при аутентификации на Портале Госуслуг
 - * выпуск электронной подписи в приложении Госключ и ФНС России
 - * получение Fan ID
 - * биокайринг
 - * подтверждение оплаты через «Интернет»
 - * проход в метро

**Цифровые финансовые активы (ЦФА)**

- > устранение налогового арбитража и гармонизация налогового режима цифровых прав и традиционных финансовых инструментов
- > создание условий для участия традиционной инфраструктуры в обращении цифровых прав
- > гармонизация подходов к выпуску и обращению цифровых прав – возможность выпуска УЦП в информационной системе выпуска ЦФА
- > учет особенностей ЦФА в регулировании кредитных организаций и некредитных финансовых организаций

**Цифровые технологии. Планы на 2023 год.****Открытые API**

- > Доработанная модель открытых API по результатам обратной связи
- > Разработка дорожной карты проекта внедрения и предложений по изменению регулирования
- > Разработка стандартов Открытых API: рекомендательных и обязательных
- > Концепция Платформы коммерческих согласий

**Другие проекты**

- > Цифровой профиль для ЮЛ
 - > Сквозное ID
 - > Платформа Согласий
 - > Развитие ЭПР
 - > Платформа «Госключ»
 - > Трансграничная идентификация
- > Национальная экосистема цифровых платформ

как третья форма денег, которая сочетает в себе качества наличного и безналичного рубля. При этом новшество состоит в том, что оператором будет выступать ЦБ и кошельки для клиентов будут открываться на платформе Банка России.

ЦБ не планирует начислять проценты на остаток, при этом хочет ввести лимиты на остатки по цифровым кошелькам.

«Это новое платёжное средство, но ни в коем случае не замена депозитов или иных продуктов, которые делают коммерческие банки. Коммерческие банки сохраняют весь перечень обслуживания и привлечения клиентов, в том числе предоставляя доступ к цифровому кошельку через свои мобильные приложения».

ЕБС: ПЕРЕЗАПУСК СИСТЕМЫ

ЦБ потратил много времени на совершенствование законодательства и обдумывание того, как необходимо развивать единую биометрическую систему, чтобы она реально заработала. С этой целью было принято решение о запуске совместного предприятия, состоящего из трёх акционеров (Минцифры, ЦБ и Ростелекома), которое уже начало функционировать.

Регулятор планирует в текущем году активно развивать новые сервисы в ЕБС. Также было создано специальное мобильное приложение для сдачи биометрии, которое должно заработать.

«Для нас это краеугольный камень с точки зрения сбора информации, потому что клиенты в цифровом мире хотели бы никуда не выходить и даже первый раз не приходить и не сдавать биометрию в офисе банков (причём есть и такие кредитные организации, которые не имеют офисов)», — отметила Скоробогатова.

Важно было сделать этот процесс безопасным, чтобы не было никаких подмен биометрических данных со стороны мошенников, подчеркнула она.

«Мы решили этот вопрос с помощью мобильного приложения для сдачи биометрии», — заявила Скоробогатова.

Подготовила
Оксана Дяченко



Дмитрий КУКОЛЕВ
директор по информационной
безопасности Дзен

АВТОМАТИЗАЦИЯ APPSEC

КАК ОБЕСПЕЧИТЬ БЕЗОПАСНОСТЬ И ЗАЩИЩЁННОСТЬ ПРОДУКТОВ В СЖАТЫЕ СРОКИ

Сложность и скорость процессов производства ИТ-продуктов растут с каждым годом: увеличивается количество инструментов, объём кодовой базы, а вместе с тем и число уязвимостей в ПО, что пропорционально усложняет задачи по обеспечению безопасности ИТ-продуктов. В связи с постоянно растущим количеством кибератак и сложностью ИТ-ландшафта ИБ должно менять свои традиционные методы и подходы, подстраиваясь под новую реальность с помощью автоматизации.

ПРОДУКТ ИЛИ БЕЗОПАСНОСТЬ?

Продуктовая безопасность — это одна из наиболее актуальных областей информационной безопасности, в то же время испытывающая голод в области средств контроля и экспертов. На сегодняшний день ИТ-ландшафт практически любой компании, устроенной по принципу «Энтерпрайз», — это логически сложная, технологически гетерогенная и распределённая инфраструктура, которая в любой момент может быть подвержена кибератаке. И тем не ме-

нее для большинства ИТ-компаний, производящих цифровые продукты и владеющих ими, ключевой фактор — показатель T2M (Time to Market). Скорость, с которой продуктовые команды должны представлять новые релизы, чтобы соответствовать требованиям рынка и интересам бизнеса, вытесняет вопросы безопасности на второй план.

Поэтому современные задачи по обеспечению защищённости требуют трансформаций от команд ИБ: большего уровня погружения и скорости реагирования, чем было несколько лет



Рисунок 1. Подход предоставления сервисов ИБ через платформы

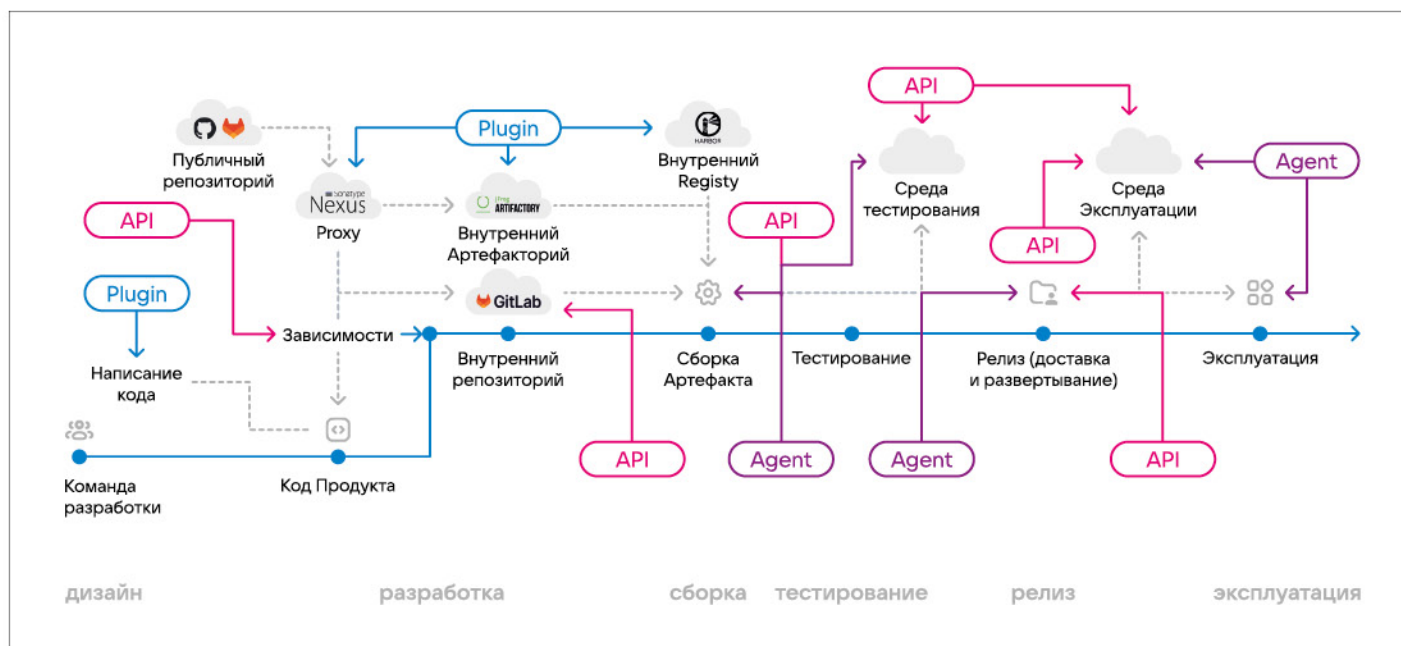


Рисунок 2. Пример того, как может быть интегрирована платформа в процесс производства продукта

назад, освоения новых подходов, практик и инструментов.

5 ключевых принципов, по которым должно сейчас работать продуктовое ИБ:

- ♦ обеспечивать безопасность «по дизайну» и иметь фокус на автоматизацию;
- ♦ уметь работать с инновациями и обеспечивать Compliance при постоянно меняющихся правилах и требованиях;
- ♦ быть прозрачным и удобным для цифрового потребления сервисов;
- ♦ быть быстрее ИТ, работая на опережение;
- ♦ отсутствие задержек и трений при взаимодействии ИТ и ИБ.

Чтобы безопасность приложений, из которых строится продукт, стала одной из ключевых ценностей для разработчиков, а не только страхом перед вероятностью киберугрозы или исполнением обязательных требований регуляторов, необходимо выстроить корректный процесс безопасной разработки. Один из способов достижения данной цели – автоматизация контролей ИБ, которая достигается созданием платформенных решений.

ФОКУС НА АВТОМАТИЗАЦИЮ, УДОБСТВО И ПРОЗРАЧНОСТЬ

Определив для себя, что количество ручных операций ИБ и явных Security

Gates для команд разработки должно быть снижено, мы сформировали подход предоставления сервисов ИБ через платформы (рис. 1). Они работают в режиме Self-Service (единое окно для самостоятельного взаимодействия с функциями ИБ) и поддерживают процесс безопасного производства с помощью интеграции этих контролей «под капот» (непрерывные сканирования и контроли на каждом этапе создания приложения). Это позволяет повысить уровень наблюдаемости за процессом создания приложений и получить больший объем информации, что приводит к внедрению контролей ИБ с качественным уровнем погружения в контекст.

Внедрение большего количества «целевых» контролей, выставленных на различных этапах процесса, позволяет на этапах сборки, доставки и частично производства применить проактивный подход к безопасности создаваемых приложений. Таким образом, снизить нагрузку на команду продуктов за счёт более раннего обнаружения уязвимостей, большого количества подсказок, рекомендаций, шаблонов корректного использования Inner Source экосистемных компонентов и недопущения возможности использования недоверенного компонента, который может использоваться для блокирования уязвимости типа PROTESTWARE (рис. 2, 3).

При таком подходе построения процессов ИБ удастся качественно повысить уровень их прозрачности и получить большое количество сводной и скоррелированной информации, специально проработанных метрик и статистик в реальном или почти реальном времени. Это помогает не только продуктовым командам и ИБ, но и смежным подразделениям — IP Compliance, HR и даже C-Level, позволяя им отслеживать уровень «здоровья» продукта и его зависимостей по ИБ в удобном дашборде с понятными и описанными метриками.

КОРОТКО ПРО МЕТРИКИ И ФАКТЫ

Сейчас ни одна сфера бизнеса не может представить свою работу без метрик, но интеграция аналитики до сих пор вызывает немало вопросов и проблем. С помощью разработанного подхода через автоматизированную платформу можно получить доступ к информации о составе продукта, результатов анализа SAST, SCA (например, статистику по уязвимостям и OSS компонентам, стеки разработки и лицензии). Также о Supply Chain, релизах и экземплярах (например, динамику появления и исправления уязвимостей, их жизненный цикл, Products Security Heatmap) и о профиле разработчиков, поверхности атаки, исторических данных. Например,

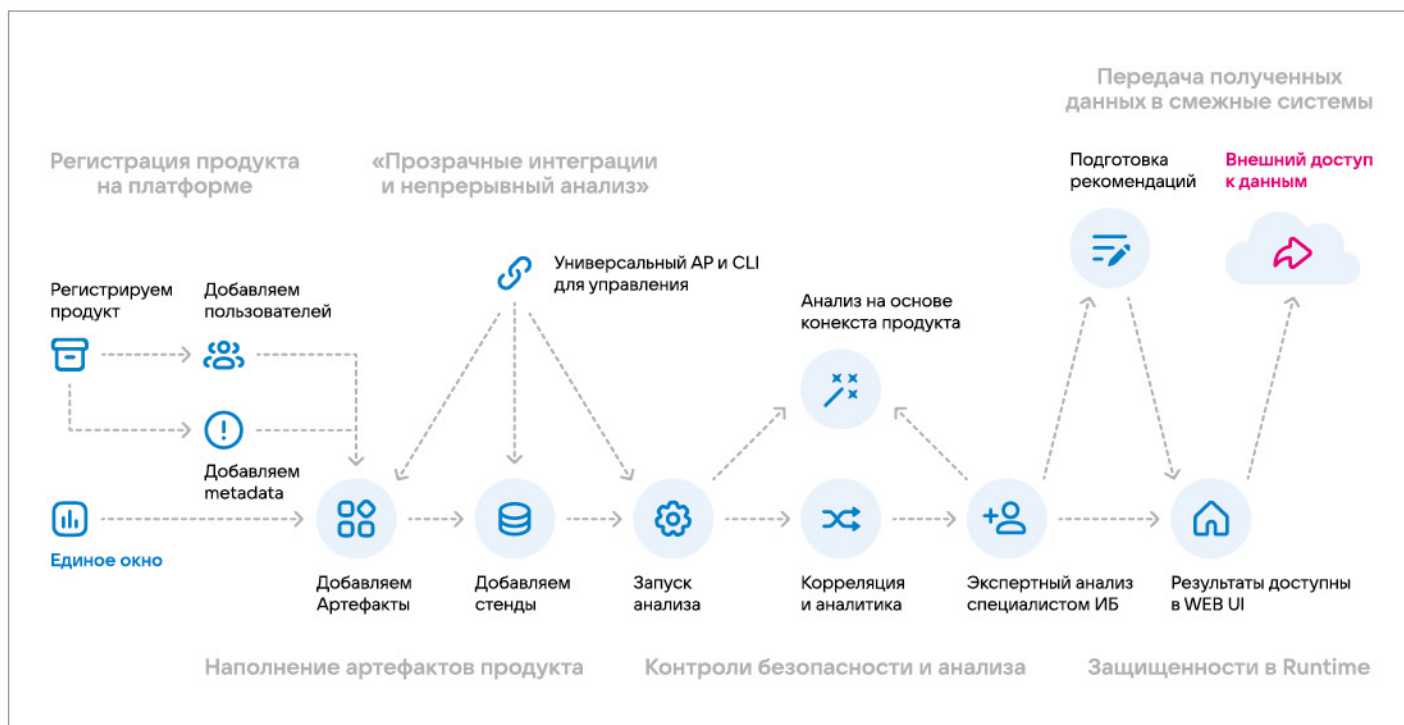


Рисунок 3. Принцип работы с платформой для продуктовой команды

жизненный цикл анализаторов и контролей, технический долг по ИБ и его стоимость, наиболее часто допущенные уязвимости при разработке и пр.

И это подводит к одной из краеугольных проблем текущего уровня ИТ и ИБ-специалистов в России — их профессионализму и пониманию процессов безопасности.

ВЗАИМОДЕЙСТВИЕ ИТ И ИБ: НАВСТРЕЧУ ДРУГ ДРУГУ

К сожалению, большинство разработчиков до сих пор не воспринимают безопасность как ценность продукта, а относятся к ней скорее как к теоретической данности или навязанной необходимости. На это, в частности, влияет и общепринятый подход ИБ — запрещать, не вдаваясь в подробности. Чтобы перебороть этот тренд, необходимо предложить команде разработчиков удобные процессы и факты, которые позволят быстро выявлять и анализировать наиболее частые ошибки, разбирать их на реальных уязвимостях в продукте, определять индивидуальный вектор обучения и отслеживания успехов разработчика.

Это требует и пересмотра функциональности инженеров ИБ. С повышением уровня зрелости ИБ, а именно

глубинного внедрения платформ ИБ в производство продуктов и масштабированием этого подхода на большее количество команд, обязательным требованием для специалистов ИБ стало понимание процессов производства и умение интегрировать безопасность в эти процессы. Для эффективной работы с ИТ над ценностью продукта специалисты ИБ должны уметь говорить с ними на одном языке, понимать малейшие нюансы продукта и уметь программировать. К сожалению, без этих навыков современный AppSec не получит качественного изменения процессов ИБ и уважительного отношения со стороны команд разработчиков.

РАБОТАЮЩИЙ МЕТОД

Описанный подход через платформы ИБ уже с успехом внедряется в Дзен и в других продуктах и приложениях VK. На возможную критику о том, что данный подход может быть применен только в компаниях, где уровень зрелости ИБ уже достаточно высок, стоит отметить, что он был также удачно опробован и на опыте «бирюзовой» компании.

Платформы ИБ легко встроить в существующие процессы производства и эксплуатации за счёт большого уровня

универсализации и широких возможностей интеграции. Это позволяет реализовать контроли прозрачно и в непрерывном режиме, а за счёт их гибкости ИБ и ИТ могут в дальнейшем совместно повышать общую зрелость без задержек и трений между двумя командами. Наш опыт показывает, что с повышением прозрачности процессов ИБ и демонстрацией реального уровня безопасности и защищённости ИТ-продукта возрастает и уровень лояльности продуктовой команды к ИБ. Это, в свою очередь, влияет на качество и количество исправленных уязвимостей командой ИТ без эскалации и дополнительных напоминаний со стороны команды ИБ.

Подход через платформы ИБ не серебряная пуля, его основной минус — высокие требования к инженерам ИБ, потому что им нужно понимать процессы производства, уметь разрабатывать средства защиты, системы-оркестраторы и платформы, а также дорабатывать уже существующие анализаторы. Но есть и плюсы — таких инженеров требуется намного меньше.



Данила ЧЕЖИН
директор по продуктам
Servicepipe

ЗАЩИЩАЯ ПОЛЬЗОВАТЕЛЕЙ, ЗАЩИЩАЙТЕСЬ САМИ

ЧЕМ ОПАСЕН SMS-БОМБИНГ И КАК ЗАЩИТИТЬ
ОНЛАЙН-РЕСУРС ОТ АТАК НА БИЗНЕС-ЛОГИКУ

С конца 2021 года мы начали фиксировать новый тип атак на бизнес-логику веб-приложений. Этот вектор часто называют SMS Leak, SMS-бомбингом или атакой на баланс SMS.

ОБ АТАКЕ

SMS Leak — это автоматизированная атака на бизнес-логику веб-ресурса (веб-сайта или API мобильного приложения). Механизм атаки эксплуатирует функциональность автоматизированной отправки SMS. Компании используют её для подтверждения авторизации при регистрации новых пользователей, восстановления паролей, заказов и оповещений клиентов.

SMS-бомбинг нацелен на исчерпание баланса у SMS-агрегатора или неконтролируемый расход бюджета компании-жертвы на отправку сообщений.

КТО ПОД УГРОЗОЙ

В зоне риска любой онлайн-бизнес, использующий двухфакторную авторизацию пользователей в личном кабинете: ретейл, банки, интернет-магазины, службы доставки еды, такси, каршеринг и многие другие сервисы.

КАК ПРОХОДИТ АТАКА

1. Злоумышленники используют ботнет. В этом случае алгоритм атаки запускается одновременно на множестве устройств, каждое из которых имеет свой IP-адрес. Это сильно затрудняет поиск и блокировку источника атаки.

2. Боты задействуют механизм двухфакторной авторизации. Используя «утёкшие» базы и генератор телефонных номеров, они формируют множество запросов на отправку авторизационных SMS.

3. Каждый нелегитимный запрос приводит к отправке SMS-кода подтверждения. На веб-приложение поступают десятки и сотни тысяч паразитных запросов в сутки. Месячный бюджет на SMS расходуется за несколько дней, а счёт от SMS-агрегатора может вырасти в десятки раз.

4. Пользователи начинают массово обращаться в техподдержку атакованной компании. Клиенты, получившие SMS-коды подтверждения, ошибочно полагают, что подверглись мошенничеству или попытке взлома аккаунта. Они обращаются в поддержку и создают дополнительную нагрузку, которая приводит к ухудшению качества клиентского сервиса.

РАЗМЕРЫ УБЫТКОВ

Впервые с SMS-бомбингом мы столкнулись в банковской сфере. Один из наших клиентов узнал об атаке постфактум. К моменту обнаружения счёт от SMS-агрегатора уже достигал 6 миллионов рублей.

Количество запросов к веб-приложению банка в среднем составляет 40 млн в сутки, из них — ботовых запросов было около 10%, и только 1% трафика составляли запросы SMS-бомбера. Даже такой, казалось бы, незначительный объём атаки может привести к ощутимым потерям. Если предположить, что стоимость отправки SMS составляет 1,5 руб. за сообщение, суточные убытки составят 600 000 рублей.

ПОЧЕМУ SMS LEAK СЛОЖНО ПРЕДОТВРАТИТЬ

Распределённые источники. Источники ботовой активности сильно распределены по множеству IP-адресов. С каждого отправляются единицы запросов в минуту. Из-за этого они не выглядят подозрительными для систем обнаружения аномалий.

Имитация суточной активности. Ботнет умело имитирует суточную активность пользователей — объём запросов плавно повышается днём и снижается ночью.

Однако ботовые фермы не знают о легитимных всплесках в мобильном трафике (например, реакция на маркетинговую активность, пуш-уведомлениях или обновлениях) (рис. 1).

Источники ботов и пользователей совпадают. Даже если SMS Leak был обнаружен, самостоятельно отсечь трафик атаки будет проблематично. В простейшем сценарии ботнет развёрнут в одной или нескольких хостинговых подсетях. В этом случае можно самостоятельно заблокировать атаку по IP-адресам источников.

В реальности основная часть продвинутых ботнетов использует сети мобильных операторов. Поэтому при попытке заблокировать ботов по IP-адресу источника доступ к ресурсу потеряют и легитимные пользователи, что приведёт к ещё большему росту обращений клиентов в поддержку.

Чтобы не затронуть легитимный трафик, потребуется его более тонкая фильтрация.

ОПТИМАЛЬНОЕ РЕШЕНИЕ — ЗАЩИТА С ПОМОЩЬЮ АНТИБОТ-ТЕХНОЛОГИИ

Для защиты от таких атак привычных средств защиты от DDoS-атак и взлома недостаточно. Необходимо в реальном времени определить, кто сформировал запрос — реальный пользователь или атакующий алгоритм. Даже если запросы ботов по своим параметрам не отличаются от «человеческих».

Такие решения называют *Bot Protection*, а ключевыми параметрами их работы являются точность и скорость детектирования.

Мы развиваем собственную технологию защиты от ботов Servicepipe Cybert с 2019 года. Услуги защиты на её базе способны определять и блокировать ботов с первого запроса, пропуская реальных пользователей, даже если с их устройств фильтруется трафик атаки.

КАК РАБОТАЕТ МНОГОФАКТОРНЫЙ АНАЛИЗ

Высокая точность и скорость блокировки достигается за счёт многофакторного анализа трафика в реальном времени:

- ♦ выявляются статистические аномалии;

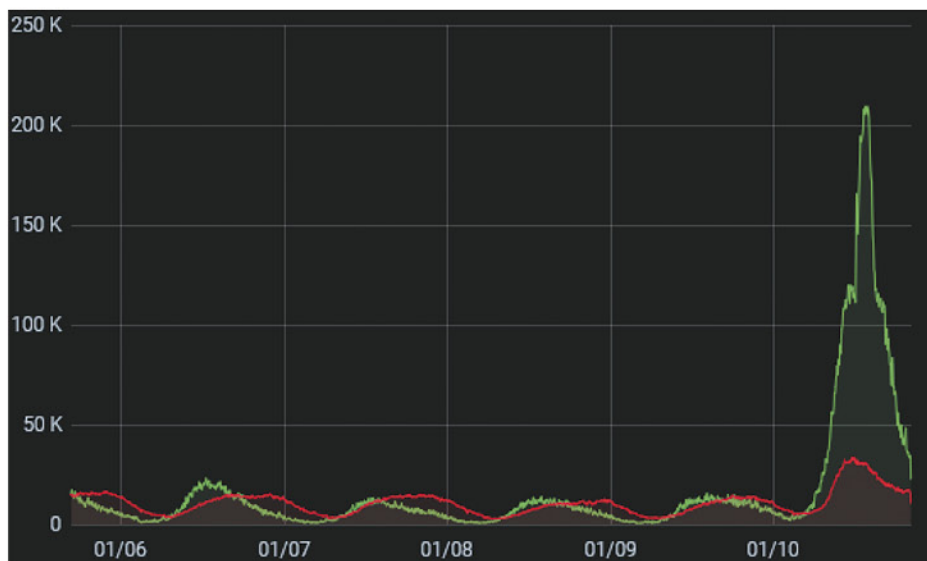


Рисунок 1. График разметки трафика за недельный период



Рисунок 2. Работа платформы Servicepipe Cybert

- ♦ анализируются более 100 технических метрик запроса;
- ♦ запрос сопоставляется с подозрительными сигнатурами из нашей базы ботнетов и сигнатурами легитимных мобильных клиентов и браузеров;
- ♦ в случае сомнений — вычисляются поведенческие факторы.

В итоге для каждого запроса строится вектор факторов и вычисляется его легитимность. Все этапы анализа занимают менее 1 мс (рис. 2).

КОМПЛЕКСНАЯ ЗАЩИТА ОТ АТАК НА БИЗНЕС-ЛОГИКУ

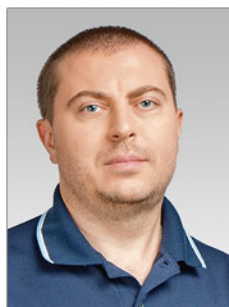
SMS Leak — это лишь одна из атак на бизнес-логику. Её, конечно, мож-

но минимизировать собственными силами. Например, ограничить частоту отправки SMS для отдельного мобильного номера (допустим, не более 1 сообщения в 1–2 минуты). Или сделать доступной отправку SMS только на мобильных российских операторов либо ограниченного списка стран. Однако всё это лишь уменьшит ущерб, а не предотвратит атаки.

Мы в Servicepipe рекомендуем решать проблему системно и выбрать универсальное решение, которое защитит ваши онлайн-ресурсы и от SMS Leak, и от любых других автоматизированных угроз.



Рами МУЛЕЙС
менеджер продуктов
безопасности, Yandex Cloud



Дмитрий КУДИНОВ
ISMS-менеджер, Yandex Cloud

ЧТО ТАКОЕ DEVSECOPS

И КАК АВТОМАТИЗИРОВАТЬ КОМПЛАЕНС

Согласно результатам нашего опроса, 25% пользователей Yandex Cloud используют облачную платформу для разработки. И это понятно, так как в облаке достаточно просто развернуть всё, что нужно для автоматизации разработки, тестирования, доставки и стабильной работы приложения. Но как быть тем организациям, которым, кроме стандартных задач обеспечения защиты, необходимо контролировать соблюдение формальных требований по безопасности? Яркий пример — финтех-приложения, которые должны соответствовать множеству стандартов: 152-ФЗ, ГОСТ 57580, PCI DSS и другим. Это и раньше была непростая задача, а сейчас, когда жизненный цикл современных приложений настолько ускорился, что уже нет времени на проведение аудитов

и контроль соответствия, проблем стало ещё больше. Поговорим о том, как соответствовать требованиям безопасности в условиях автоматизации разработки и непрерывной доставки приложений.

DEVOPS В ОБЛАКЕ

Всё больше и больше продуктовых команд выбирают облако из-за возможности ускорить выход приложения в промышленную эксплуатацию и, соответственно, на рынок. Облачные решения дают разработчику, тестировщику и DevOps-инженеру большую свободу. Они получают требуемый уровень абстракции и переносят в облако основные компетенции, связанные с эксплуатацией необходимой для работы инфраструктуры. Не нужно думать о том, как реализовывать систему виртуализации, как оркестрировать контейнеры и организовывать

микросервисную архитектуру приложения. В облаке есть готовые сервисы, которые можно использовать.

Однако для наиболее эффективной и надёжной разработки программного обеспечения и его вывода на рынок требуется тесное взаимодействие разных команд: не только разработчиков и системных администраторов, но и специалистов по информационной безопасности. Автоматизация разработки приложений может включать в себя и учёт рисков безопасности, анализ кода и конфигураций, контроль безопасности и проверку на соответствие и соблюдение законодательства. Это особенно важно при создании и эксплуатации финтех-приложений (рис. 1).

SEC В DEVOPS: КОНЦЕПЦИЯ SHIFT-LEFT

Почему безопасностью нужно заниматься как можно раньше? Как пра-

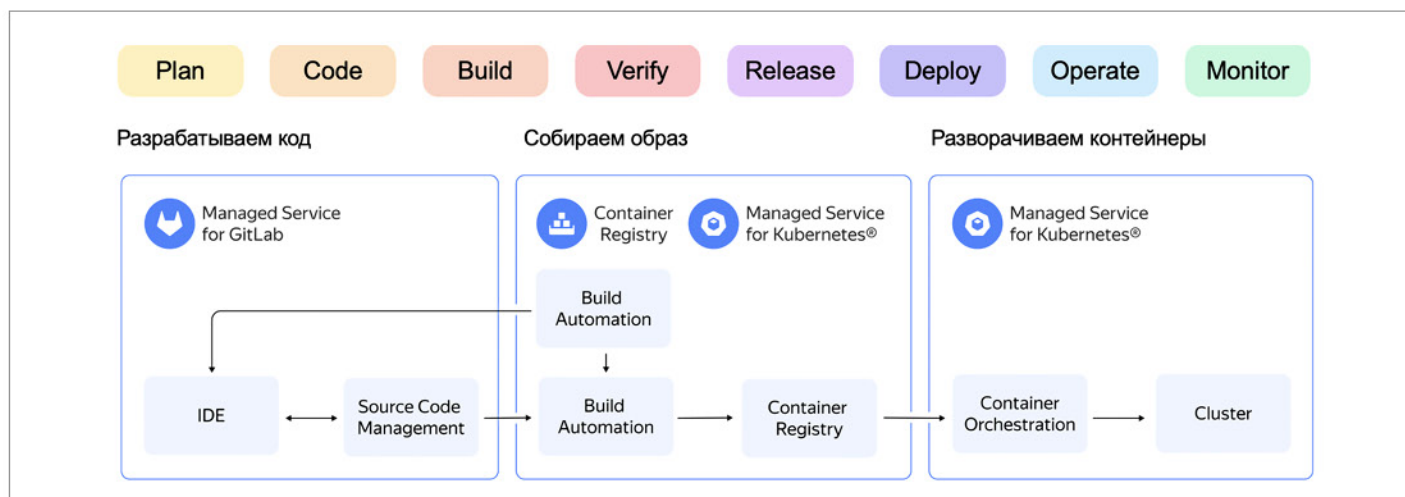


Рисунок 1. Автоматизация разработки и доставки приложения в облачных платформах

Экономика безопасности разработки

Этапы
CI/CD

Plan

Code

Build

Verify

Release

Deploy

Operate

Monitor

Затраты
на исправление
ошибок



Рисунок 2. Стоимость исправления ошибок на различных этапах жизненного цикла разработки приложения

вило, разработчики создавали версию приложения, и только затем тестировщики и специалисты по безопасности проводили анализ её защищённости. Но в условиях, когда в командах разработки практикуется методология непрерывной интеграции и развёртывания кода (CI/CD), длительные задержки на проверку ИБ становятся недопустимыми. Более того, внедрение сложнее. Присутствие специалистов по ИБ требуется на всех этапах разработки.

Всё это привело к следующему этапу развития DevOps — DevSecOps и внедрению практики включения контролей безопасности на более ранних этапах — Shift-left. DevSecOps меняет традиционное представление о роли подразделения информационной безопасности в обеспечении качества и надёжности кода. Новая методология повышает прозрачность процесса разработки, делая оценку угроз безопасности более результативной за счёт использования методов выявления

уязвимостей и автоматизации процесса их исправления.

Но ценность внедрения DevSecOps для бизнеса не только в раннем подключении к процессам обеспечения безопасности смежных специалистов. Экономика безопасности разработки такова, что увеличение стоимости исправления ошибки или уязвимости на уже собранном приложении может доходить до ста раз. Её обнаружение перед тем, как функция будет внедрена в рабочую среду, невозможно переоценить.

В облаках на всех этапах — разработка кода, сборка образа и разворачивание контейнеров — есть сервисы, которые помогают не только автоматизировать процессы, но и обеспечить контроль безопасности. Например, управляемые GitLab или Kubernetes. В этих продуктах большое количество инструментов и подходов к обеспечению безопасности, контроля безопасности, различные плагины и инструменты (рис. 2).

КАК ПОСТРОИТЬ БЕЗОПАСНЫЙ ПРОЦЕСС РАЗРАБОТКИ И СООТВЕТСТВОВАТЬ ТРЕБОВАНИЯМ

Вернёмся к финтех-приложению. Ему необходимо соответствовать сразу многим законам, положениям и отраслевым стандартам.

Для упрощения разделим жизненный цикл разработки приложения на три основных этапа (рис. 3):

Этап безопасной разработки

◆ Этап безопасного развёртывания приложения

◆ Этап защиты инфраструктуры

Этап безопасной разработки.

Начинать нужно с обучения разработчиков. Подготовить гайды и рекомендаций по безопасному программированию с примерами на ваших языках. Это поможет не допускать типовых и простых ошибок в самом начале пути. Материалы должны находиться всегда под рукой. Мы в Yandex Cloud внутри храним такие практики на внутреннем

Plan

Code

Build

Verify

Release

Deploy

Operate

Monitor

Безопасная разработка

Безопасное развёртывание

Безопасная инфраструктура

Рисунок 3. Основные задачи обеспечения безопасности приложения в условиях автоматизации

портале Yandex Wiki. Это сервис для создания корпоративной базы знаний, которую наполняют и обновляют сами сотрудники компании. А для планирования и обсуждения деталей используем Yandex Tracker — сервис для управления проектами и процессами.

Этап безопасного развёртывания приложения. Безопасное развёртывание приложений можно разделить на три части.

♦ **Управление изменениями.** Простое правило: всё, что попадёт в продакшен, должно подтверждаться «незаинтересованной стороной». Например, код-ревью должен выполнить тот, кто не принимал участия в разработке. Аудейты — протестированы. Процесс — прозрачен, чтобы при запросе показать его аудиторам.

♦ **Управление уязвимостями.** В продакшен не должны попадать уязвимости, в том числе уязвимые third-party-компоненты. Их нужно вовремя обнаруживать, ранжировать по критичности и исправлять. Самые требовательные стандарты требуют, что патч, исправляющий уязвимость, нужно установить не позднее 30 дней после его выхода. Для поиска уязвимых компонентов в Yandex Cloud есть сканер, который встроен в сервис Container Registry. А включение динамического и статического анализатора кода из Managed Service for GitLab поможет сделать исходный код безопаснее.

♦ **Управление ключами и секретами.** Ключи и секреты нужно хранить и передавать так, чтобы злоумышленник не смог к ним добраться. «Хардкодить» такие данные — очень плохая практика. Для управления секретами в Yandex Cloud есть сервисы KMS и Lockbox. KMS в том числе защищает секреты, которые хранятся в кластере Kubernetes. Правильно построенный процесс и использование этих инструментов позволят легко пройти любой аудит.

Этап защиты инфраструктуры. Это защита вашего работающего продакшен-кластера. Возьмём несколько базовых процессов:

♦ **Управление доступом.** Если вы в облаке, то используете IAM. В IAM есть роли, и чтобы соответствовать требованиям, нужно, чтобы вы на своей стороне соблюдали принцип минимальных

полномочий. То есть давали доступ только тому, кому он необходим.

♦ **Сетевая безопасность.** Среду тестирования необходимо отделить от среды продакшен. Например, в Yandex Cloud есть VPC с механизмами Security Group. Эта связка очень выгодная не только со стороны ограничения сетевого трафика. Вам не нужно думать, какой вендор ушёл или какое сетевое устройство отключилось. Просто настраивайте группы безопасности и управляйте правилами фаервола и потоками трафика.

♦ **Управление инцидентами.** Сбор логов аудита, корреляция, алерты — это всё требуется многими стандартами. Для того чтобы соответствовать требованиям и строить безопасность, в облаке есть много инструментов. Например, Cloud Trail и Cloud Logging. А свою систему мониторинга событий безопасности можно построить на базе Yandex Audit Trails и интеграции сервисов Yandex Managed Service for Elasticsearch или Yandex Managed OpenSearch.

АВТОМАТИЗАЦИЯ КОНТРОЛЯ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ

По всему жизненному циклу можно использовать как продукты Yandex Cloud, так и различные наложенные средства для контроля соответствия требованиям в рамках всё той же концепции shift-left. Например, Checkov (<https://github.com/bridgecrewio/checkov>), разработанный компанией BridgeCrew, сканирует конфигурации облачной инфраструктуры, которая управляется в разных средах

виртуализации и контейнеризации таких как Kubernetes и выявляет ошибки с точки зрения безопасности и соответствия требований и стандартов. Также инструмент позволяет написать и добавить собственные проверки, что позволяет контролировать актуальную версию приложения намного эффективнее. Есть в Checkov и автоматическое исправление обнаруженных уязвимостей, что имеет особую практическую значимость на этапе развёртывания уже написанного кода.

С недавних пор Checkov поддерживает Yandex Cloud и содержит целый перечень проверок, которые можно использовать для контроля соблюдения нормативных требований. К примеру, PSI DSS требует в некотором контексте отсутствие наличия публичных IP-адресов для некоторых компонентов или шифрования. Вы можете автоматизировать эту проверку на этапе развёртывания уже написанного кода (рис. 4).

Но кроме Checkov, есть целый набор инструментов, которые дают возможность контролировать соответствие развёрнутой инфраструктуры требованиям безопасности, такие как Falco и Kyverno (рис. 5).

Кроме опенсорс-приложений, можно подключить и корпоративные системы мониторинга. Например, MaxPatrol позволяет контролировать события безопасности в финтех-инфраструктуре. А контролировать соответствие всего облака можно с помощью класса решений CSPM (Cloud Security Posture Management). На российском рынке представлены NeoCat и Cloud Advisor (рис. 6).

Требование PCI DSS	№ проверки	Проверка Checkov
PCI DSS 1.2 PCI DSS 1.3	CKV_YC_1	"Ensure security group is assigned to database cluster."
PCI DSS 1.3.6	CKV_YC_2	"Ensure compute instance does not have public IP."
PCI DSS 3.4	CKV_YC_3	"Ensure storage bucket is encrypted."
PCI DSS 2.1	CKV_YC_4	"Ensure compute instance does not have serial console enabled."
PCI DSS 1.3.6	CKV_YC_5	"Ensure Kubernetes cluster does not have public IP address."
PCI DSS 1.3.6	CKV_YC_6	"Ensure Kubernetes cluster node group does not have public IP addresses."
PCI DSS 6.2	CKV_YC_7	"Ensure Kubernetes cluster auto-upgrade is enabled."
PCI DSS 6.2	CKV_YC_8	"Ensure Kubernetes node group auto-upgrade is enabled."
PCI DSS 3.6.4	CKV_YC_9	"Ensure KMS symmetric key is rotated."
PCI DSS 3.4	CKV_YC_10	"Ensure etcd database is encrypted with KMS key."

Рисунок 4. Соответствие требований PCI DSS с помощью проверок Checkov

Требования стандартов	Osquery	Falco	CiamAV	OPA Gatekeeper / Confest	Kyverno	GitLab (kubesecc)	Aqua Security Enterprise	Sysdig	Luntry	Cilium Enterprise
PCI DSS 2.2.3 Inspect configuration..				✓	✓		✓	✓		
PCI DSS 2.2.3 Активный runtime security на Kubernetes container		❗ ✓ Детект			✓		✓	✓	❗ ✓ Детект	
PCI DSS 2.2.3 Политики на образы: non-root, base image, version of packets				✓		✓	✓	✓		
PCI DSS 2.2.4 Ограничение системных вызовов SYSCALLS	❗ ✓ Детект	❗ ✓ Детект					✓	✓		❗ ✓ Детект
PCI DSS 2.2.4 Построение профиля контейнера (вызовы, файлы, сетевая активность и т. д.) + ограничение	❗ ✓ Детект						✓	✓	✓	
PCI DSS 5.1 Защита от malware внутри контейнеров	❗ ✓ Детект	❗ ✓ Детект	✓				✓	✓	❗ ✓ Детект	
PCI DSS 5.2 Проверка памяти контейнера для защиты от fileless-атак							✓			
PCI DSS 5.1 Защита от malware Kubernetes node	❗ ✓ Детект	❗ ✓ Детект	✓				✓	✓	❗ ✓ Детект	
PCI DSS 10.5.5 FIM файлов на Kubernetes node	✓						✓			
PCI DSS 10.5.5 FIM файлов внутри pods	✓						✓			
PCI DSS 10.1 Экспорт событий	✓	✓	stdout	stdout	✓	✓	✓	✓	❗ ✓	✓

Рисунок 5. Сравнение инструментов безопасности в контексте контролей PCI DSS

Конечно, вы не сможете заменить классические аудиты и другие подходы контроля соответствия требованиям, где требуется человеческий труд. Но упростить людям эту задачу и держать руку на пульсе возможно. Важно исходить из тех требований, которые являются наиболее критичными для архитектуры вашего приложения, и подобрать правильный арсенал для автоматизации контроля требований. Как можно видеть, инструментов немало.

БЕЗОПАСНАЯ РАЗРАБОТКА В ОБЛАКЕ — ЭТО РЕАЛЬНО

Сейчас в разработке складывается такая ситуация, что нужно ускоряться и максимально всё автоматизировать. Что делать с безопасностью? Либо принимать риски, либо вливаться в процесс DevOps, хорошо, что сейчас есть все инструменты для безопасности. С внедрением DevSecOps появляется возможность создавать, разрабатывать и поддерживать безопасные продукты. При этом можно контролировать

степень соответствия требованиям регуляторов и стандартов в условиях динамической среды. Вы также можете автоматизировать задачи безопасности в облаке, где для вас подготовлены готовые инструменты.

Мало того, в текущих условиях, когда некоторые вендоры безопасности ушли с российского рынка, стоит обратить внимание на open-сোর্с-решения. Их полностью хватает для обеспечения задач безопасности на всех этапах жизненного цикла приложений.

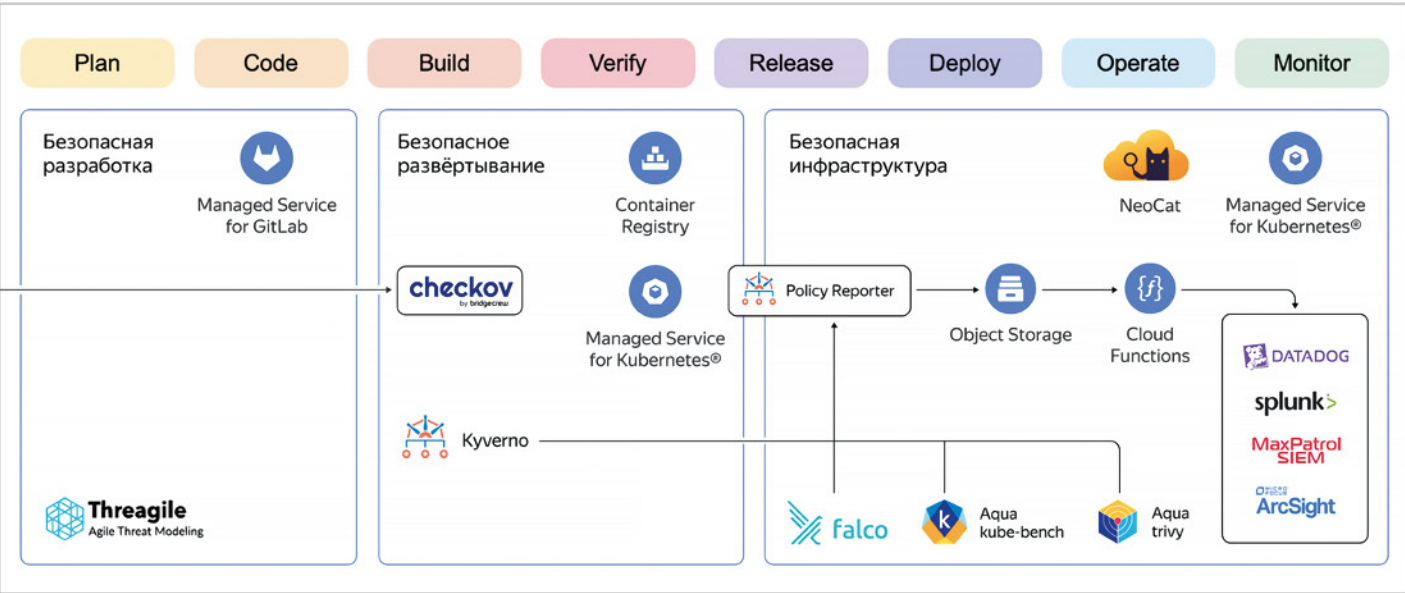


Рисунок 6. Автоматизация задач соответствия требованиям

ЗАЧЕМ МОШЕННИКИ МУЧАТ КОТА ШРЁДИНГЕРА?

ЧТОБЫ ИЗВЛЕЧЬ ВЫГОДУ. АЛЛЕГОРИЯ XXI ВЕКА



Андрей ЖАРКЕВИЧ
эксперт
ООО «Антифишинг»

Квантовая механика — одна из отраслей науки, о которой много говорят, но которую мало кто понимает. Известный эксперимент с котом Шрёдингера, который находится в состоянии «суперпозиции», пока не будет измерен, продемонстрировал, что квантовые явления могут вызывать путаницу даже среди учёных.

Вполне закономерно, что эта путаница привлекла мошенников, активно использующих её для создания новых способов обмана. В этой статье обсудим, как мошенники добрались до квантовой физики и какие квантовые эффекты они используют в своей деятельности.

ОБОЗНАЧИМ ГРАНИЦЫ

Самая эффективная технология для проведения мошеннических кампаний — социальная инженерия. Под этим выражением принято понимать процесс использования научных знаний и методов для изменения поведения и мышления людей в определённых ситуациях. Социальная инженерия может применяться в различных областях, таких как маркетинг, политика, образование, психология.

Управление поведением и мышлением людей, помимо прочего, позволяет убедить их выполнить определённые целевые действия и тем самым добиться результата, нужного выполняющему воздействию. Вполне закономерно, что методы социальной инженерии оказались чрезвычайно востребованы в преступной среде. Ведь угрожать людям нет смысла, если можно просто убедить их отдать свои деньги или сделать что-то ещё.

Основной метод социальной инженерии — воздействие на эмоции, достаточно сильное, чтобы отключить рациональное мышление. При этом эмоции могут быть разные — страх, любопытство, смущение, стыд, радость.

При этом нужно иметь в виду вот что:

1. Нет способа объективно измерить интенсивность эмоций.
2. Сила воздействия эмоций, то есть способность отключить рациональное мышление

и побудить к целевому действию, зависит от конкретных обстоятельств, в которых находится субъект, а также от его душевного состояния.

3. Присутствие рядом других людей оказывает непредсказуемое влияние на спектр и интенсивность возникающих эмоций.

Таким образом, результат воздействия социальной инженерии невозможно рассчитать заранее, оценить его можно лишь непосредственно в момент наблюдения. Получается, что система мошенник — жертва находится в состоянии, чрезвычайно напоминающем квантовую неопределённость.

Сравните:

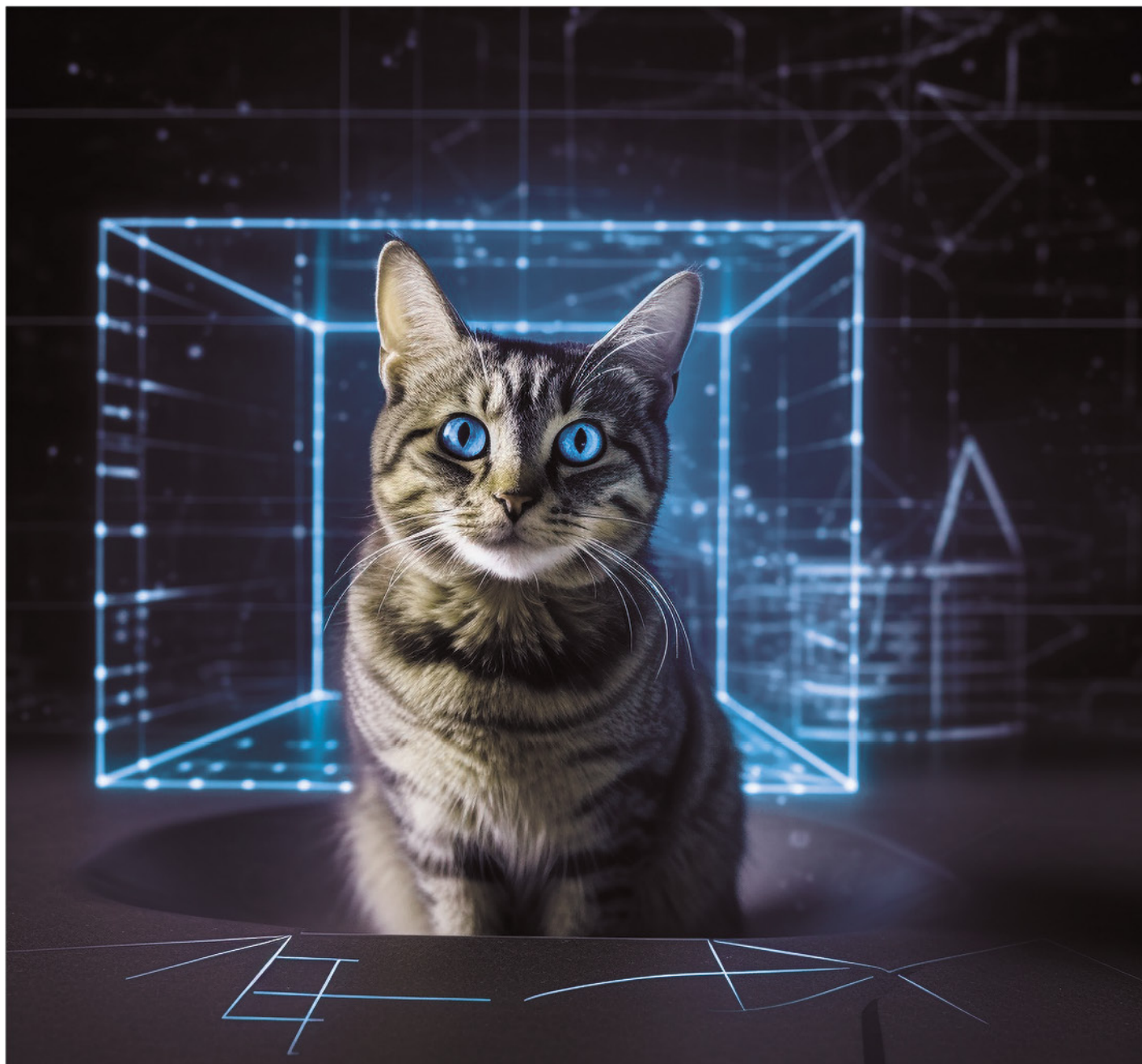
♦ *Кот Шрёдингера*: одновременно жив и не жив до тех пор, пока коробка не открыта. Нет способа определить состояние системы, используя какие-либо её измеримые свойства.

♦ *Жертва социнженерии*: одновременно выполнила и не выполнила целевое действие. Нет способа заранее спрогнозировать результат воздействия, пока оно не произошло.

Квантовая неопределённость означает, что состояние системы нельзя установить, исходя из уникального набора значений для всех ее измеримых свойств. Согласно теореме Кохена — Шпекера, в квантовой механике невозможно, чтобы для данного квантового состояния каждое из измеримых/наблюдаемых свойств имело точное значение. Наблюдаемые значения будут меняться в соответствии с распределением вероятностей, которое однозначно определяется состоянием системы.

Заметим, что состояние социинженерной системы, как и квантовой, разрушается при измерении. Например, в случае со звонком мошенников таким измерением может быть либо включение рационального мышления и трезвая оценка жертвой собственных действий, либо вопрос находящегося рядом человека по поводу действий, которые пытается выполнить жертва.

Таким образом, несмотря на то, что квантовая физика имеет дело с частицами и волнами, а социальная инженерия — с людьми и эмоциями,



Кот Шрёдингера и квантовые эффекты в представлении нейросети Midjourney

имеется довольно заметное сходство в поведении систем, относящихся к таким разным областям знаний. Далее рассмотрим некоторые квантовые эффекты и попробуем спроецировать их на действия мошенников.

КВАНТОВАЯ СУПЕРПОЗИЦИЯ

Квантовая суперпозиция — свойство системы, которое может быть описано как комбинация двух или более возможных состояний, причём эти состояния могут быть совершенно различными. Например, электрон может находиться в суперпозиции двух возможных состояний спина: «вверх» и «вниз» одновременно. При

измерении состояния системы квантовая суперпозиция «рушится», и система «выбирает» одно из возможных состояний.

Аналогию квантовой суперпозиции можно найти в поведении людей, когда они сталкиваются с неопределённой ситуацией и вынуждены принимать решение без чёткого представления о том, какое решение будет наилучшим. Например, при принятии важного решения, человек может ощущать в себе две противоположные точки зрения, и оба варианта для него равноценны.

Например, если человек стоит перед выбором, как поступить с деньгами на счёте во время

звонка мошенников, он находится в состоянии суперпозиции, пока не сделает выбор. При этом он одновременно рассматривать несколько вариантов. Но как только выбор сделан, система «коллапсирует» в конкретное состояние, и человек либо переводит деньги мошенникам, переходя в состояние «жертва», либо кладёт трубку и перезванивает в банк, фиксируя состояние «молодец».

ПОЛЯРИЗАЦИЯ

Поляризация — свойство квантовых частиц (например, фотонов) иметь определённое направление колебаний в электромагнитной волне. Частицы могут быть «поляризованы» вертикально, горизонтально или в другом направлении, в зависимости от способа, которым были созданы. Поляризация фотона может быть измерена с помощью фильтров, пропускающих только частицы определённого типа.

Поляризация в поведении людей может быть связана с их убеждениями и точками зрения. Люди могут быть «поляризованы» в определённом направлении, и, сталкиваясь с информацией, которая не соответствует их убеждениям, могут отвергать её или не замечать. Это может использоваться в социальной инженерии для манипулирования мнениями людей путем представления им определенной информации, которая будет поддерживать их существующие убеждения, в том числе ошибочные.

ЭФФЕКТ НАБЛЮДАТЕЛЯ

Эффект наблюдателя проявляется в том, что измерение состояния системы приводит к коллапсу квантовой суперпозиции в определенное состояние. Другими словами, измерение заставляет систему «выбрать», что с ней происходит или не происходит.

Аналогией этому эффекту в поведении людей может служить, например, влияние ожиданий окружающих на поведение человека. Если человек знает, что другие ожидают от него определённого поведения, то он может изменить поведение в соответствии с этими ожиданиями. Это может проявляться, например, в контексте социальной конформности или социальной нормы, когда люди стремятся соответствовать поведенческим стандартам, принятым в их социальной группе. Люди ведут себя по-разному на работе, где они находятся под наблюдением начальства, и дома, когда никто за ними не наблюдает.

Этим успешно пользуются мошенники, заставляя человека делать выбор и совершать действия в стрессовой ситуации, когда на него

«смотрит вся страна» или «от него зависит сохранность сбережений».

КВАНТОВАЯ ЗАПУТАННОСТЬ

Квантовая запутанность — эффект, при котором два или более квантовых объекта, например, фотона, становятся связанными таким образом, что состояние одного объекта немедленно влияет на состояние другого объекта, даже если они физически удалены друг от друга на большое расстояние.

Мошенники могут использовать похожий эффект, чтобы создать иллюзию подлинности их лживых утверждений. Например, они могут передать одной жертве информацию, полученную от другой. Подобно тому, как изменение состояния одной частицы влияет на другую, действия мошенников могут запутать жертв и вызвать доверие к ним, несмотря на реальные угрозы.

Другая аналогия квантовой запутанности в социнженерии — эмоциональная связь между мошенниками и их жертвами. Например, мошенники могут использовать тактики, направленные на установление доверия с жертвой, такие как симпатия, общность интересов, страх, а также обещание быстрого решения проблемы. Эти тактики могут привести к тому, что жертва будет склонна доверять мошенникам и принимать их предложения, несмотря на рациональные аргументы против.

КВАНТОВЫЙ БЛЕФ

Квантовый блеф (англ. quantum bluffing) — это приём, при котором человек, не имея реального понимания квантовой физики, использует термины и понятия квантовой механики, чтобы создать впечатление своей компетентности и авторитетности. *Этот термин не имеет отношения к квантовой физике* и является формой манипуляции, в ходе которой человек пытается воздействовать на поведение других людей, создавая иллюзию того, что происходит что-то крайне важное и сложное.

Например, можно использовать квантовый блеф, чтобы заставить человека поверить в то, что квантовый компьютер может взломать его пароль, и в результате заставить его изменить свой пароль на более сложный. В этом случае, даже если у человека не было причин менять свой пароль, квантовый блеф может заставить его это сделать на фишинговом сайте, который отправит старый и новый пароль злоумышленникам.

Также мошенники могут использовать термин «квантовое шифрование», чтобы убедить людей в безопасности личной информации. Однако в реальности квантовое шифрование

является сложной технологией, которая на данный момент не применяется в повседневной жизни и не защитит от хакерских атак.

Квантовый блеф может оказывать сильное влияние на поведение людей, особенно если они не имеют достаточных знаний о квантовой физике и не могут определить, является ли утверждение реальным или нет. Это может привести к принятию неправильных решений, например, связанных с инвестициями в ненастоящие квантовые технологии или покупкой дорогостоящего устройства, которое представляется как квантовое, но на самом деле им не является.

В качестве разновидности квантового блефа можно рассматривать известный сценарий с «мастером спорта майором Чингачуком» из несуществующей Службы безопасности Центрального банка, который предлагает перевести деньги на защищённый счёт в государственном хранилище. Не понимая, как работает банковская система, люди проникаются доверием к звонящим, которые свободно оперируют солидными и явно сложными терминами, обещая решение возникшей проблемы.

ШРЁДИНГЕР И ЕГО КОТ

Кот Шрёдингера воплощает в себе сразу два квантовых эффекта — квантовую суперпозицию и эффект наблюдателя. Когда кот находится в закрытом ящике, он находится в состоянии суперпозиции, то есть он одновременно жив и мёртв. Пока ящик не открыт, нельзя узнать, в каком именно состоянии находится кот. С помощью измерения мы «вынуждаем» систему «выбрать» одно из двух возможных состояний. Таким образом, при измерении наблюдатель становится фактором, определяющим, какое из двух состояний станет реальностью.

В случае диалога с мошенниками человек может быть представлен в качестве квантового объекта, который находится в суперпозиции двух возможных состояний — перевести или не перевести деньги. При этом мошенники, которые звонят и просят перевести деньги, могут быть рассмотрены в качестве наблюдателей, которые оказывают влияние на систему, заставляя её сделать выбор.

Разумеется, аналогия с котом Шрёдингера имеет свои ограничения, и использование её в контексте социальной инженерии может быть не совсем точным. В отличие от квантовой системы, человек обладает свободой воли и имеет возможность самостоятельно принимать решения, несмотря на влияние со стороны других людей. Поэтому при анализе ситуаций в социальной инженерии важно учитывать не столько квантовые эффекты, сколько другие факторы,

которые могут влиять на принятие решения человеком:

1. Эмоции и стресс. Человек может быть в состоянии эмоционального стресса, что может повлиять на его способность анализировать ситуацию и принимать обоснованные решения.

2. Предыдущий опыт. Опыт может повлиять на решения человека. Если человеку уже удалось избежать мошенничества в прошлом, то он может быть более скептически настроен и менее подвержен обману.

3. Наличие информации. Человек может принимать решения на основе наличия информации. Если у него есть достаточно информации о мошенничестве, то он может быть более защищён и менее уязвим к подобным аферам.

4. Доверие. Человек может принимать решения на основе своего уровня доверия к человеку, который обращается к нему за помощью. Если человеку кажется, что он общается с человеком, которому можно доверять, то он может быть более склонен довериться ему и сделать то, что ему предлагают.

ЗАКЛЮЧЕНИЕ

Квантовые эффекты, пусть и косвенным образом, могут использоваться в социальной инженерии для следующих видов воздействия на людей:

Создания иллюзии сложности. Квантовые эффекты и явления вполне успешно убеждают жертв мошенников, что происходит что-то крайне сложное и непонятное.

Убеждения в необходимости действий. Например, можно использовать квантовый блеф, чтобы убедить человека сменить пароль или выполнить какие-то другие действия для укрепления безопасности.

Усиления авторитета. Квантовые эффекты могут быть использованы для усиления авторитета и значимости какого-либо события или объекта. Например, можно упомянуть квантовые эффекты, чтобы создать ощущение того, что какой-то продукт или технология являются наиболее современными и передовыми, что может привести к повышению их авторитета и значимости.

В заключение стоит в очередной раз отметить, что чрезвычайно важно на государственном уровне проводить образовательную работу, повышая осведомлённость граждан о возможных угрозах и способах их защиты, а также вырабатывая навыки безопасного поведения. Только так можно обеспечить безопасное использование квантовых технологий и защитить людей от мошенничества, даже если в нём задействован знаменитый кот Шрёдингера.



Ксения ТРОХИМЕЦ
заместитель CSO hh.ru

НА ОДНУ ВАКАНСИЮ ДВА РЕЗЮМЕ

ДЕФИЦИТ ИБ-СПЕЦИАЛИСТОВ ОСЛАБЕВАЕТ НА ФОНЕ ВОССТАНОВЛЕНИЯ СПРОСА

В начале 2023 года спрос на специалистов в сфере кибербезопасности почти восстановился до прошлогодних значений, показали данные hh.ru. При этом восстановление проходит активнее, чем по всей сфере ИТ, а дефицит кадров немного ослабевает. Ксения Трохимец, заместитель CSO hh.ru, специально для BIS Journal рассказала, как чувствует себя рынок труда в кибербезопасности в начале текущего года.

В первом квартале 2023 года компании-работодатели опубликовали на hh.ru в России 7,2 тыс. вакансий в поисках ИБ-специалистов. Это всего на 5% меньше, чем за сопоставимый период 2022 года. Спрос в данной сфере почти восстановился после падения на 22% по итогам прошлого года, и это не единственный позитивный тренд. В сравнении с динамикой вакансий во всей сфере ИТ, которая на текущий момент остаётся всё ещё ниже уровня прошлого года на 20%, кибербезопасность восстанавливается активнее и в соответствии с общим спросом на персонал на всём рынке труда.

Общее количество резюме ИБ-специалистов на hh.ru за рассматриваемый период немногим превышает 30 тысяч, из которых в активном поиске находятся 16,3 тысячи, а каждое

третье резюме со статусом «не ищет работу». Таким образом, конкуренция сегодня составляет два активных резюме на одну вакансию, что является хорошей новостью для работодателей и небольшим ослаблением дефицита. Напомню, что в течение последних двух лет на одну ИБ-вакансию приходилось 0,6–0,8 резюме.

Среди отраслей бизнеса по уровню найма ИБ-специалистов продолжают лидировать ИТ-компании, которые разместили 2,5 тыс. вакансий (+7% к 1 кварталу 2022) и формируют уже свыше трети (35%) всего спроса. Также в плюсе госструктуры (почти 300 вакансий, +45%) и профильные компании, оказывающие b2b-услуги в сфере кибербезопасности (почти 500 вакансий, +10%). Потребность в ИБ-специалистах выросла и в нефтегазовом секторе (330 вакансий, +17%). На фоне ниспадающей активности мошенников в отношении финансового и телеком-секторов падение вакансий от компаний в них выглядит атипичным. В первом падение составило 17%, во втором — наполовину, что сократило долю телекома в спросе на 4 п.п.

В региональном разрезе по сравнению с началом 2022 года также происходят интересные изменения. Так, доля Москвы в генерации

спроса на ИБ приближается к половине — 45% в I квартале 2023 против 40% в I квартале 2022 года. Из первой десятки регионов по числу открытых ИБ-вакансий только в двух зафиксирована положительная динамика — в Москве (+6%) и Татарстане (+7%). Наиболее существенное падение спроса — в Красноярском крае (–32%) и Самарской области (–29%), что отразилось в падении их доли на 1 п.п.

В общем тренде со всем ИТ-рынком находится рост потребности в зрелых специалистах. Так, число вакансий для самых опытных (от 6 и выше лет в сфере) увеличилось на 49%; для тех, кто работает от 3 до 6 лет, — на 7%. И хотя основной объём вакансий (почти каждая вторая) по-прежнему рассчитан на специалистов с опытом 1–3 года, спрос на них немного сократился (–10%), а в не имеющих никакого опыта потребность упала на четверть.

В отношении формата удалённой работы ситуация выглядит стабильной: при найме ИБ-специалистов он не приветствуется, число таких вакансий было в первом квартале 2023 года всего пятьсот (+7%), предложения гибкого и сменного форматов занятости продолжают сокращаться (в среднем на 20%).

«ТРЕБУЕТСЯ СИСАДМИН СО ЗНАНИЕМ ИБ»

ОБОЗРЕВАТЕЛЬ BIS JOURNAL ПОГРУЗИЛСЯ В ПУЧИНУ РЕКРУТИНГОВОГО ПОРТАЛА

Нехватка квалифицированных кадров — постоянная тема ИБ-мероприятий. Там называются цифры в десятки и сотни тысяч вакансий, которые надо заполнить специалистами по кибербезопасности для выполнения Указа № 250, требований регуляторов и просто для закрытия вопросов ИБ в компаниях. Часть рабочих мест ещё только предстоит создать, о чём многие предприятия пока не догадываются.

ТЕНДЕНЦИЯ ОЧЕВИДНА

Итак, обратимся к популярному portalу HeadHunter — крупнейшей российской компании интернет-рекрутмента.

По запросу «информационная безопасность» портал выдаёт 7061 вакансию на начало третьей декады марта 2023 г. При указании специализации «специалист по ИБ» — 2612 предложений. Уточняем запрос: работу «информационная безопасность» ищет человек со средним специальным образованием, опыт и зарплата не указаны. 254 вакансии. Беглый просмотр объявлений показывает: запрос снова придётся уточнять, так как в подборку попадают и менеджеры по работе с клиентами, и бухгалтеры, и медсёстры.

Тенденция очевидна на первом десятке вакансий. Даже на уровне техника ИТ-отдела работодателя хотят видеть традиционного сисадмина-эникейщика, который и сервер настроит, и кабель протянет, и пользователям поможет. Поэтому на него можно повесить и «регулярную реализацию мероприятий по информационной безопасности», и «ответственность за кибербезопасность

компании». Будущий сотрудник должен уметь расставлять приоритеты и быть стрессоустойчивым.

Пример? Городская больница среднего города. Несколько вакансий системного администратора в отдел ИТ, требования классические, но в середине списка мелькают «базовые знания по ИБ». Вакансий специалистов по кибербезопасности в больнице нет. Вспоминаются хакерские атаки на систему здравоохранения США (снизу доверху) и утечки конфиденциальных сведений. Для российского города атака на больницу будет чувствительной. А полное описание программно-аппаратных комплексов и ИС из вакансии станет отличным подспорьем для атакующих. Но кто об этом думает?

Другая вакансия. Компания описывает себя как подрядчика крупных организаций. Среди обязанностей сисадмина — обеспечение надёжного функционирования и развития внутренней ИТ-инфраструктуры предприятия, а также обеспечение ИБ, оценка рисков и угроз, разработка мер ИБ, тестирование уязвимостей; плюс повышение надёжности и защищённости, сокращение издержек ИТ... Прочие задачи — техподдержка пользователей и создание новых АРМ, закупка

оборудования и расходников, диагностика, ремонт, инвентаризация... Тут не до мониторинга киберрисков, успеть бы МарьИванне компьютер настроить. Лучше места для начала атаки третьей стороны на заказчиков этого подрядчика не найти.

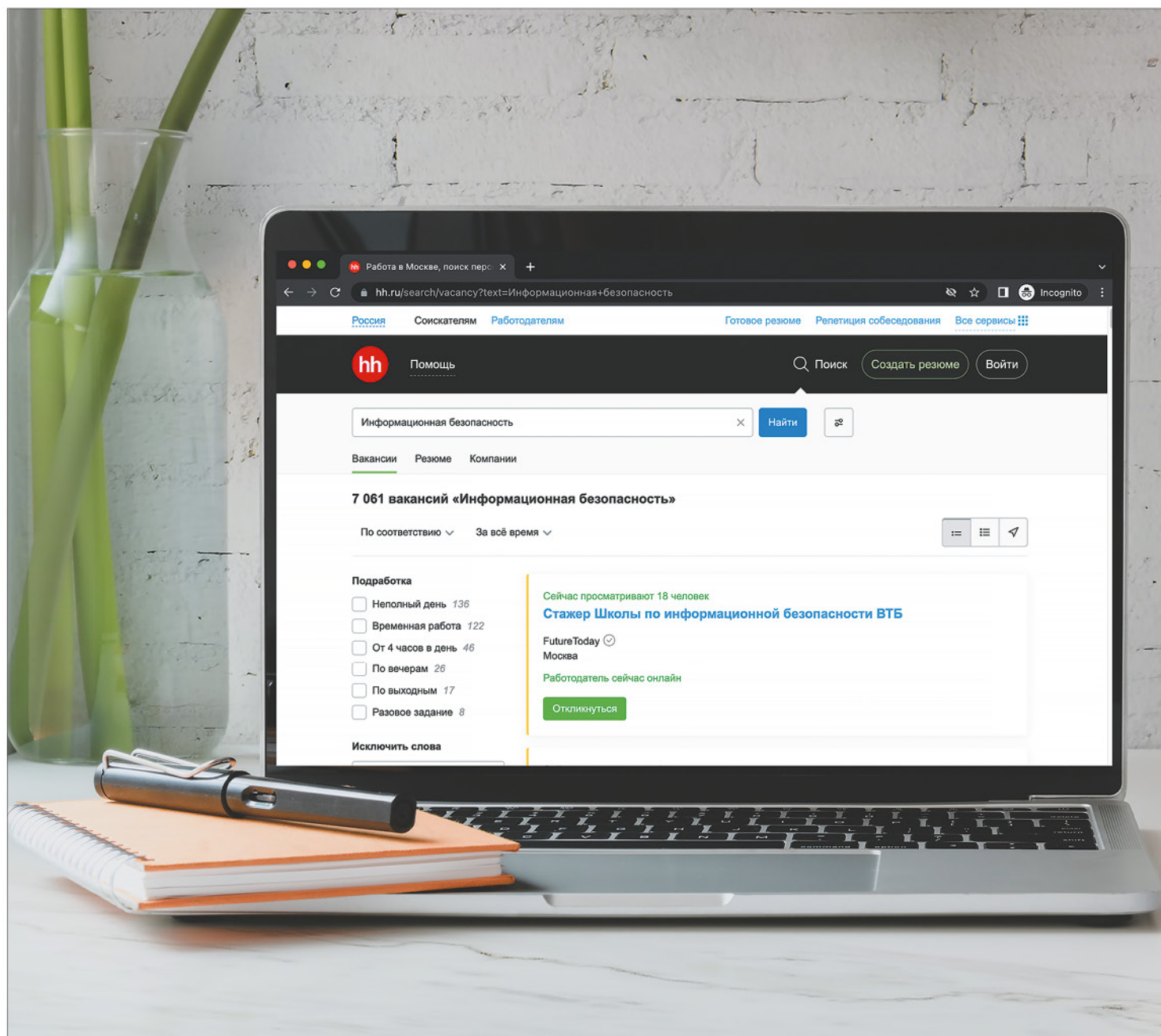
Ещё пример. В вакансии ведущего специалиста по ИБ одной госкорпорации описаны классические требования для сотрудника ИТ-подразделения. И видно, для отчёта проверяющим добавляется: «Специалисты по кибербезопасности в штатном расписании есть».

Зарплаты везде разные, старт от 30 тыс. рублей, чаще — по итогам собеседования. Если сузить поиск до Москвы, то молодого специалиста по ИБ со средним техническим образованием и минимальным опытом работы (6 месяцев или стажировки в период учёбы) ищут в федеральном ведомстве. В обязанности сотрудника входят только вопросы ИБ. Зарплата — 50–60 тыс. руб., премии, соцпакет, возможность профессионального роста.

С ВЫСШИМ ОБРАЗОВАНИЕМ...

Следующая выборка — специалист по ИБ с высшим образованием из России без указания уровня зарплаты. Выпадает 3664 вакансии, первые же

Тенденция очевидна на первом десятке вакансий. Даже на уровне техника ИТ-отдела работодателя хотят видеть традиционного сисадмина-эникейщика, который и сервер настроит, и кабель протянет, и пользователям поможет



предложения — менеджеры по продажам в крупных компаниях-интеграторах ИБ-решений, для которых знание профильной области — преимущество при трудоустройстве. Далее идут инженерные должности в банках и компаниях, работающих в области кибербезопасности.

Есть и редкие исключения, например спрос на направление инфобеза со стороны налогового ведомства. Его структуры активно ищут специалистов, готовых разработать документацию в области ИБ, провести внедрение и администрирование систем и СЗИ.

А также готовых на практике обеспечивать киберзащиту ресурсов и участвовать в аудите ИБ. Среди других предложений — операторы ЦОД, работающего в режиме 24/7.

Несколько работодателей — учебные заведения, фармкомпания и компании нефтегазового комплекса, подрядчики госкорпораций — находятся в поиске опытных специалистов, которые займутся обеспечением соответствия ИС требованиям законодательства в области ИБ, практическим внедрением, администрированием, сопровождением эксплуатируемых СЗИ. В ряде случаев

соискатель должен уметь взламывать и защищать внутренние корпоративные сети и сайты работодателя.

Если поставить максимально привередливые условия поиска — специалист по ИБ с высшим образованием, опытом работы от 6 лет и желаемым доходом от 150 тыс. руб., то портал показывает всего несколько десятков вакансий, и по ним можно проследить тенденции, отбросив банки и профильные ИБ-компании.

Ряд ИТ-компаний, работающих с середины 2010-х гг., «внезапно» вспомнили о кибербезопасности своих



Популярную тему инфобеза включают в резюме как специалисты в ИТ, так и специалисты в пожарной безопасности и даже сотрудники ЧОПов — таких минимум треть от всех претендентов

так и для её сервисов, возглавить отдел ИБ в компании нефтеперерабатывающего холдинга или перспективной энергетической компании, сосредоточить внимание на взаимодействии с госорганами и регуляторами, создать SOC и перейти на российские СЗИ. Обещают платить от 250 до 350 тыс. рублей ежемесячно.

Интересна вакансия по защите КИИ одной из городских служб города федерального значения. Необходим опыт работы с автоматизированными системами управления технологическими процессами (АСУ ТП), разработка вариантов архитектурных и технических решений подсистем защиты АСУ ТП, выявление угроз безопасности объектов КИИ и участие в расследовании инцидентов кибербезопасности. Правда, зарплата за всё это — 90 тыс. рублей. Льготы и поощрения — после года ударной работы.

ПРО СОИСКАТЕЛЕЙ

На что рассчитывают соискатели? Задаём критерии поиска: «граждане России, специалисты ИБ, ищут работу и рассматривают предложения по России». Таковых 962 человека, более 500 из них — в активном поиске.

Популярную тему инфобеза включают в резюме как специалисты в ИТ, так и специалисты в пожарной безопасности и даже сотрудники ЧОПов — таких минимум треть от всех претендентов. Резюме, имеющие прямое отношение к ИБ, начинаются в четвёртой сотне. Желаемый уровень зарплаты такого специалиста (настоящего ибэшника) из региона со стажем более 15 лет, не готового к переезду, — 45–50 тыс. рублей. На такую же зарплату претендует и молодой специалист из крупного города. Он получил профильное ИБ-образование, видел, как работают с аппаратно-программными комплексами шифрования, «знаком с СЗИ», но его

интересы лежат в области дизайна или фотографии, о чём он честно пишет. Уровень зарплатных ожиданий таких «специалистов» растёт с уменьшением возраста и приближением к большим городам.

В ценовой группе с зарплатами от 90 тыс. рублей среди сисадминов и сотрудников техподдержки всё-таки можно найти и специалистов по ИБ. Имеющие опыт работы от 10 лет оценивают себя в 130 тыс. рублей и выше. Здесь и больше резюме, авторы которых уже ведут переговоры с работодателями.

ВЫВОДЫ

Какие выводы можно сделать, просмотрев вакансии и резюме по ИБ на портале hh.ru?

- ◆ Число вакансий почти в три раза превышает число резюме соискателей, а с учётом отсева — более чем в четыре раза.

- ◆ Основные потребители квалифицированных кадров — компании, работающие в области ИБ, финансовые организации, разработчики и поставщики комплексных ИТ- и ИБ-решений.

- ◆ Многие работодатели, особенно малый и средний бизнес, не понимают различия между ИТ- и ИБ-секторами и пытаются нагрузить сисадминов вопросами кибербезопасности разного уровня сложности.

- ◆ Многие соискатели не понимают различия между ИТ- и ИБ-секторами и пытаются «продать» себя подороже, не имея опыта работы в области кибербезопасности.

- ◆ Организации госсектора, крупные компании начинают интегрировать информационную безопасность в бизнес-системы.

- ◆ Ряд компаний, работающих в критически значимых секторах экономики, «вспомнили» про ИБ и срочно планируют выполнять требования регуляторов. Хотя это радует.

продуктов и срочно ищут руководителей ИБ направлений. Кто-то начнёт с базовых мер — анализа и оценки состояния ИБ в компании определения ресурсов, подлежащих защите, определения требований по защите информации для ранее созданных и новых ИС... Один работодатель скромно упоминает «более 850 сервисов для автоматизации бизнеса» в своём портфеле решений, которые неплохо бы защитить.

Работодатели ищут желающих возглавить новое ИБ-направление в системном ИТ-интеграторе и сформировать стратегию ИБ как для компании,

С УЧЁТОМ НАЦИОНАЛЬНЫХ ОСОБЕННОСТЕЙ

В МИРЕ ВСЁ БОЛЬШЕ УЧЕБНЫХ ПРОГРАММ
ПО КИБЕРБЕЗОПАСНОСТИ РАЗРАБАТЫВАЕТСЯ С УЧЁТОМ
МЕСТНОЙ ИДЕНТИЧНОСТИ ЖИТЕЛЕЙ

ФИНСКИЙ ПРОЕКТ: ИБ ТАКАЯ РАЗНАЯ!

Финляндия запустила проект Cyber Citizen — результат совместной работы Университета Аалто и Министерства транспорта и коммуникаций. Его цель — создание общей модели обучения навыкам кибербезопасности граждан государств — членов ЕС.

Проект Cyber Citizen направлен на создание учебного портала, который будет включать контент, ориентированный на различные целевые группы. Портал будет предоставлять образовательные и коммуникационные элементы для повышения киберграмотности граждан в цифровом мире. В рамках проекта разрабатывается игра для обучения навыкам кибербезопасности.

Проект получил трехлетнее финансирование в размере €5 млн от Фонда ЕС по восстановлению и жизнестойкости.

Первый этап проекта включал исследование текущего состояния дел в сфере обучения навыкам кибербезопасности граждан во всех странах ЕС. В итоговом отчете подчеркивается, что ИБ воспринимается по-разному жителями разных стран. И хотя повседневная цифровая жизнь становится неотъемлемой частью жизни, восприятие знаний и навыков, связанных с кибербезопасностью, значительно варьируется от одной страны ЕС к другой.

Исследование показало, что в странах Европы есть желание развивать навыки граждан в области ИБ и поддерживать обучение на протяжении жизни. Однако различия между целевыми группами ещё недостаточно изучены и требуют дополнительных исследований. Сказывается и тот факт,

что руководящие принципы стратегического обучения в области ИБ в странах ЕС появились относительно недавно.

На втором этапе проекта Cyber Citizen будет разработана модель обучения граждан навыкам кибербезопасности, а на третьем этапе — создан учебный портал, разработаны игры и начато производство другого контента. Геймификация обучения станет неотъемлемой частью учебного портала, поскольку исследование показало, что игры зарекомендовали себя важной формой обучения.

Дальнейшая работа по проекту включает создание европейской сети сотрудничества, включающей все заинтересованные в развитии у граждан навыков в ИБ компании.

Проект Cyber Citizen является важным шагом в решении проблем просвещения в области кибербезопасности и киберзащиты простых граждан в цифровом мире, пишет Helsinki.

С ИРЛАНДСКИМ АКЦЕНТОМ

Британская компания по обеспечению информационной безопасности NCC Group PLC объявила о заключении соглашения о трёхлетнем партнёрстве в области кибербезопасности с HEAnet, ирландской образовательной и исследовательской сетью. В NCC уже заявили о возможности продлить партнёрство ещё на семь лет.

Компания Fox-IT (Нидерланды), входящая в состав NCC Group, будет предоставлять круглосуточную информацию о безопасности и управление событиями, а также услуги по обеспечению безопасности для клиентов HEAnet. Два года назад Fox-IT запустила аналогичную услугу в Голландии

вместе с компанией SURF. По словам представителя NCC, опыт такого партнёрства использован для того, чтобы ирландский сектор образования и исследований получал новейшие высококачественные услуги в области кибербезопасности.

Ронан Бирн, главный исполнительный директор HEAnet, отметил, что Fox-IT предлагает расширенный спектр услуг кибербезопасности клиентам HEAnet и имеет большой опыт работы в этой области. «Безопасность является одним из стратегических столпов HEAnet, учитывая растущий спрос клиентов на услуги, которые необходимо ежедневно защищать от кибератак. Предоставление отраслевых услуг SOC и SIEM поможет нашим клиентам снизить киберриски и связанные с этим перерывы в работе», — отметил представитель HEAnet.

HEAnet — национальная образовательная и исследовательская сеть Ирландии. Услуги электронной инфраструктуры HEAnet поддерживают примерно 210 тыс. студентов и сотрудников в Ирландии и примерно 800 тыс. студентов и сотрудников, пользующихся сетью HEAnet.

СПЕЦИАЛЬНО ДЛЯ МАОРИ

Крупнейшая организация в области профессионального образования, новозеландский институт навыков и технологий Te Pūkenga присоединился к компаниям Microsoft, Turoto и Te Whatu Ora, чтобы совместными усилиями восполнить нехватку квалифицированных экспертов по кибербезопасности и привлечь в отрасль коренных жителей региона.

Учреждение профессионального образования разрабатывает программу подготовки в области кибербезопасности. Платное обучение за счёт микрокредита будет включать работу в кампусе и на рабочем месте. Учащиеся смогут получить должности начального уровня в сфере кибербезопасности в организациях Новой Зеландии.

Социальная организация Tiroto, которая занимается программами летней стажировки в корпоративном секторе для студентов вузов из числа маори и жителей тихоокеанского региона, сотрудничает с Microsoft в рамках глобальной инициативы.

Ранее институт Te Pūkenga и Агентство общественного здравоохранения Te Whatu Ora разработали индивидуальную образовательную программу по кибербезопасности для всех новозеландцев, отражающую инклюзивные ценности, чтобы сделать её доступной для людей всех культур. Te Whatu Ora готова взять до 10 учеников в рамках программы.

«Пандемия ускорила темпы цифровизации, и это открывает огромные возможности для амбициозных людей, строящих карьеру, — считает Ванесса Соренсон, управляющий директор Microsoft в Новой Зеландии. — Кибербезопасность — это не просто технические навыки. Нам нужны люди, которые понимают человеческую психологию или могут научиться важным навыкам безопасности. Поэтому мы хотим открыть двери возможностей как можно шире».

НА ЯЗЫКЕ МАЛЕНЬКОГО АРАБА

Национальное агентство кибербезопасности Катара в сотрудничестве с Министерством образования и высшей школы запустило проект «Образовательная программа по кибербезопасности».

Проект «Образовательная программа по кибербезопасности» разработан под патронажем премьер-министра и министра внутренних дел страны шейха Халида бен Халифы бен Абдель Азиза Аль Тани и направлен на достижение ряда целей, среди которых выделяют знакомство общества с концепцией цифрового гражданства, которая заключается в ответственном, этичном и безопасном использовании



Здание Национального агентства кибербезопасности Катара

информационных и коммуникационных технологий. Программа расскажет об опасностях в интернете и защите персональных данных, повысит осведомлённость об общих концепциях, связанных с кибер- и цифровой безопасностью. Отдельная тема — профессиональная подготовка молодёжи.

Глава Агентства кибербезопасности Катара Абдурахман бин Али Аль Фарахиди аль Малки сказал, что этот проект реализуется с целью повышения осведомлённости граждан о киберрисках, построения кибербезопасного общества, способного противостоять будущим вызовам, сопровождающим технологическую революцию, свидетелями которой является мир.

«Наше партнёрство с Министерством образования привело к созданию инновационного национального проекта. Это первый подобный проект в регионе, он ориентирован на учащихся школ, учащихся с ограниченными возможностями, предназначен для дополнительного образования и повышения грамотности, чтобы обеспечить распространение кибернетической осведомлённости во всём сообществе», — добавил чиновник.

В рамках проекта запущена цифровая платформа, которая включает всю информацию о программах. Они доступны для студентов в любое время. Обучение кибербезопасности будет плавным и приятным, оно даст пользователю всю информацию и заставит его искать больше сведений, подчеркнул Аль Малики.

Проект учебной программы по кибербезопасности включает визуальный контент, который содержит более пятидесяти образовательных анимационных видеороликов, учитывающих национальную идентичность Катара и одобренных Министерством образования.

Видеоролики ориентированы на учащихся трёх ступеней: начальной, подготовительной и средней — и учитывают разницу в когнитивном уровне детей в зависимости от каждой возрастной группы.

Учебная программа также включает набор плакатов и инфографики. Агентство стремилось сформулировать чёткое видение процессов ИБ и выбрало опытную команду для подготовки образовательного контента.



Марина БРОДСКАЯ
обозреватель BIS Journal

ГЛОБАЛИЗАЦИЯ КИБЕРБЕЗОПАСНОСТИ

СТРАНЫ И ПРАВИТЕЛЬСТВЕННЫЕ АГЕНТСТВА
ОБЪЕДИНЯЮТСЯ ПЕРЕД ЛИЦОМ НОВЫХ ХАКЕРСКИХ
УГРОЗ, КИБЕРШПИОНАЖА И СЕРВИСОВ

ПОД КОНТРОЛЕМ MI5

Правительство Великобритании объявило о создании нового агентства безопасности — Национального управления безопасности (NPSA), которое поможет организациям защититься от потенциальных угроз национальной безопасности, включая поддерживаемый иностранными государствами кибершпионаж. NPSA будет контролироваться внутренним агентством контрразведки и безопасности MI5 и сотрудничать с существующими органами, включая Национальный центр

кибербезопасности и Национальное управление по борьбе с терроризмом, чтобы предоставлять комплексные рекомендации по безопасности.

NPSA берёт на себя обязанности Центра защиты национальной инфраструктуры (CPNI), но с более широкими полномочиями, поскольку угрозы хакеров, поддерживаемых иностранными государствами, распространяются на такие организации, как научно-технические фирмы и исследовательские институты, которые не классифицируются как критически важная

инфраструктура. Правительство заявило, что поддерживаемый иностранными государствами кибершпионаж может подорвать британский бизнес и нанести ущерб его конкурентоспособности на мировой арене.

«Наука, технологии и академические круги находятся на переднем крае национальной безопасности не меньше, чем важнейшая инфраструктура Великобритании, — сказал министр безопасности Том Тугендхат. — Мы знаем, что враждебно настроенные субъекты пытаются украсть интеллектуальную собственность британских учреждений, чтобы навредить стране. Национальное управление безопасности будет играть решающую роль, помогая предприятиям и университетам лучше защищать себя и сохранять конкурентные преимущества».

Ранее генеральный директор MI5 Кен МакКаллум говорил о растущей угрозе для британских компаний, которую создаёт шпионаж, в частности, со стороны китайских хакеров. История их деятельности длительная и включает кражу интеллектуальной собственности, академических исследований, а также получение конфиденциальной информации путём шпионажа и контакты через деловые социальные сети.

Россия и Иран также известны своей активностью в области шпионажа,



Штаб-квартира MI5 в Лондоне

они используют различные методы компрометации лиц, представляющих интерес для разведывательных целей. Однако первенство принадлежит Китаю. Недавнее исследование, проведенное экспертом по Китаю Чарли Партоном, показало, что технологические компании КНР используют компоненты в устройствах интернета вещей для слежки за пользователями.

NPSA заявила, что будет давать рекомендации в «доступной и информативной» форме, доступной широкому кругу лиц, от маленьких стартапов до ведущих университетов.

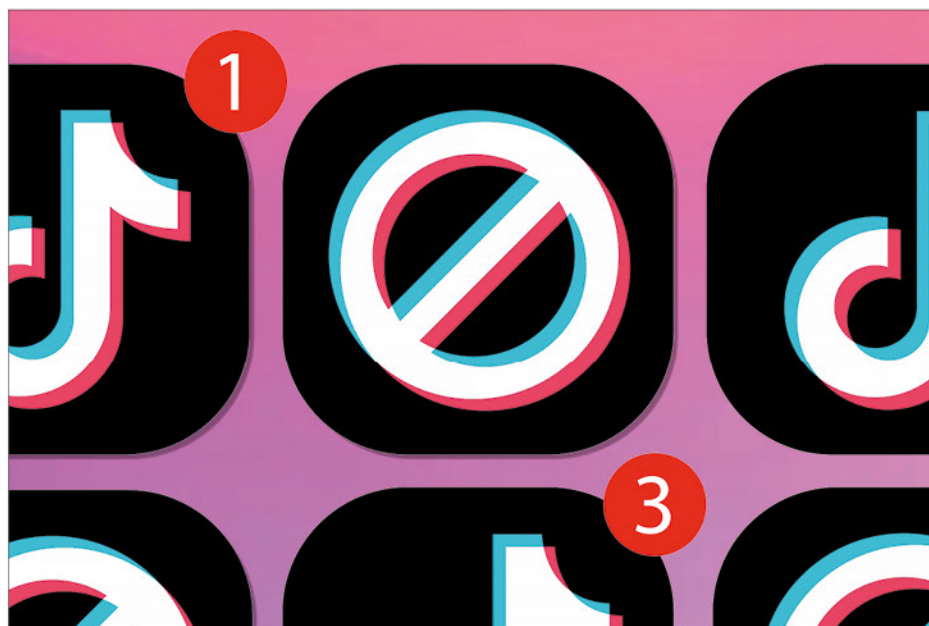
Цель Агентства — предоставить обучение и рекомендации по мерам, которые организации должны принять, чтобы помочь решить проблему шпионажа. NPSA уже выпустило руководство, охватывающее вопросы кибербезопасности и безопасности оборудования для видеонаблюдения. Также вышло мобильное приложение Think Before You Link, которое поможет пользователям ряда социальных сетей идентифицировать черты фальшивых профилей, используемых злоумышленниками, чтобы заманить свои жертвы на компрометацию. Приложение было запущено в прошлом году предшественником NPSA — CPNI.

Создание NPSA является частью Комплексного обзора безопасности 2023 года (IR23), представленного премьер-министром Великобритании Риши Сунаком на встрече с президентом США Джо Байденом и премьер-министром Австралии Энтони Альбанезе.

МИР ОПОЛЧИЛСЯ НА ТИКТОК

Социальная сеть коротких видеороликов TikTok готова отделиться от материнской компании ByteDance, пишет агентство Bloomberg. На такие крайние меры сервис готов пойти, чтобы не попасть под запрет в США. Разделение компаний произойдет только в том случае, если разработанный ранее план Project Texas не будет одобрен.

Разговоры о полном запрете социальной сети TikTok в США ведутся давно, в прошлом стороны разработали план Project Texas, учитывающий национальную безопасность Соединенных Штатов. Для хранения и обработки данных пользователей TikTok на



территории США планируется привлечь мощности корпорации Oracle, курировать деятельность соцсети должен специальный комитет, состоящий из трёх человек. Если план не сработает, а он уже встретил противодействие со стороны федеральных ведомств США, ByteDance готова продать TikTok или вывести его на публичное размещение акций. Однако сделка всё равно потребует одобрения правительства КНР, что усложняет процесс переговоров.

Запрет на установку приложения TikTok на рабочие телефоны введён в государственных и правительственных учреждениях Австралии, Канады, Индии, структурах ЕС, Еврокомиссии и странах Евросоюза. С предложением проверить приложение на безопасность в Национальный центр кибербезопасности Великобритании обратился министр безопасности Том Тугендхат. Парламент Великобритании закрыл свой аккаунт в сервисе в 2022 г. после того, как депутаты выразили обеспокоенность по поводу связей компании TikTok с правительством Китая.

В Соединённых Штатах рассматривается законопроект, предусматривающий полный запрет TikTok на территории страны, при этом он уже запрещён в ряде штатов и непосредственно Конгрессе США. Беспокойство чиновников всех стран вызывают не столько вопросы сбора и защиты данных пользователей, сколько возможные связи

компании с Коммунистической партией Китая и продвижение пропекинских взглядов.

О попытках Китая использовать TikTok для распространения нужной ему информации на Тайване и создания угрозы национальной безопасности Тайваня сообщает Taipei Times. Ранее правительство запретило использование платформы коротких видеороликов Douyin, китайской версии TikTok, на служебных гаджетах.

Представители сервиса TikTok называют все запреты «ошибочными и основанными на фундаментальных заблуждениях». По их мнению, запрет TikTok или его отделение от ByteDance в США не будут иметь ничего общего с обеспечением интересов национальной безопасности.

СЕВЕРОКОРЕЙСКИЕ ХАКЕРЫ ПРЕДЛАГАЮТ «РАБОТУ МЕЧТЫ» БЕЗОПАСНИКАМ

С лета 2022 г. исследователи компании Mandiant отслеживают хакерскую кампанию, нацеленную на западные СМИ и технологические компании. В проведении кампании подозревают северокорейскую шпионскую группу, получившую название UNC2970. Однако с большой долей вероятности это UNC577, также известный как Temp. Hermit. UNC577 — это кластер северокорейской киберактивности, который был активен как минимум с 2013 г.,

говорится в сообщении Mandiant. UNC2970 имеет много общего вредоносного ПО с другими операторами КНДР. И хотя активность UNC577 в первую очередь нацелена на компании Южной Кореи, она также атакует организации по всему миру.

В июне 2022 года Mandiant Managed Defense обнаружила фишинговую кампанию UNC2970, нацеленную на технологические компании США. UNC2970 использует три новых семейства кодов: TOUCHMOVE, SIDESHOW и TOUCHSIFT. Mandiant подозревает, что эти злоумышленники специально предназначались для исследователей безопасности. Позднее Mandiant зафиксировал многочисленные атаки UNC2970 на американские и европейские СМИ с помощью целевого фишинга. UNC2970 исторически рассылает адресные фишинговые электронные письма с темой «поиск работы» в рамках операции «Работа мечты». Хакеры использовали тему найма на работу и в данном случае, а также демонстрировали способности работать в облачных средах и противостоять инструментам Endpoint Detection and Response (EDR).

Недавно UNC2970 сменил тактику и перешёл на использование фейковых аккаунтов LinkedIn, якобы принадлежащих рекрутерам. Учётные записи профессионально разработаны и имитируют личности реальных людей, чтобы обмануть жертвы и повысить шансы на успех кибератаки.

Используя методы социальной инженерии, хакеры добиваются взаимопонимания с жертвой. После чего пытаются перевести разговор в WhatsApp, чтобы затем использовать либо сам мессенджер, либо электронную почту для доставки под видом теста при приёме на работу или должностной инструкции бэкдора Plankwalk, а также других семейств вредоносных программ, в которых прослеживается код и инструменты, используемые ранее UNC577.

Бэкдор Plankwalk, написанный на основе C++, обменивается данными через HTTP и использует несколько уровней боковой загрузки DLL для выполнения зашифрованной полезной нагрузки. Plankwalk первоначально запускается через программу запуска, которая импортирует и выполняет программу

запуска второго этапа, прокладывая путь для распространения дополнительных инструментов, в т.ч. кейлоггеров и утилиты для создания скриншотов и полнофункциональных бэкдоров.

Выявленные новые инструменты вредоносных программ указывают на продолжающуюся разработку вредоносных и развёртывание новых инструментов UNC2970, отмечают исследователи Mandiant. Если группа ранее нацеливалась на оборонные предприятия, СМИ и технологические отрасли, то смещение целей на исследователей в области ИБ предполагает изменение стратегии или расширение её деятельности. Также отмечается, что группа адаптирует свои возможности по мере того, как всё больше их целей переходят на облачные сервисы.

Для противостояния хакерам Mandiant рекомендует компаниям рассмотреть средства и методы защиты, включая блокировку макросов и использование привилегированного управления идентификацией, политику условного доступа и ограничений безопасности в Azure AD. Также рекомендуется требовать подтверждения транзакций InTune несколькими администраторами.

ПРИНЦИП SECURE BY DESIGN СО СТУДЕНЧЕСКОЙ СКАМЬИ

Джен Истерли, глава Агентства по кибербезопасности и защите инфраструктуры США (CISA), призвала переходить к принципу Secure by Design с университетского уровня. Методы безопасного кодирования и современные языки программирования, безопасные для памяти, должны быть включены в учебную программу по информатике, считает она.

«Студенты должны быть хорошо осведомлены о безопасности, в том числе о безопасности памяти и методах безопасного кодирования. И профессора играют здесь важную роль, — написала Истерли в своём блоге. — Шаги, предпринятые сегодня в университетах по всей стране, могут помочь стимулировать общепрофессиональные изменения в сторону языков, безопасных для памяти, и повысить качество тестирования при разработке программного обеспечения, что, в свою очередь, защитит всех пользователей технологий».

По словам Истерли, переход к практике Secure by Design потребует серьёзных изменений в методах разработки технологических продуктов, что отразится на коде, используемом при разработке программного обеспечения. Производителям технологий необходимо изменить способ разработки новых продуктов, чтобы тратить меньше времени на исправление ошибок. Это даст больше времени для инноваций и роста. При этом бремя безопасности никогда не должно ложиться на потребителей.

Производители технологий должны обеспечить полную прозрачность и быстро сообщать о проблемах безопасности. Им также следует составить дорожную карту, показывающую планы разработки и обновления продуктов, чтобы убедиться в их фундаментальной безопасности и в безопасности по умолчанию.

CERT ИНДИИ ОТЧИТАЛСЯ О РАБОТЕ

В течение 2021 и 2022 гг. в Индии было зарегистрировано 1 402 809 и 1 391 457 инцидентов кибербезопасности. В 42 из 50 инцидентов, соответственно, произошёл взлом веб-сайтов, принадлежащих центральному правительству и правительствам штатов, заявил министр по электронике и информационным технологиям Индии Раджив Чандрасекар во время выступления в парламенте страны.

Чандрасекар также заявил, что CERT-In уведомил пострадавших и скоординировал меры реагирования на инциденты с подвергшимися атакам организациями, поставщиками услуг, отраслевыми регуляторами, правоохранительными органами.

По словам Раджива Чандрасекара, для сокрытия источников, с которых злоумышленники осуществляют атаки, они используют скомпрометированные компьютерные системы, расположенные в разных частях мира, и «используют методы маскировки и скрытые серверы».

По словам министра, злоумышленники продолжают разрабатывать новые стратегии атак, используют общеизвестные уязвимости, крадут учётные данные из служб удалённого

доступа, проводят фишинговые операции для получения доступа к инфраструктуре предприятий в различных отраслях.

«Инновации в технологиях, рост цифровой инфраструктуры, переход в киберпространство бизнеса и услуг приводит к увеличению числа кибератак, создаёт угрозу конфиденциальности, целостности и доступности данных и услуг, что может оказать прямое или косвенное влияние на экономику бизнеса и поставщиков услуг, — отметил Чандрасекара. — Такое экономическое воздействие специфично для пострадавшей организации и зависит от степени воздействия на её инфраструктуру в ходе кибератаки, в том числе на сервисы, данные и активы».

Правительство Индии работает над несколькими законопроектами для защиты киберпространства страны, напомнил Чандрасекар парламентариям. Он отметил, что правительство не только осведомлено об угрозах, но и стремится к тому, чтобы интернет был доступным, заслуживающим доверия и подотчётным для пользователей.

ЛАТВИЯ ГОТОВИТСЯ К КИБЕРВЫЗОВАМ

Правительство Латвии одобрило проект «Стратегии кибербезопасности Латвии на 2023–2026 годы», разработанный Министерством обороны страны. Документ определяет основные направления действий национальной политики кибербезопасности и будущие вызовы.

Выделены пять основных направлений действий: улучшение управления кибербезопасностью; продвижение кибербезопасности и повышение киберустойчивости; информирование общественности, образование и исследования; международное сотрудничество и правосудие в киберпространстве; предотвращение киберпреступности и борьба с ней.

«Задача Латвии состоит в том, чтобы укрепить свою кибербезопасность как путём улучшения управления кибербезопасностью и содействия международному сотрудничеству, так и путём повышения осведомлённости общественности и усиления реагирования и активных возможностей



Массовая компьютеризация и стремительный рост цифровой инфраструктуры в Индии привели к увеличению числа кибератак и угрозе для экономики страны

учреждений», — заявила министр обороны Латвии Инара Мурниеце.

Стратегия кибербезопасности была разработана в соответствии с действующим законодательством Европейского союза. Национальный центр кибербезопасности (CERT.LV) сформирует ядро национальной системы управления кибербезопасностью совместно со службой безопасности Бюро защиты конституции (SAB).

ЦЕНТРЫ КИБЕРМАСТЕРСТВА

По решению Министерства внутренней безопасности и АНБ США Университет Святого Франциска в шт. Пенсильвания, округ Камбрия, стал Национальным центром академического мастерства в области киберзащиты (CAE-CD). Здесь можно получить степень бакалавра наук в области администрирования кибербезопасности, упор на ИБ сделан и в других основных направлениях обучения. Университет предлагает обучение кибербезопасности и через Образовательный центр по киберзащите.

Статус CAE-CD получила и Школа уголовного правосудия, разведки и кибербезопасности — факультет SUNY Canton, колледжа Северного Нью-Йорка. Ранее четырёхлетняя программа кибербезопасности Школы получила одобрение Агентства национальной безопасности (NSA).

«Высококвалифицированная рабочая сила в области кибербезопасности — это стратегическое преимущество в сфере национальной безопасности, — считает руководитель программы NSA

САЕ Энни Беккер. — Правительство США продолжит инвестировать и совершенствовать программы, которые готовят профессиональные кадры на всех уровнях обучения, от начального до высшего образования».

Кибербезопасность стала одной из популярных программ в колледже: по состоянию на осень 2022 г. здесь обучалось 202 студента. В 2018 г., когда программа только стартовала, на неё поступили всего 13 студентов. За эти годы рост составил 1400%, отмечает руководство учебного заведения. Большой популярностью пользуется только курс Управления здравоохранением, на котором обучается 242 студента. Обе программы доступны онлайн с возможностью выбора личного или гибкого класса.

Программа CAE-CD спонсируется АНБ и Министерством внутренней безопасности США. Она призвана решить проблему острой потребности страны в квалифицированных специалистах по ИБ, разработана для снижения уязвимости национальной информационной инфраструктуры и содействует развитию высшего образования и исследованиям в области киберзащиты.

Колледжи и университеты, получившие статус CAE-CD, официально признаны правительством США, их учебные программы по ИБ прошли углублённую оценку и соответствуют строгим требованиям, многие учебные заведения среднего звена заключили договоры с университетами об ускоренной подготовке выпускников по программам высшего образования.

ПЯТЬ СТОЛПОВ ОДНОЙ БЕЗОПАСНОСТИ

1 МАРТА 2023 ГОДА ПРЕЗИДЕНТ США ДЖОЗЕФ БАЙДЕН ПОДПИСАЛ «СТРАТЕГИЮ НАЦИОНАЛЬНОЙ КИБЕРБЕЗОПАСНОСТИ США»¹

В информационном бюллетене, открывающем документ, Администрация Байдена-Харрис объявляет о национальной стратегии кибербезопасности, направленной на обеспечение всех преимуществ безопасной цифровой экосистемы для всех американцев. «В это решающее десятилетие США переосмысливают киберпространство как инструмент для достижения целей таким образом, чтобы оно отражало наши ценности: экономическую безопасность и процветание; уважение прав человека и основных свобод; доверие к нашей демократии и демократическим институтам и справедливое, разнообразное общество. Чтобы реализовать это видение, мы должны внести фундаментальные изменения в то, как США распределяют роли, обязанности и ресурсы в киберпространстве», — говорится в обращении.

Стратегия требует двух фундаментальных изменений в обществе: изменения баланса ответственности и переориентации стимулов в пользу долгосрочных инвестиций.

¹ <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>

«Мы должны сбалансировать ответственность за защиту киберпространства, переложив бремя кибербезопасности с частных лиц, малого бизнеса, региональных и местных органов власти на организации, которые наиболее способны и находятся в наилучшем положении для снижения рисков для всех нас».
Джозеф Байден

Чтобы стимулировать эти сдвиги, Стратегия структурирована по пяти направлениям:

1. Защита критической инфраструктуры
2. Разрушение и ликвидация субъектов угрозы
3. Формирование рыночных сил для обеспечения безопасности и устойчивости
4. Инвестиции в устойчивое будущее
5. Налаживание международных партнёрских отношений для достижения общих целей

1. ЗАЩИТА КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

За последний год в США были внесены улучшения в защиту критической инфраструктуры с помощью стандартизации, но по-прежнему отсутствуют обязательные требования, что приводит к противоречивым результатам при реагировании на кибератаки. В Стратегии указывается, что должны быть введены жёсткие требования обеспечения кибербезопасности и устойчивости, заложенные в основы экономики и повседневной жизни.

В целях улучшения киберзащиты регуляторные ведомства должны

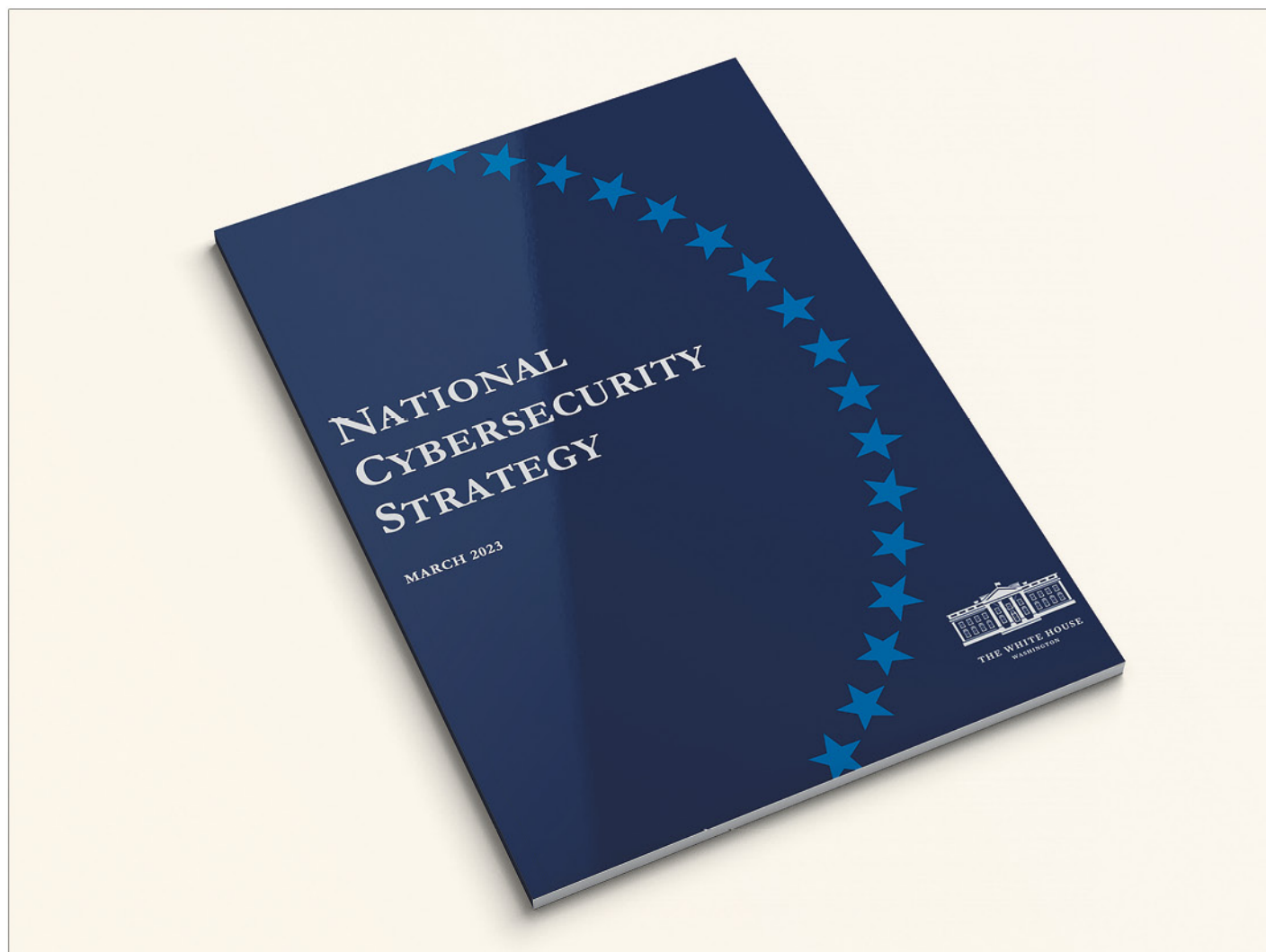
применять старые и вводить новые обязательные требования по ИБ для критически важных инфраструктурных организаций, а также привлекать к работе такие структуры, как Национальный институт стандартов и технологий (NIST) и другие.

В работу по кибербезопасности также входит укрепление сотрудничества между государственным и частным секторами, интеграция правительственных учреждений и ведомств в области ИБ, создание обновлённых федеральных планов реагирования на инциденты и модернизация национальной обороны.

Защита критически значимой инфраструктуры (КЗИ) от вражеских действий и других угроз требует модели киберзащиты, имитирующей распределённую структуру интернета. США реализует эту сетевую модель путём организационного сотрудничества и технологического взаимодействия, что позволит создать основанную на доверии «сеть сетей», которая будет способствовать повышению осведомлённости о ситуации и стимулировать коллективные синхронизированные действия по защите объектов КЗИ.

Агентство по кибербезопасности и защите инфраструктуры (CISA) является национальным координатором по вопросам безопасности и устойчивости КЗИ. CISA координирует работу с отраслевыми Агентствами по управлению рисками (SRMA), что позволяет федеральному центру расширить взаимодействия с операторами КЗИ по всей территории США.

Отраслевые SRMA ежедневно отвечают за кибербезопасность и киберустойчивость, обладают опытом по повышению ИБ. Каждое отраслевое агентство поддерживает операторов



КЗИ, отвечающих за свои системы и активы. Организации по обмену и анализу информации (ISAO), отраслевые центры по обмену и анализу информации (ISAC) и иные ведомства проводят операции по киберзащите в сложных секторах экономики.

Федеральное правительство продолжит координировать работу CISA и сети SRMA. Инвестиции федерального правительства в развитие возможностей отраслевых Агентств позволят повысить безопасность и устойчивость всей КЗИ США.

Федеральное правительство будет работать с различными ведомствами для выработки общего видения развития модели их взаимодействия, что потребует использования новых технологических решений для разнонаправленного обмена информацией в режиме реального времени и координации усилий по противодействию кибератакам.

В партнёрстве с частным сектором CISA и SRMA будут разрабатывать механизмы межмашинного обмена данными, развивать сотрудничество с поставщиками ПО, оборудования и услуг, способными изменить ландшафт в сторону повышения кибербезопасности и устойчивости.

2. РАЗРУШЕНИЕ И ЛИКВИДАЦИЯ СУБЪЕКТОВ УГРОЗЫ

Цель второго направления Стратегии — сделать злоумышленников неспособными проводить киберкампании, угрожающие национальной или общественной безопасности США. Соединённые Штаты будут использовать все имеющиеся возможности для пресечения и ликвидации субъектов угроз, чьи действия угрожают национальным интересам. Эти усилия включают дипломатические,

информационные, военные (как кинетические, так и кибернетические), финансовые, разведывательные и правоохранные возможности.

В Стратегии сформулирован план по разработке и обновлению стратегии безопасности Министерства обороны с целью прояснения действий ведомства при проведении операции по защите интересов США в киберпространстве против субъектов, представляющих угрозы на стратегическом уровне.

Национальная объединённая целевая группа по расследованию кибератак (NCIJTF) как межведомственный центр для координации кампаний правительства по пресечению деятельности хакерских группировок расширит свои возможности. Аналогичным образом Минобороны и разведывательное сообщество намерены задействовать весь спектр дополнительных полномочий для проведения

кампаний по пресечению деятельности киберпреступников.

Эффективное пресечение вредоносной кибердеятельности требует более тесного сотрудничества между частными структурами, обладающими уникальными знаниями и возможностями, и федеральными агентствами, имеющими средства и полномочия к действию. Рассматривается вопрос обмена разведывательными данными и уведомлениями между государственными и частными структурами для повышения скорости и масштабов реагирования для повышения эффективности борьбы с киберпреступностью и программ-вымогателями.

В рамках стратегии программы-вымогатели считаются угрозой национальной безопасности. Учитывая воздействие вымогателей на ключевые услуги КЗИ, США будут использовать все возможности государственной машины для противодействия этой угрозе по четырём направлениям:

- ♦ использование международного сотрудничества для разрушения экосистемы программ-вымогателей и изоляции тех стран, которые служат убежищем для преступников;
- ♦ расследование преступлений, связанных с программами-вымогателями, и использование правоохранительных органов для пресечения деятельности инфраструктуры и субъектов программ-вымогателей;
- ♦ повышение устойчивости КЗИ к атакам программ-вымогателей;
- ♦ борьба со злоупотреблением криптовалют для отмывания платежей за выкуп.

Поскольку программы-вымогатели являются проблемой без границ, требующей международного сотрудничества, Белый дом созвал Инициативу по борьбе с программами-вымогателями (CRI) с участием представителей более чем тридцати стран. CRI провела глобальные учения для повышения устойчивости и начиная с января 2023 г. запустила международную целевую группу по борьбе с вымогателями под руководством Австралии для обмена информацией о субъектах, осуществляющих атаки вымогателей, и инфраструктуре. Группа будет поддерживать и координировать усилия стран — членов CRI

по пресечению кибератак. Инициатива будет способствовать синхронизации политических и дипломатических усилий своих членов.

Новый подход будет включать борьбу с незаконными криптовалютными биржами, на которые опираются операторы программ-вымогателей, и внедрение международных стандартов борьбы с незаконным финансированием через криптоактивы. В США финансовые учреждения, предлагающие услуги в криптовалютах, подлежат контролю в области борьбы с отмыванием денег и финансированием терроризма. Отслеживание платежей и выкупов возложено на профильные разведывательные агентства и министерства.

3. ФОРМИРОВАНИЕ РЫНОЧНЫХ СИЛ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И УСТОЙЧИВОСТИ

Третье направление — перераспределение ответственности. Те, кто имеет наилучшие возможности для снижения рисков с целью создания современной цифровой экономики, способствуют безопасности и устойчивости, сохраняя при этом инновации и конкуренцию.

При создании программных продуктов и услуг многие поставщики «игнорируют передовые методы безопасной разработки, поставляют продукты с небезопасными конфигурациями по умолчанию или известными уязвимостями и интегрируют стороннее программное обеспечение неизвестного или непроверенного происхождения». Безопасность по принципам проектирования или предварительное тестирование должны быть выполнены для снижения риска, но часто производители программного обеспечения и интернета вещей (IoT) не заинтересованы в этом, поскольку могут отказаться от ответственности по контракту, используя своё положение на рынке.

Стратегия предлагает переложить ответственность на производителей ПО, чтобы предотвратить последствия эксплуатации небезопасного программного обеспечения для конечных пользователей. Ожидается, что будет создана структура для защиты ответственности компаний, которые

разрабатывают и поддерживают собственные продукты.

Администрация продолжит повышать кибербезопасность IoT посредством федеральных исследований и НИОКР, закупок и управления рисками, как это предусмотрено в Законе об улучшении кибербезопасности IoT от 2020 г. Кроме того, администрация продолжит развивать программы маркировки безопасности IoT в соответствии с указаниями Указа № 14028. Благодаря расширению маркировки безопасности IoT потребители смогут сравнивать средства киберзащиты IoT, что создаст рыночный стимул для повышения безопасности всей экосистемы интернета вещей.

Также планируется поощрение скоординированного раскрытия уязвимостей во всех технологиях, разработка процесса выявления и снижения рисков в широко используемом неподдерживаемом программном обеспечении, продолжении поиска улучшений в безопасности IoT и других стимулах безопасности.

Администрация рассмотрит возможности введения киберстрахования, чтобы в случае катастрофического киберинцидента федеральное правительство могло стабилизировать экономику и помочь её восстановлению. Для этого Администрация оценит необходимость и возможность федерального страхового ответа на киберпроисшествия, который будет поддерживать существующий рынок киберстрахования. При разработке этой оценки она будет работать со всеми регуляторами и заинтересованными сторонами отрасли.

4. ИНВЕСТИЦИИ В УСТОЙЧИВОЕ БУДУЩЕЕ

Четвёртое направление Стратегии представляет собой «устойчивое и процветающее цифровое будущее, построенное завтра, которое начинается с инвестиций, сделанных сегодня».

Технические основы цифровой экосистемы уязвимы по своей природе. Число уязвимостей растёт при модернизации системы, увеличивая риск. Планируется предпринять шаги по смягчению части проблем, таких как уязвимости протокола Border Gateway

Protocol, незашифрованные запросы к системе доменных имён и медленное внедрение IPv6. Такая «чистка» требует определения наиболее актуальных проблем и дальнейшего развития эффективных мер безопасности, тесного сотрудничества государственного и частного секторов для снижения риска без нарушения работы платформ и сервисов, построенных на этой инфраструктуре. Федеральное правительство будет играть ведущую роль, обеспечивая внедрение в своих сетях этих и других мер безопасности, сотрудничая со всеми сторонами в разработке и внедрении решений, которые повысят безопасность экосистемы интернета, и поддерживая исследования для понимания и устранения причин медленного внедрения.

Поддерживая неправительственные организации по разработке стандартов (SDO), США будут сотрудничать со всеми заинтересованными организациями для обеспечения безопасности новых технологий, операционной совместимости, содействия глобальной рыночной конкуренции, защиты национальной безопасности и экономических преимуществ.

В рамках обновления «Федерального стратегического плана исследований и разработок в области ИБ» федеральное правительство определит и расставит приоритеты, будет стимулировать НИОКР для активного предотвращения и снижения рисков ИБ в существующих и новых технологиях в таких областях, как искусственный интеллект, операционные технологии и промышленные системы управления, облачная инфраструктура, телекоммуникации, шифрование, прозрачность систем и аналитика данных, используемых в критической инфраструктуре. Эти усилия будут поддерживаться федеральными Агентствами и финансируемые федеральным правительством центрами исследований и разработок посредством партнёрства с научными кругами, производителями, технологическими компаниями, владельцами и операторами.

Надёжное шифрование является основой кибербезопасности и глобальной коммерции. Это основной способ защиты данных в интернете,

Федеральное правительство определит приоритетность перехода уязвимых общественных сетей и систем на квантово устойчивые криптографические среды и разработает дополнительные стратегии снижения рисков для обеспечения криптографической гибкости

аутентификации пользователей и подписей, подтверждения информации.

Квантовые вычисления способны разрушить некоторые из самых распространённых сегодня стандартов шифрования. Поэтому необходимо определить приоритеты и ускорить инвестиции в замену оборудования, ПО и услуг, которые могут быть легко взломаны квантовыми компьютерами, чтобы защитить информацию от будущих атак.

Федеральное правительство определит приоритетность перехода уязвимых общественных сетей и систем на квантово устойчивые криптографические среды и разработает дополнительные стратегии снижения рисков для обеспечения криптографической гибкости перед лицом будущих рисков. Частный сектор должен следовать модели правительства в подготовке своих сетей и систем к постквантовому будущему.

Национальный переход к экологически чистой энергии приводит к появлению нового поколения программно-аппаратных комплексов, которые способны повысить устойчивость, безопасность и эффективность электрических сетей США. Эти технологии, включая распределённые энергоресурсы, умные устройства для выработки и хранения энергии, современные облачные платформы управления электросетями, а также ЛЭП, предназначенные для управляемых нагрузок большой мощности, являются гораздо более сложными, автоматизированными и взаимосвязанными в цифровом формате, чем системы электросетей предыдущих поколений.

Поскольку США инвестируют в новую энергетическую инфраструктуру, Администрация воспользуется стратегической возможностью для

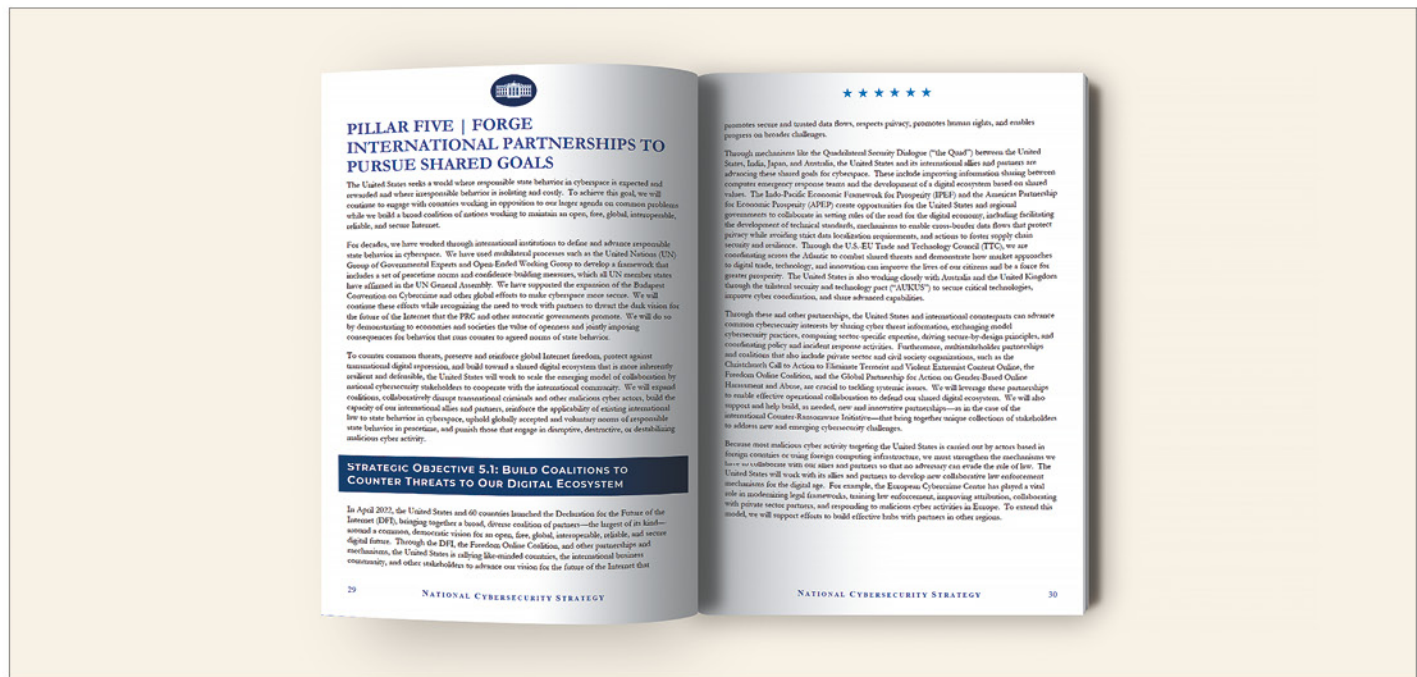
обеспечения кибербезопасности на упреждающей основе путём реализации Национальной киберинформированной инженерной стратегии, разработанной вместе с Конгрессом, и скоординирует работу заинтересованных сторон всех уровней власти по развёртыванию безопасной, совместимой сети зарядных устройств для электромобилей, инфраструктуры заправки с нулевым уровнем выбросов, транзитных и школьных автобусов с нулевым уровнем выбросов.

Министерство энергетики продолжит продвигать кибербезопасность для распределения электроэнергии и распределённых энергетических ресурсов в партнёрстве с промышленностью, государствами, федеральными регуляторами, конгрессом и другими агентствами.

Ещё одной целью Стратегии является поддержка развития экосистемы цифровой идентификации. Хотя цифровая идентификация может обеспечить более инновационную, безопасную и эффективную цифровую экономику, необходимы инвестиции в надёжные, поддающиеся проверке решения для цифровой идентификации для обеспечения безопасности, доступности и функциональной совместимости.

Отсутствие безопасных, сохраняющих частную жизнь и основанных на согласии решений в области цифровой идентификации позволяет процветать мошенничеству, сохраняет неравенство, а также трудности в финансовой деятельности и повседневной жизни.

От утечек персональных данных только в 2021 г. пострадали около 300 млн человек. Злоумышленники обманном путём получили миллиарды долларов из фондов помощи пострадавшим от пандемии COVID-19, предназначенных



для малого бизнеса и нуждающихся. Эта деятельность принесла колоссальные убытки предприятиям и нанесла ущерб государственным программам социальной помощи. Ни частный, ни государственный сектор, действуя разрозненно, не смогли решить эту проблему.

Федеральное правительство будет стимулировать инвестиции в надёжные решения для цифровой идентификации, которые будут способствовать безопасности, доступности и совместимости, финансовой и социальной интеграции, конфиденциальности потребителей и экономическому росту.

Усилия будут включать укрепление безопасности цифровых удостоверений; предоставление услуг по проверке атрибутов и удостоверений; проведение фундаментальных исследований; обновление стандартов, руководящих принципов и процессов управления для поддержки последовательного использования и операционной совместимости и разработку платформ цифровой идентификации.

Принимая во внимание экспериментальное внедрение мобильных водителевских удостоверений, авторы Стратегии призывают сосредоточиться на вопросах конфиденциальности, безопасности, гражданских свобод, справедливости, доступности и операционной совместимости.

При развитии этих возможностей политики и технологии цифровой идентификации будут защищать и укреплять неприкосновенность частной жизни, гражданские права и гражданские свободы с учётом непреднамеренных последствий, предвзятости и возможных злоупотреблений.

Отдельным пунктом направления выделена разработка национальной стратегии для укрепления кадровой политики в области ИБ с учётом сотен тысяч незаполненных вакансий в сфере кибербезопасности. Работодатели частного и государственного секторов сталкиваются с проблемами при наборе, найме и удержании специалистов по ИБ, что негативно сказывается на коллективной кибербезопасности.

Стратегия призывает использовать стратегические государственные инвестиции в инновации наряду с образованием для достижения экономически устойчивых результатов, которые служат национальным интересам. Этому помогут как существующие программы, так и работа с другими странами по оптимизации технологий кибербезопасности.

Одним из важных аспектов данного направления является план по усилению и диверсификации рабочей силы в области кибербезопасности. Директор Управления национальной кибербезопасности

возглавит, разработает и реализует Национальную стратегию кибербезопасности и образования, которая будет основываться на существующих усилиях, разработанных Национальной инициативой по обучению кибербезопасности (NICE) и другими заинтересованными ведомствами и организациями.

5. НАЛАЖИВАНИЕ МЕЖДУНАРОДНЫХ ПАРТНЁРСКИХ ОТНОШЕНИЙ ДЛЯ ДОСТИЖЕНИЯ ОБЩИХ ЦЕЛЕЙ

Работа по определению и продвижению ответственного поведения в киберпространстве велась международными организациями на протяжении десятилетий. Последняя часть Стратегии направлена на дальнейшее развитие путём создания коалиций для противодействия угрозам, расширение и укрепление партнёрских отношений, на повышение узнаваемости за счёт объединения государственного и частного секторов и поощрения сотрудничества с международными организациями, например National Cyber-Forensics и Training Alliance.

Для противодействия общим угрозам, сохранения и укрепления глобальной свободы интернета, защиты от транснациональных цифровых репрессий и создания общей цифровой экосистемы,

более устойчивой и защищённой по своей природе, США будут работать над расширением новой модели сотрудничества национальных субъектов кибербезопасности с международным сообществом.

В рамках партнёрств США и международных партнёры могут продвигать общие интересы кибербезопасности путём обмена информацией о киберугрозах, обмена типовыми практиками кибербезопасности, сравнения отраслевого опыта, внедрения принципов безопасного проектирования, а также координации политики и деятельности по реагированию на инциденты.

Существующие сложные глобальные взаимосвязанные цепочки поставок, производящие информационные, коммуникационные и операционные технологические продукты, движут экономикой США. Эта глобальная зависимость обеспечивает растущую сеть международных поставщиков. Для снижения рисков срыва поставок потребуется долгосрочное стратегическое сотрудничество между государственным и частным секторами как внутри страны, так и за рубежом для обеспечения баланса, устойчивости и безопасности.

Федеральное правительство будет уделять приоритетное внимание обобщению уроков, извлечённых из киберинцидентов, и применять эти уроки при реализации данной Стратегии, говорится в заключительных строках документа, реализация которого будет проводиться в течение 10 лет.

О ПОЛИТИЧЕСКОМ КОНТЕКСТЕ

Сам документ представляет ценность с точки зрения международного опыта, поэтому, представляя его, мы сконцентрировали внимание именно на этом. В то же время невозможно игнорировать и политический контекст. Сам документ предваряется обширным введением, часть которого мы приводим ниже. Делая это, мы настоятельно призываем читателей, как говорится, отделять мух от котлет, то есть серьёзную работу, проделанную для защиты цифровой экосистемы большой страны, от текущих политических взглядов некоторых лидеров этой страны. Эти взгляды, как нам известно, весьма сомнительны,

но они выражены в конкретных словах, с которыми также имеет смысл ознакомиться.

«Правительства Китая, России, Ирана, Северной Кореи и других авторитарных государств с ревизионистскими намерениями агрессивно используют передовые кибервозможности для достижения целей, которые противостоят интересам США и общепринятым международным нормам. Их безрасчётное пренебрежение верховенством закона и правами человека в киберпространстве угрожает национальной безопасности и экономическому процветанию США.

Китайская Народная Республика (КНР) в настоящее время представляет самую широкую, активную и наиболее устойчивую угрозу как для сетей правительства, так и для частного сектора и является единственной страной, имеющей намерение изменить международный порядок и, во всё большей степени, экономическую, дипломатическую, военную и технологическую мощь для этого. За последние десять лет она расширила масштабы киберопераций за пределы кражи интеллектуальной собственности и стала нашим самым передовым стратегическим конкурентом, способным угрожать интересам США и доминировать в новых технологиях, имеющих решающее значение для глобального развития. Успешно используя интернет как основу государственного наблюдения и влияния внутри страны, КНР экспортирует своё видение цифрового авторитаризма, стремясь сформировать глобальный интернет по своему образу и подобию, подвергая опасности права человека за пределами границ Китая.

Более 20 лет Россия остаётся постоянной киберугрозой, поскольку использует свои возможности для дестабилизации соседей и вмешательства во внутреннюю политику демократических стран по всему миру. Россия остаётся постоянной киберугрозой, поскольку совершенствует свои возможности для кибершпионажа, атак, влияния и дезинформации для давления на суверенные страны, укрывательства транснациональных преступных групп, ослабления альянсов и партнёрства США и подрыва международной

системы, основанной на правилах. Как и атака NotPetya в 2017 г., кибератаки России в поддержку вторжения в Украину в 2022 г. привели к безответственному вторичному воздействию на гражданскую критическую инфраструктуру других европейских стран.

Правительства Ирана и Корейской Народной Демократической Республики (КНДР) аналогичным образом растут в своей изощрённости и готовности осуществлять вредоносную деятельность в киберпространстве. Иран использовал кибернетические возможности, чтобы угрожать союзникам США на Ближнем Востоке и в других местах, в то время как Северная Корея проводит кибератаку для получения дохода через преступные предприятия, такие как кража криптовалют, программы-вымогатели и развёртывание тайных работников информационных технологий для подпитки своих ядерных амбиций, говорится в релизе. Дальнейшее развитие этих возможностей может оказать значительное влияние на интересы США, союзников и партнёров.

Кибероперации преступных синдикатов в настоящее время представляют угрозу национальной и общественной безопасности, экономическому процветанию США, их союзников и партнёров. Инциденты с программами-вымогателями привели к сбоям в работе важнейших служб и предприятий по всей стране и по всему миру, от энергетических трубопроводов и пищевых компаний до школ и больниц. Общие экономические потери от атак программ-вымогателей продолжают расти, достигая миллиардов долларов США ежегодно.

Преступные синдикаты часто работают в государствах, которые не сотрудничают с правоохранительными органами США, поощряют, укрывают или терпимо относятся к такой деятельности. Эти и другие вредоносные действия в киберпространстве продолжают угрожать американскому обществу, оказывая огромное воздействие на тех, у кого нет ресурсов для самозащиты, восстановления или обращения за помощью».

*Документ прочитала
Марина Бродская*

ОПЫТ СТРАНЫ ЦВЕТУЩЕГО ЛОТОСА



Амина ЗАМУЛИНА
руководитель
направления Центра
ДРО, Сбербанк

РЕГУЛИРОВАНИЕ СФЕРЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНДИИ

1 марта 2023 года вступил в силу Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее — Роскомнадзор) от 05.08.2022 № 128 «Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных» (далее — Перечень стран), в соответствии с которым Индия признаётся страной с адекватным уровнем защиты прав субъектов персональных данных (ПДн). Решение Роскомнадзора упрощает порядок трансграничной передачи персональных данных в Индию, что может иметь существенное значение для отечественных компаний, желающих установить/продлить деловые отношения с индийскими контрагентами.

В соответствии с новыми требованиями Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ (далее — Закон о ПДн), перед осуществлением трансграничной передачи ПДн каждый оператор¹ обязан уведомить Роскомнадзор о намерении передавать данные за рубеж. При этом, если страна признана обеспечивающей адекватный уровень защиты прав субъектов ПДн, как в случае с Индией,

российским операторам не требуется выжидать 10-дневный срок, отведённый Роскомнадзору для принятия решения о разрешении или запрете такой передачи, — трансграничная передача ПДн разрешается сразу после подачи уведомления в Роскомнадзор.

Тем не менее операторам будет необходимо соблюсти все прочие требования, установленные в ст. 12 Закона о ПДн, которые могут включать в себя необходимость провести оценку видов наказания за нарушение требований к обработке ПДн и размеров штрафных санкций, собрать информацию об уполномоченном органе по защите прав субъектов ПДн в стране получателя данных и др. Для этого необходимо иметь общее понимание о порядке обработки ПДн в стране, на территорию которой планируется трансграничная передача ПДн. Несмотря на включение в Перечень стран с адекватными мерами защиты ПДн, в Индии до сих пор отсутствует единый и всеобъемлющий закон, который был бы посвящён регулированию сферы персональных данных. Хотя попытки систематизировать регулирование в области ПДн наблюдаются ещё с 2019 года.

ОСНОВНЫЕ НОРМАТИВНЫЕ АКТЫ

На сегодняшний день основными нормативными документами, регулирующими вопросы сбора, хранения и обработки ПДн в Индии, являются:

- ♦ Закон об информационных технологиях, 2000 г.² (далее — Закон об ИТ);

- ♦ Поправки к Закону об информационных технологиях, 2008 г. (Пункты 43А и Секция 72А)³;

- ♦ Правила (разумно обоснованные практики и процедуры защиты чувствительных персональных данных или информации) информационных технологий от 11 апреля 2011 г., принятые Министерством связи и информационных технологий⁴ (далее — Правила ИТ);

- ♦ Уточнения к Правилам информационных технологий от 24 августа 2011 г., принятые Министерством связи и информационных технологий⁵.

Не являются документами в области персональных данных, однако имеют непосредственное отношение к организации обработки информации (в том числе ПДн) в банковской сфере:

- ♦ Основы кибербезопасности в Банках № RBI/2015–16/418 от 2 июня 2016 г., опубликованные Резервным банком Индии⁶;

- ♦ Хранение данных о платёжных системах, Директива Резервного банка

³ The Information Technology (Amendment) Act, 2008 (No.10 of 2009).

⁴ Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (Privacy Rules), No. G.S.R. 313(E) of 11 April 2011.

⁵ Clarification on Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 under section 43A of the Information Technology Act, 2000 (Press Note) of 24 August 2011.

⁶ Cyber security Framework in Banks, Directive № RBI/2015–16/418 of 2 June 2016 adopted by Reserve Bank of India (notification).

¹ Оператор — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

² The Information Technology Act, 2000 (No. 21 of 2000).



Индии № RBI/2017–18/153 от 6 апреля 2018 г.

Закон об ИТ можно назвать единственным «профильным» законом в сфере защиты персональной информации в Индии. Несмотря на это, данный закон не предусматривает детального регулирования вопросов сбора и обработки ПДн. По большому счёту, Закон об ИТ представляет собой нормативный акт, регулирующий вопросы электронной коммерции и киберпреступности, тем не менее он всё же содержит ряд положений об ответственности за нарушение конфиденциальности персональной информации. Закон об ИТ имеет экстерриториальное действие и применяется к любым правонарушениям, совершаемым за пределами Индии любыми лицами вне зависимости от гражданства, если эти правонарушения совершаются с использованием «компьютеров» или «компьютерных систем», расположенных на территории Индии⁷.

Дальнейшую реализацию Закона об ИТ обеспечивают принятые в 2011 году на законодательном уровне Правила

ИТ, которые более детально рассматривают вопросы сбора, хранения, обработки, передачи и защиты ПДн.

Понятие персональных данных: «Персональная информация» в вышеупомянутых Правилах ИТ определяется как любая информация, относящаяся к физическому лицу, которая прямо или косвенно, в сочетании с иной информацией, доступной или потенциально доступной оператору, может идентифицировать соответствующее физическое лицо⁸. К чувствительным данным относится информация о паролях, финансовой информации (например, информация о банковских счетах или картах), состоянии физического, физиологического или психологического здоровья, сексуальная ориентация, медицинские записи, история болезней, биометрические данные.

Политика конфиденциальности: операторы ПДн обязаны разработать и сделать доступной для субъектов ПДн, в том числе путём размещения на сайте оператора, политику конфиденциальности (policy for privacy and disclosure

of information), описывающую порядок обработки ПДн. Такая политика должна содержать:

- ♦ ясное и легкодоступное описание принятых оператором практик и политик в отношении обработки ПДн;
- ♦ виды обрабатываемых ПДн, включая чувствительные ПДн;
- ♦ цели обработки ПДн;
- ♦ информацию о раскрытии ПДн третьим лицам;
- ♦ описание мер защиты, реализуемых оператором для защиты обрабатываемых ПДн.

При сборе ПДн непосредственно от субъекта ПДн оператору необходимо предпринять разумные в конкретной ситуации и обстоятельствах шаги для того, чтобы обеспечить информирование субъектов ПДн о факте сбора ПДн, целях сбора ПДн, предполагаемых получателях ПДн, а также о лицах, осуществляющих сбор и дальнейшее хранение ПДн.

Правовые основания обработки ПДн: Правилами ИТ не предусматривается широкого перечня правовых оснований, как, например, в других юрисдикциях. Тем не менее при сборе или передаче чувствительных персональных данных оператор обязан получить письменное согласие субъекта на обработку ПДн. Передача ПДн, включая

⁷ Shilpa Thakur, «Privacy and Data Protection Regime in India: a Curtain Raiser!», 2022, Sber Privacy Journal // Кибрарий [Электронный ресурс]. URL: https://www.sberbank.ru/mon/img/uploaded/kibrary/dpo/sber_privacy_journal_2_2022.pdf

⁸ Shilpa Thakur, Privacy and Data Protection Regime in India: a Curtain Raiser!, 2022, Sber Privacy Journal // Кибрарий [Электронный ресурс]. URL: https://www.sberbank.ru/mon/img/uploaded/kibrary/dpo/sber_privacy_journal_2_2022.pdf

трансграничную, допускается при наличии согласия субъекта, а также в случаях, когда это необходимо для исполнения договора, стороной которого является субъект ПДн, или когда такое обязательство возлагается на оператора в силу закона.

Принципы обработки ПДн: при работе с чувствительными ПДн операторам следует руководствоваться сроками, необходимыми для достижения целей обработки. Хранение чувствительной информации дольше строго необходимого времени не допускается. Правила ИТ также предусматривают принцип ограничения целью — ПДн могут обрабатываться только для целей, для достижения которых они были первоначально собраны.

Права субъектов ПДн: субъекты ПДн имеют право на доступ к ранее предоставленной ими информации, а также на внесение уточнений и исправлений в неточную/некорректную информацию. Кроме того, субъектам ПДн предоставляется право на отзыв согласия на обработку ПДн.

Отличительной чертой текущего законодательства является отсутствие требования о назначении лица, ответственного за обработку и защиты ПДн (Data Protection Officer). Вместо этого операторам необходимо назначить **лицо, ответственное за рассмотрение жалоб субъектов ПДн** (Grievance Officer), а также опубликовать контактные данные такого лица на официальном сайте оператора.

Меры защиты ПДн: операторы обязаны разработать и внедрить программы и политики информационной безопасности, описывающие организационные, технические и физические меры защиты информации. Правила ИТ не детализируют, какие конкретно меры защиты обязаны внедрить операторы, чтобы исполнить требования о защите данных, но приводят в качестве примера подтверждения выполнения условий о защите ПДн соответствие признанным международным стандартам, например, *ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements*.

Трансграничная передача ПД: по общему правилу трансграничная

передача ПДн допускается с согласия субъекта ПДн. При этом, однако, отраслевыми регуляторами могут приниматься собственные правила передачи персональных данных, которым необходимо следовать в соответствующих отраслях. Так, в соответствии с Директивой Резервного банка Индии все платёжные данные должны храниться только на территории Индии⁹. Такие данные могут содержать данные клиента (имя, номер мобильного телефона, электронную почту, номер Aadhaar, номер PAN и т.д.); конфиденциальные платёжные данные (данные о клиенте и счёте получателя); платёжные реквизиты (ОТР, PIN, пароли и т.д.); и данные транзакции (системная информация об отправителе и получателе, ссылка на транзакцию, отметка времени, сумма и т.д.). В случае если обработка данных осуществляется за рубежом, обрабатываемая информация должна быть возвращена в Индию не позднее 24 часов с момента осуществления платежа¹⁰.

УПОЛНОМОЧЕННЫЙ ОРГАН

В отличие от России, в Индии отсутствует единый уполномоченный орган по защите персональных данных и прав субъектов ПДн. Тем не менее в Индии существуют несколько государственных органов, регулирующих вопросы персональных данных в пределах своих полномочий:

♦ **Министерство электроники и информационных технологий** (далее — MeitY) отвечает за администрирование Закона об ИТ, за издание дополнительных правил и разъяснений в соответствии с ним.

♦ **Индийский центр по реагированию на чрезвычайные ситуации в компьютерной сфере** (*the Indian Computer Emergency Response Team* (далее — Cert-In) — учреждённая MeitY организация, уполномоченная собирать, анализировать и распространять информацию об инцидентах,

связанных с кибербезопасностью. На операторов и обработчиков ПДн возлагается обязанность уведомлять Cert-In обо всех возникающих инцидентах кибербезопасности, например, о несанкционированном доступе к ИТ-системам или компрометации данных. В соответствии с директивой Cert-In об определённых типах киберинцидентов (таких как компрометация критически важных систем/информации, несанкционированный доступ к ИТ-системам/данным и т.д.) операторы данных обязаны сообщать в течение шести часов после их обнаружения¹¹. Cert-In уполномочен координировать действия по реагированию на такие инциденты. При этом в Индии отсутствуют требования по уведомлению субъектов ПДн о нарушении безопасности принадлежащих им данных.

♦ **Резервный банк Индии (Reserve Bank of India)** издаёт руководящие принципы по организации обработки данных в финансовых учреждениях, а также выступает контролирующим органом в пределах своих полномочий (например, в случае нарушения безопасности данных банковская организация обязана уведомить об инциденте Резервный банк).

ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ

Неисполнение обязанности по защите ПДн: в соответствии с Разделом 43А Закона об ИТ, в случае если оператор, обрабатывающий чувствительные ПДн или иную информацию о физическом лице, проявил халатность в отношении мер защиты ПДн, что привело к вреду для субъекта ПДн, такой оператор обязан возместить вред, причинённый физическому лицу путём выплаты соответствующей компенсации. При этом Закон об ИТ не предусматривает максимальный раздел такой компенсации.

Нарушение конфиденциальности и приватности: пункт 72 Закона об ИТ предусматривает ответственность за разглашение третьим лицам ПДн без согласия субъекта ПДн в виде лишения свободы на срок до 2 лет и/или

⁹ «Storage of Payment Data», Reserve Bank of India, DPSS.CO.OD.No 2785/06.08.005/2017-18 dated April 06, 2018.

¹⁰ «Storage of Payment Data», Frequently Asked Questions, Reserve Bank of India // URL: <https://www.rbi-ind.org/Scripts/FAQView3af3.html?Id=130>

¹¹ No. 20(3)/2022-CERT-In, Government of India Ministry of Electronics and Information Technology (MeitY), Indian Computer Emergency Response Team (CERT-In), 28 April, 2022.

штрафа в размере до 100 000 рупий ($\approx 92\,700$ р.).

Раскрытие информации в нарушение договора: пунктом 72А Закона об ИТ предусматривается ответственность лица — стороны договора за раскрытие ПДн физического лица — другой стороны договора без согласия такого лица, осуществлённое при этом умышленно, с намерением причинить убытки или с осознанием, что контрагенту могут быть причинены неправомерные убытки или неправомерная прибыль. Такое деяние наказывается лишением свободы на срок до 3 лет и/или штрафом в размере до 500 000 рупий ($\approx 464\,000$ р.).

Непредставление сведений об инцидентах информационной безопасности. В соответствии с пунктом 70В Закона об ИТ CERT-IN может запрашивать у операторов ПДн информацию о киберинцидентах, включая инциденты, затрагивающие ПДн. Непредставление данной информации наказывается лишением свободы на один год и/или штрафом в размере до 100 000 рупий ($\approx 92\,800$ р.).

ЗАКОНОПРОЕКТ О ЗАЩИТЕ ПДН (PERSONAL DATA PROTECTION BILL 2019)

Закон об ИТ был принят в 2000 году, на заре эры интернета, более детальные Правила ИТ также были приняты более 10 лет назад, когда общество ещё не вступило в эпоху цифровой трансформации, поэтому потребность обновления правового регулирования сферы ПДн в Индии более чем актуальна. В 2017 году Конституционный суд Индии признал право на приватность фундаментальным конституционным правом¹², что во многом послужило толчком к развитию сферы персональных данных в Индии. В 2018 году был предложен первый проект нового закона о персональных данных — Personal Data Protection Bill (далее — PDPB), после чего в 2019 году PDPB был направлен на рассмотрение Парламентского комитета.

Законопроект преимущественно был составлен по образцу регламента GDPR

и был направлен на защиту персональных данных физических лиц, а также на учреждение органа по надзору за соблюдением законодательства о защите персональных данных, который мог бы регулировать всю деятельность в сфере персональных данных на территории Индии¹³.

Однако PDPB не устоял перед давлением и критикой со стороны технологического сектора, в том числе в лице таких гигантов индустрии, как Facebook и Google, которые выступали против его принятия, в частности против положений о локализации данных на территории Индии и запрета на экспорт «критически важных» персональных данных за пределы Индии (данная мера была предложена авторами законопроекта в качестве меры, необходимой для обеспечения «цифрового суверенитета» Индии). В результате в августе 2022 года, спустя почти 4 года обсуждений, законопроект был снят с рассмотрения.

ЗАКОНОПРОЕКТ О ЗАЩИТЕ ЦИФРОВЫХ ПДН (DIGITAL PERSONAL DATA PROTECTION BILL 2022)

В 2022 году был внесён новый законопроект о защите ПДн. Ожидается, что он может быть принят уже в первой половине 2023 года. Следуя популярной мировой тенденции последних лет, Digital Personal Data Protection Bill (далее — DPDPB) предусматривает экстерриториальный характер действия. Тем не менее он не так похож на GDPR, как его предшественник, и имеет ряд особенностей.

♦ Область применения DPDPB сводится к обработке цифровых ПДн. За рамками остаётся вся обработка ПДн, осуществляемая без средств автоматизации.

♦ В отличие от предшественника, DPDPB не предусматривает требований к локализации баз ПДн на территории Индии. Вместо этого предполагается, что правительство Индии будет уведомлять иностранные государства,

на территорию которых трансграничная передача ПДн допускается.

♦ В отличие от иных зарубежных аналогов, DPDPB не разграничивает ПДн на категории в зависимости от чувствительности обрабатываемой информации, вместо этого индийский законопроект предусматривает понятие «существенный оператор» (англ. significant data fiduciary). Вместе с тем в самом законопроекте отсутствуют критерии, по которым операторы будут отнесены к «существенным», полномочия определять операторов в качестве «существенных» отведены правительству. В случае признания «существенными операторами» компании будут обязаны выполнить дополнительный ряд мер: назначить лицо, ответственное за защиту ПДн (DPO), проводить оценку DPIA (data protection impact assessment), а также назначить независимого аудитора, ответственного за проведение систематического контроля за соблюдением положений DPDPB.

♦ Отличительной чертой DPDPB также является специально предусмотренная ответственность субъектов ПДн. В отличие от законов, регулирующих обработку и защиту ПДн в России, Китае, странах ЕС и др., DPDPB предусматривает обязанности не только для операторов данных, но также и для самих субъектов, за нарушение которых субъект ПДн может быть привлечён к ответственности. Целью данных положений является недопущение злоупотребления правами со стороны субъектов ПДн. Так, субъектам ПДн запрещается подавать ложные и необоснованные жалобы, предоставлять ложные данные, скрывать существенную информацию, выдавать себя за другое лицо или представлять недостоверную информацию при реализации права на исправление или уничтожение ПДн. Нарушение субъектами ПДн данных требований влечёт за собой назначение штрафа в размере до 10 000 рупий ($\approx 9\,300$ р.).

♦ В отличие от PDPB, GDPR, PIPL и иных зарубежных законов о ПДн, законопроект не предусматривает «процентную вилку» штрафов. В соответствии с DPDPB, ответственность операторов за нарушение требований к обработке и защите ПДн не должна превышать 500 крор (≈ 5 млрд р.).

¹² Justice K. S. Puttaswamy (Retd.) v. Union of India [Writ Petition No. 494/ 2012].

¹³ Shilpa Thakur, «Privacy and Data Protection Regime in India: a Curtain Raiser!», 2022, Sber Privacy Journal // Кибарий [Электронный ресурс]. URL: https://www.sberbank.ru/mon/img/uploaded/kibariy/dpo/sber_privacy_journal_2_2022.pdf

ГОРИЗОНТ — 0-10+ ЛЕТ

ПРОГНОЗ ВЛИЯНИЯ ПЕРСПЕКТИВНЫХ ТЕХНОЛОГИЙ НА ЛАНДШАФТ УГРОЗ КИБЕРБЕЗОПАСНОСТИ

**Михаил
АНИСТРАТЕНКО**

Лаборатория
кибербезопасности
ПАО СберБанк

Илья БОЛОТОВ

Лаборатория
кибербезопасности
ПАО СберБанк

**Дмитрий
КУДИЯРОВ**

Лаборатория
кибербезопасности
ПАО СберБанк

**Александр
КУЗЬМИН**

Лаборатория
кибербезопасности
ПАО СберБанк

В прошлом номере BIS Journal мы начали публикацию аналитического отчёта «Прогноз влияния перспективных технологий на ландшафт угроз кибербезопасности» (Hypervector 2022), подготовленного в Лаборатории кибербезопасности Сбера. Эту работу трудно переоценить. Новые технологии влияют на все аспекты нашей жизни. В том числе используются для кибератак и, напротив, для защиты от них. В отчёте каждая такая технология проанализирована и оценена с точки зрения степени влияния на ландшафт киберугроз. Также указан период, в течение которого технология предположительно достигнет зрелости и начнёт применяться массово. Для каждой из рассмотренных технологий приведены примеры возможных угроз или её использования в кибербезопасности. В прошлом номере были рассмотрены технологии ближнего горизонта — 1–5 лет, в этом рассматривается горизонт 5–10 лет.

ТЕХНОЛОГИИ С ВЫСОКИМ УРОВНЕМ ВЛИЯНИЯ НА МАСШТАБ КИБЕРУГРОЗ

Социальный рейтинг (Social Rating). Уже сейчас в отдельных странах мы видим попытки внедрения интегрального цифрового рейтинга гражданина, на основании которого будет приниматься решение о доступе или отказе в услугах, определяться права и полномочия гражданина. Если этот тренд будет развиваться и дальше, то нам потребуются механизмы обеспечения безопасности и целостности этого рейтинга, так как манипуляция с рейтингом или данными, на базе которых он строится, будут приводить к ряду нежелательных последствий: ограничение доступа к отдельным функциям/инструментам/услугам добропорядочным гражданам или же необоснованное их получение злоумышленником.

Искусственный интеллект с сохранением приватности (Privacy-preserving AI). Комплекс технологий, обеспечивающий сохранение приватности данных, задействованных в жизненном цикле модели ИИ, а именно:

- ♦ приватность данных для обучения модели — из модели невозможно восстановить данные, использовавшиеся для её обучения;

- ♦ приватность данных на входе — пользовательские данные, подаваемые на вход модели, не раскрываются другим лицам, включая создателя модели.

Приватность данных на выходе — вывод модели недоступен для наблюдения никому, кроме пользователя, на чьих данных он рассчитан.

Приватность модели — модель не может быть украдена и использована злоумышленником.

Конкретные подходы, реализующие концепцию Privacy-preserving AI, ещё не финализированы, но активно исследуются научным сообществом.

Реализация искусственного интеллекта с сохранением приватности позволит расширить рынок услуг по обучению и предоставлению моделей ИИ, а также позволит компаниям совместно обучать и эксплуатировать эффективные модели ИИ без нарушения приватности используемых для этого данных и позволит уменьшить сопряжённые с этими данными риски кибербезопасности. Поэтому влияние на ландшафт угроз кибербезопасности оценивается как высокое.

Безопасные распределённые вычисления (Secure Multi-party Computation, SMPC).

Ряд криптографических подходов, позволяющих нескольким участникам произвести совместные вычисления, зависящие от тайных входных данных каждого из них, таким образом, чтобы ни один участник не смог получить никакой информации о чужих тайных входных данных. В том числе данный подход не раскрывает другим участникам промежуточные результаты вычислений, что обеспечивает большую безопасность по сравнению с технологией распределённого обучения моделей ИИ. SMPC может быть использован для коммерческого обмена данными без риска их раскрытия или нарушения их приватности. В том числе данный подход может быть использован для безопасного обмена данными кибербезопасности и антифрода с соответствующими службами других участников рынка или госорганами без раскрытия

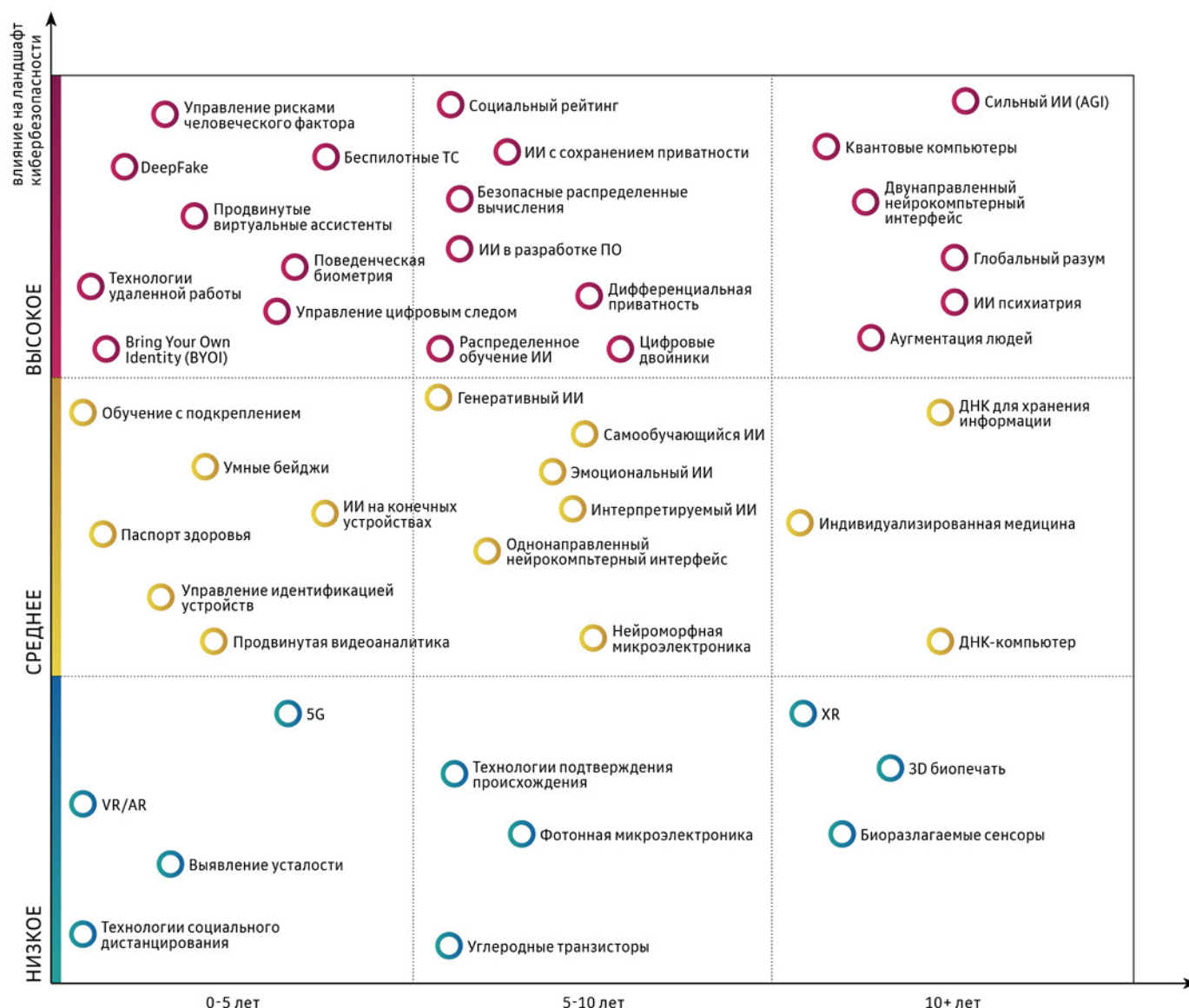


Рисунок 1. Hypervector — итоговый прогноз влияния технологий на ландшафт киберугроз. Ось X на графике — время в годах, разделённое на три промежутка: от 0 до 5 лет, от 5 до 10 лет и более 10 лет. Ось Y — влияние на ландшафт кибербезопасности, также разделённое на три промежутка: низкое, среднее и высокое.

персональных или конфиденциальных данных, например списки мошенников или индикаторы компрометации.

Искусственный интеллект в разработке ПО (AI-augmented Software Development). Уже сейчас исследуются возможности применения ИИ в разработке программных продуктов, и согласно прогнозам в недалёком будущем ИИ сможет существенно упростить эту задачу, помогая человеку разрабатывать ещё более сложные программные продукты, обеспечивать отсутствие программных ошибок и уязвимостей, оптимизировать эффективность ПО и ускорять процесс

разработки. С точки зрения безопасности это порождает ряд проблем.

Воздействие на этот ИИ может приводить к внедрению уязвимостей или незадекларированных возможностей в код (например, бэкдоры), нарушению функциональности ПО, краже исходного кода и обрабатываемых им данных.

Распределённое обучение моделей ИИ (Federated Learning). Технология машинного обучения, обеспечивающая децентрализованное обучение модели на множестве устройств, хранящих данные для обучения локально без обмена исходными данными между устройствами.

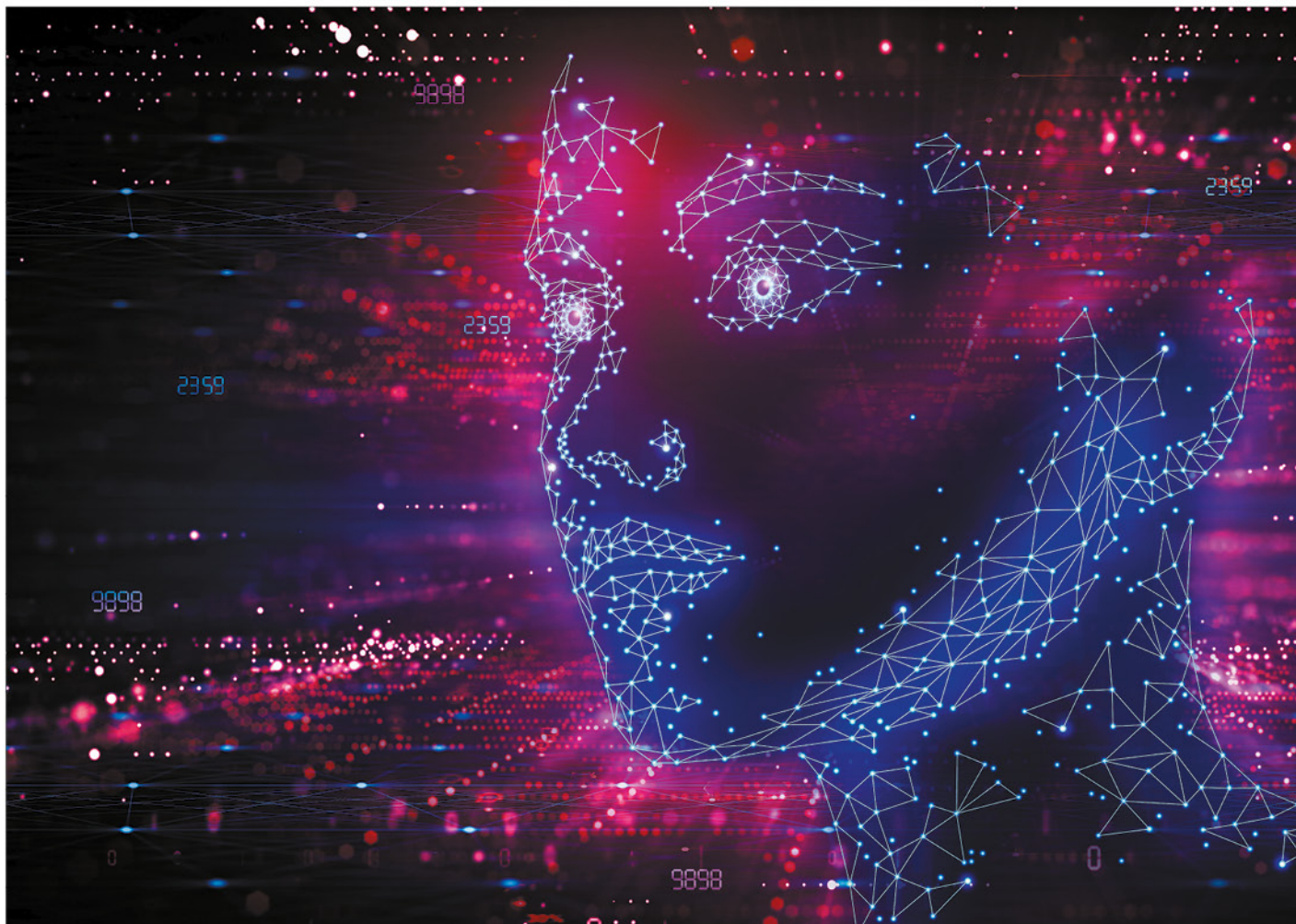
По сравнению с SMPC данный подход позволяет участвовать в процессе практически неограниченному количеству участников и, как правило, демонстрирует более высокую производительность, но при этом обладает меньшими гарантиями безопасности данных, так как другим устройствам могут быть доступны промежуточные результаты обучения, используя которые можно теоретически восстановить исходные данные. Данная технология применима для распределённого обучения единой модели с использованием данных, собираемых множеством конечных устройств. В интересах кибербезопасности распределённое обучение может быть применено в выявлении мошенничества, для повышения эффективности выявления мошеннических транзакций за счёт информации на устройствах пользователей без нарушения конфиденциальности.

Дифференциальная приватность (Differential Privacy). Технология, обеспечивающая максимально точные ответы на статистические и аналитические запросы к данным без возможности раскрытия содержания отдельных записей даже при выполнении большого количества запросов.

Дифференциальная приватность основана на введении случайности в данные, без существенного влияния на их статистические характеристики. На данный момент технология довольно нова и ограниченно известна за пределами исследовательского сообщества, но активно развивается в связи с растущим спросом на решения по сохранению приватности данных. При этом уже сегодня технологию начинают использовать некоторые технологические компании для анализа данных пользовательских устройств и приложений без нарушения приватности пользователей, например, Apple использует её для анализа некоторых данных с устройств на базе iOS. Использование данной технологии при коммерческом обмене аналитическими и статистическими данными между компаниями или между компаниями и конечными пользователями их продуктов позволит снизить риски раскрытия конфиденциальной информации или персональных данных.

Цифровые двойники (Digital Twins). Виртуальный аналог реального объекта, компьютерная модель, которая в своих ключевых характеристиках дублирует его и способна воспроизводить его состояния при разных условиях. Данная технология изначально возникла как часть четвёртой промышленной революции

для оцифровки физических объектов или процессов в производстве с целью помочь предприятиям быстрее обнаруживать физические проблемы, точнее предсказывать результаты и производить более качественные продукты. Дальнейшее развитие технологии цифровых двойников позволит оцифровывать более сложные объекты, в том числе живые организмы и другие сложные динамические системы. Например, для фармацевтической индустрии в сфере разработки лекарственных препаратов цифровой двойник может симулировать сложный комплекс физических и биохимических взаимодействий в организме человека для оценки действия новых лекарств. В сфере управления государством и охраны правопорядка цифровой город, населённый большим количеством цифровых двойников, поможет прогнозировать реакцию общества на те или иные решения и законы, массовые беспорядки или стихийные бедствия. Для человека персональный цифровой двойник с искусственным интеллектом может быть незаменимым ассистентом как в физическом мире, так и в метаверсе. С теми же эмоциями, поведением и паттерном действий и принятия решений, собранными на базе цифрового следа «оригинала», он может брать на себя выполнение части задач, так как с точки зрения цифровых взаимодействий с внешним миром такая реплика будет неотличима от оригинала. И хотя технологии для создания полноценного и полнофункционального цифрового двойника кажутся фантастикой, уже сейчас собирается огромное количество данных о цифровых взаимодействиях реальных людей, которые послужат «строительным материалом» для создания цифрового двойника, когда технологии позволят их использовать. С точки зрения безопасности основными угрозами для данной технологии может быть кража, злонамеренная модификация или вывод из строя цифровых двойников. Также цифровой двойник может обеспечивать псевдоудалённое присутствие пользователя на различных встречах и публичных мероприятиях, что порождает дополнительные проблемы с подтверждением аутентичности и права представительства цифрового двойника (прислан ли цифровой двойник самим владельцем оригинальной личности, уполномочен ли он владельцем на те слова и действия, которые он произносит или производит). Соответственно, с точки зрения безопасности потребуется ряд инструментов и технологии для контроля аутентичности, целостности и права представительства цифрового двойника.



ТЕХНОЛОГИИ СО СРЕДНИМ УРОВНЕМ ВЛИЯНИЯ НА ЛАНДШАФТ КИБЕРУГРОЗ

Генеративный искусственный интеллект (Generative AI). Технология, позволяющая генерировать новый цифровой контент на основании анализа существующих фото, видео, аудио, текстов или других типов данных. Генеративный ИИ может применяться в различных сферах — от развлечений, искусства и электронной коммерции до биологии, медицины и инженерного дела. Уже сейчас различные компании экспериментируют с применением этой технологии в своей деятельности, например, в фармацевтике для генерации новых химических соединений с заданными свойствами или в электронной коммерции для виртуальной примерки одежды или макияжа. В части влияния на ландшафт угроз кибербезопасности генеративный ИИ может быть использован для генерации синтетических данных, используемых для обучения других моделей искусственного интеллекта без риска нарушения приватности. Также данная технология уже находит применение у злоумышленников,

например, для генерации дипфейков или создания онлайн-профилей синтетических личностей для дальнейшего мошенничества.

Самообучение ИИ (Self-supervised Learning).

Технология машинного обучения на неразмеченных данных, где модель ИИ сама обнаруживает закономерности в структуре данных и обучается на них. В данный момент эта технология чаще всего применяется в задачах обработки естественного языка, где на большом объеме текста модель учится правильно предсказывать слова, идущие перед текущим словом или после него.

Также самообучение применимо для предсказания расположения объектов или их частей относительно друг друга при анализе изображений. Данный подход имеет большой потенциал применения, в том числе и в задачах кибербезопасности, так как не требует долгой и трудоемкой разметки больших датасетов, выполняемой людьми, в связи с чем самообучением ИИ активно исследуется ведущими технологическими компаниями, например Meta.

Эмоциональный искусственный интеллект (Affective Computing). Комплекс технологий, направленный на распознавание, интерпретацию, обработку и симуляцию человеческих эмоций на основании данных от различных устройств (сенсоров, камер, микрофонов и пр.). Развитие эмоционального ИИ позволит учитывать эмоции пользователя при его взаимодействии с различными устройствами, программами или сервисами и подстраивать результаты взаимодействий под его эмоциональный статус, как бы предугадывая его текущие желания и потребности и создавая у пользователя ощущение комфорта. В сфере безопасности данная технология может быть применена для оценки эмоционального состояния сотрудников с целью прогнозирования возникновения различных рисков, например инсайдерской угрозы. Стоит учитывать, что эмоциональный ИИ также может быть использован злоумышленниками при проведении атаки с использованием социальной инженерии для оценки эмоционального состояния жертвы и выбора наиболее эффективной стратегии развития атаки.

Интерпретируемый искусственный интеллект (Interpretable AI). Набор процессов и методов, позволяющих человеку понять, почему именно модель ИИ пришла к тем или иным результатам или выводам. По мере расширения возможностей ИИ людям становится всё сложнее осознать, каким образом модель пришла к тому или иному результату. Процесс вычисления превращается в так называемый чёрный ящик, который не поддаётся интерпретации. Модели, работающие по принципу чёрного ящика, создаются непосредственно на основе данных. При этом даже создавшие модель специалисты не в состоянии понять и объяснить, что именно в ней происходит и как модель пришла к конкретному результату. Возможность определить, как именно система на основе ИИ получила конкретный вывод, обладает множеством преимуществ. Объяснимость позволяет разработчикам убедиться в том, что система работает правильным образом, может потребоваться для обеспечения соответствия нормативным стандартам, а также может оказаться важной функцией, позволяющей заинтересованным лицам опротестовать или изменить полученный результат. В части кибербезопасности интерпретируемость моделей ИИ может позволить реализовать процесс их аттестации на отсутствие логических уязвимостей, несущих

потенциальную угрозу, а также повысить доверие к моделям, используемым непосредственно в целях кибербезопасности.

Однонаправленный нейрокомпьютерный интерфейс (One-way BCI). Система для обмена информацией между мозгом и электронным устройством (например, компьютером). В однонаправленных интерфейсах внешние устройства могут либо принимать сигналы от мозга, либо посылать ему сигналы, например, имитируя сетчатку глаза с помощью электронного импланта.

Простые неинвазивные нейроинтерфейсы уже сейчас могут применяться для передачи команд компьютерам и другим электронным устройствам. Технология нейроинтерфейсов также нашла своё применение в протезировании, позволяя восстанавливать нарушенные функции сенсорных органов, например слуха с помощью кохлеарного импланта или зрения с помощью импланта сетчатки. По мере развития технологии прогнозируется расширение использования нейроинтерфейсов не только для восстановления утраченных функций организма, но и для расширения их возможностей сверх доступных обычному человеку. А снижение инвазивности при имплантации и извлечении позволит устанавливать и заменять их без особых сложностей. Широкое распространение нейроинтерфейсов породит новые угрозы кибербезопасности, такие как взлом имплантов с целью слежки или перехвата контроля, похищения конфиденциальных данных, модификация передаваемой информации и прочие.

Нейроморфная микроэлектроника (Neuromorphic Hardware). Нейроморфные чипы имеют специализированную вычислительную архитектуру, имитирующую морфологию и структуру биологических нейронных сетей: выделенные вычислительные блоки эмулируют поведение нейронов непосредственно в аппаратном обеспечении, а сеть физических взаимосвязей между ними обеспечивает быстрый обмен информацией между ними. Эта концепция вдохновлена человеческим мозгом, где биологические нейроны и синапсы работают аналогичным образом. Специализированные нейроморфные устройства менее гибкие, чем универсальные центральные процессоры, но обеспечивают исключительную производительность и энергоэффективность при обучении и эксплуатации глубоких нейронных сетей. Обычные компьютеры реализованы на базе архитектуры фон Неймана, которая состоит из

вычислительных ядер, последовательно выполняющих инструкции и обрабатывающих данные, хранящиеся в централизованной памяти. Это означает, что вычислительная производительность таких систем ограничена скоростью передачи данных, которые могут быть переданы между вычислительным блоком и внешним блоком памяти. С появлением всё более требовательных приложений интерес к высокопроизводительным вычислениям сместился в сторону увеличения параллелизма в виде многоядерных архитектур. Однако возможность распараллеливания вычислений принципиально ограничена общим доступом к ресурсам памяти. Последние достижения в области глубокого обучения упираются в эти ограничения, поскольку высокопараллельная структура глубоких нейронных сетей требует распределённого доступа к памяти, которое сложно эффективно реализовать с помощью обычных вычислительных технологий. Нейроморфная микроэлектроника призвана решить эту проблему и помочь в дальнейшем развитии технологий искусственного интеллекта.

С точки зрения кибербезопасности, помимо угроз со стороны возросшей производительности технологии нейронных сетей, новая микропроцессорная архитектура потребует анализа возможных уязвимостей на уровне процессора и, возможно, выработки ряда новых методов защиты и противодействия подобным угрозам.

ТЕХНОЛОГИИ С НИЗКИМ УРОВНЕМ ВЛИЯНИЯ НА ЛАНДШАФТ КИБЕРУГРОЗ

Фотонная микроэлектроника (Photonic Computing). Принципиально другой способ проведения вычислений с применением фотонов, а не электронов. Данный метод позволяет на несколько порядков повысить скорость вычислений с одновременным снижением энергопотребления. В теории на базе фотоники можно создавать как классические, так и квантовые компьютеры, и классический фотонный компьютер может быть логичным переходным этапом между классическим и настоящим квантовым компьютером. Недавно стартап Lightelligence продемонстрировал рабочий прототип фотонного процессора, и тесты в решении сложных математических задач показали превосходство в скорости фотонного процессора по сравнению с современным высокопроизводительным GPU в более чем 350 раз.

Классический фотонный процессор обладает такой же архитектурой, как и существующий

сейчас кремниевый, и, соответственно, к нему будет применима большая часть существующих атак. Но использование принципиально другого физического принципа для вычислений и передачи данных открывает возможность для новых атак на физическом уровне и атак по сторонним каналам с эксплуатацией физических свойств фотонов. Помимо этого, распространение фотонных компьютеров может вывести на новый уровень угрозы от применения ИИ злоумышленниками (дипфейки, атаки на ИИ или с помощью ИИ и прочее) и другие угрозы, требующие от злоумышленника больших вычислительных мощностей.

Углеродные транзисторы (Carbon-Based Transistors). Транзисторы, использующие углеродные нанотрубки в качестве материала канала вместо кремния. Поиск новых материалов для замены кремния связан с тем, что текущие полупроводники уже исчерпали себя с точки зрения дальнейшего снижения норм технологического процесса, и нанотрубки из углерода на данный момент являются наиболее многообещающей заменой.

Помимо возможности дальнейшего уменьшения размера транзистора, данный материал имеет ряд дополнительных преимуществ по сравнению с кремнием, таких как лучшее пороговое напряжение, более высокая плотность тока, подвижность электронов, транскондуктивность и лучший контроль над формированием канала. Данная технология не оказывает особого влияния на ландшафт угроз кибербезопасности.

Технологии подтверждения происхождения (Authenticated Provenance). Технологии, позволяющие на самом раннем этапе в цикле производства продукта удостоверить его аутентичность и затем дающие возможность подтвердить аутентичность по требованию на любом этапе дальнейшего цикла жизни продукта (конкретная реализация зависит от самого продукта, но зачастую подразумевает использование ИИ и блокчейн для этого). Проблема, которую решает подтверждение происхождения, — большое количество фейков и подделок, как материальных, так и нет: (не)органические продукты, (поддельные) дизайнерские вещи, фейковые новости, дипфейки и так далее. Ручные или полуручные инструменты проверки аутентичности плохо масштабируются и не успевают за быстрорастущим объёмом продуктов и контента.

(Окончание в следующем номере)



Борис СТОЛПАКОВ
историк криптографии,
кандидат физико-
математических наук

ПЕРВЫЕ ГРОМКИЕ ПУБЛИКАЦИИ ПО КРИПТОГРАФИИ

ИСТОРИЯ УДАЧНОГО КНИЖНОГО ПРОЕКТА

Начало 1960-х годов стало временем, когда криптография впервые привлекла к себе внимание мировых средств массовой информации. Тогда произошли несколько громких событий, выделившихся даже на ярком политическом фоне тех дней.

**РЕВОЛЮЦИЯ НА КУБЕ,
ПРИЗЕМЛЕНИЕ Ф. ПАУЭРСА,
ВИЗИТЫ Н. С. ХРУЩЁВА
В США...**

Напомним, каким был этот фон.

1959 г. — революция на Кубе под руководством Ф. Кастро; двухнедельный визит в США большой делегации

СССР во главе с Н.С. Хрущёвым; в Анкаре подписаны военные соглашения США с Турцией, Ираном и Пакистаном, предусматривавшие право использования их территорий американскими войсками; советские автоматические станции впервые в мире достигли поверхности другого небесного тела — Луны и передали на Землю фотографию её обратной стороны.

1960 г. — вооружённые силы СССР сокращены на 1 200 000 человек; 1 мая на Урале сбит американский самолёт-разведчик с пилотом Ф. Пауэрсом, обломки самолёта и специальной аппаратуры широко демонстрировались в Москве (илл. 1); Н.С. Хрущёв вновь посетил США, где выступил на Генеральной Ассамблее ООН и, понимая востребованность шоу в американском менталитете, стучал ботинком по столу в зале заседаний во время выступления британского премьер-министра Макмиллана.

**ПРЕСС-КОНФЕРЕНЦИЯ
АМЕРИКАНСКИХ
КРИПТОГРФОВ
В МОСКВЕ**

Вот на таком политическом фоне 6 сентября 1960 г. в Москве состоялась пресс-конференция двух сотрудников американского Агентства



Иллюстрация 1. У входа на выставку в парке им. Горького



Иллюстрация 2. В. Мартин и Б. Митчелл на пресс-конференции в Москве

национальной безопасности (АНБ) Уильяма Мартина и Бернона Митчелла. Два тридцатилетних криптографа предстали перед изумлённой прессой в Доме журналистов и заявили, что попросили убежище и советское гражданство (илл. 2).

В ходе конференции перебежчики впервые поведали миру о деятельности мало кому известного тогда АНБ, организованного в 1952 г. и быстро ставшего ключевой структурой, осуществляющей радиоэлектронную разведку по всему миру и в то же время обеспечивающей надёжность американских шифров.

ТРЕВОГА В АНБ

Тревога в Форт-Миде, штаб-квартире АНБ, была поднята ещё летом, когда перебежчики не вернулись из отпуска. Тогда же при обыске дома Митчелла сотрудники службы безопасности АНБ нашли ключ к его банковскому сейфу, специально оставленный на видном месте. Открыв сейф, сотрудники АНБ обнаружили там письмо. Его содержание не оставляло сомнений относительно намерений перебежчиков и их взглядов.

«МЫ ХОТИМ ДАТЬ ЭТИ ОБЪЯСНЕНИЯ...»

«22 июня 1960 года. Мы хотим объяснить нашим родным, друзьям и другим лицам, которые могут этим интересоваться, мотивы, побудившие нас просить гражданства Советского Союза.

С начала работы в Агентстве национальной безопасности, с лета 1957 года, мы убедились в том, что правительство Соединённых Штатов сознательно делает ложные и вводящие в заблуждение заявления, как для оправдания своей собственной политики, так и для осуждения действий других государств... Нам также стало известно, что правительство США тайно использует деньги и оружие для попыток свержения правительств, если оно полагает, что эти правительства недружественны Соединённым Штатам... Наконец, нам стало известно, что правительство США давало деньги шифровальщику, работающему в посольстве одной из стран-союзников в Вашингтоне, за информацию, которая помогла расшифровать зашифрованные телеграммы этого союзника. Такие действия убеждают нас в том, что правительство Соединённых Штатов неразборчиво в

средствах, хотя оно обвиняет в этом правительство Советского Союза...

Кроме разочарования и озабоченности, которые мы выразили по поводу некоторых действий США, имелись другие сильные мотивы для принятия нами решения о приезде в СССР.

Мы считаем, что в социальном отношении мы будем чувствовать себя там лучше и сможем лучше работать в соответствии со своей профессией. Другим мотивом является то, что в Советском Союзе таланты женщин используются и гораздо больше поощряются, чем в Соединённых Штатах. Мы считаем, что это обогащает советское общество и усиливает роль советских женщин...

Недостаток капиталистической системы заключается в том, что её наука и техника являются причиной ненужных человеческих страданий, так как содействуют безработице.

Не следует удивляться тому, что в Америке много людей относятся отрицательно к интеллектуальной и творческой деятельности. Мы надеемся стать научными работниками в Советском Союзе... Мы хотим дать

эти объяснения таким путём, чтобы потом это не могло быть расценено как пропагандистское заявление, инспирированное правительством страны, в которой мы просим разрешения проживать».

О МАРТИНЕ И МИТЧЕЛЛЕ

Копию этого письма Митчелл зачитал на пресс-конференции. Вслед за ним Мартин, хорошо владевший русским языком, огласил заявление. Частично повторив содержание письма, он упомянул и о том, что АНБ перехватывает и расшифровывает корреспонденцию союзников США, в том числе Италии, Франции, Турции, Уругвая.

Ныне известно, как сложилась дальнейшая жизнь этих перебежчиков.

Мартин (1931–1987) и Митчелл (1929–2001) были устроены на работу в ленинградский филиал Математического института АН СССР, где занялись статистикой и программированием. Оба вскоре женились, Мартин сменил фамилию на Соколовский, но прочный брак сложился лишь у Митчелла. Его жена Г.В. Яковлева преподавала на отделении фортепиано в Ленинградской консерватории. Сам Митчелл много лет трудился программистом в ЛЭИС им. Бонч-Бруевича, он похоронен в Петербурге. Мартин с 1979 г. пытался вернуться в США и неизменно получал отказ американских властей. В 1980-е годы он выехал в Мексику, где и умер в 1987 г.

СЕНСАЦИЮ НЕ УПУСТИЛИ

А тогда, в начале 1960-х, средства массовой информации впервые стали активно писать о криптографии, радио перехвате и дешифровании сообщений, а также о неведомом миру АНБ. Газета «Правда» посвятила громкому событию обширную передовицу, американская пресса тоже не упустила сенсацию. Своё мнение высказали и первые лица США и СССР. Комиссия конгресса США по расследованию антиамериканской деятельности вскоре начала дошное исследование обеспечения секретности в АНБ. В секретном докладе конгрессу бегство Митчелла и Мартина оценивалось как нанесение тяжелейшего ущерба национальной безопасности

за всю историю США. По результатам расследования 26 человек уволили из АНБ, в том числе заместителя директора по кадрам. Он лишился должности, помимо прочего, и за подделку своих личных документов.

ЗАДАЧА — УКРЕПИТЬ АВТОРИТЕТ АНБ

В такой обстановке правительство и депутаты конгресса почувствовали необходимость укрепления авторитета АНБ. Тогда в 1961 г. и появился замысел популярной публикации о достижениях американской дешифровальной службы в годы Второй мировой войны, прежде всего, конечно, против японского противника.

БОЙКИЙ ЖУРНАЛИСТ НАЙДЕН

Выбрать бойкого журналиста оказалось несложно — тема была привлекательна. Контракт на написание книги о криптографии издатели подписали с молодым редактором газеты International Herald Tribune в Париже Дэвидом Каном. Ещё в 1960 г., работая репортёром в небольшой местной газете в США, он написал статью для «Нью-Йорк Таймс» о перебежчиках из АНБ.

ДВОЙНОЙ УДАР

Актуальность будущей книги с течением времени всё росла. Достаточно напомнить, что 1962 г. стал временем опаснейшего Карибского кризиса в отношениях СССР и США. А в 1963 г. последовал двойной удар по престижу АНБ. Сначала в Москве объявился новый перебежчик-криптограф Виктор Гамильтон, американец сирийского происхождения. И не один, а вместе со своей американской женой-филологом. Супруги попросили предоставить им советское гражданство. В АНБ Гамильтон служил в отделе, занимавшемся дешифрованием сообщений из Греции и Турции, с Ближнего и Среднего Востока и Северной Африки. В своём заявлении, опубликованном 23 июля 1963 г. в газете «Известия» (илл. 3), Гамильтон отметил: «Американские власти пользуются тем, что штаб-квартира ООН находится на территории США. Зашифрованные инструкции Греции, Иордании, Ливана,

Египта и Турции своим представителям в ООН попадают в руки госдепартамента ещё до того, как доходят до своих истинных адресатов...»

Оказалось, что это только начало нового конфуза АНБ. Одновременно с бегством Гамильтона покончил с собой сержант Джек Данлап из службы охраны штаб-квартиры агентства в Форт-Миде, бывший ранее шофёром заместителя директора-начальника секретариата штаба АНБ. Вскоре после похорон сержанта с почестями на Арлингтонском мемориальном кладбище его вдова принесла в службу охраны пачку секретных документов, обнаруженных в домашнем тайнике.

ПРЕДПРИИМЧИВЫЙ СЕРЖАНТ

Следствие вскоре выяснило масштаб понесённого ущерба. Пользуясь возможностью бесконтрольного въезда и выезда с территории штаб-квартиры АНБ, а также беспрепятственного доступа в режимные отделы как курьера с особо важными материалами, общительный сержант наладил добычу и продажу ценных документов. Под умелым руководством советского разведчика-оператора он постепенно заручился содействием части персонала, заинтересованной в растаскивании по домам служебной техники и мебели. Этот случай откровенной торговли государственными секретами ныне хорошо известен. Интересно, что Данлап предложил свои услуги советской разведке за денежное вознаграждение именно во время проверки АНБ после бегства Мартина и Митчелла. Имея годовую зарплату около 5000 долларов, он, не скрываясь, потратил за три года 60 тысяч на шикарные яхту и автомобили, дорогие развлечения. По оценке официальных лиц Пентагона, ущерб, нанесённый Данлапом АНБ, в десятки раз превысил потери от перебежков-криптографов. Эти удары по престижу государства требовали скорейшего пропагандистского ответа.

ПОТРЕБОВАЛАСЬ СЕРЬЁЗНАЯ ПОДДЕРЖКА

Постепенно проект разрастался и требовал всё больших усилий. Решено

Я ВЫБРАЛ СВОБОДУ

ПОЧЕМУ ВИКТОР НОРРИС ГАМИЛЬТОН ПОКИНУЛ США и РЕШИЛ ЖИТЬ в СССР

ПРОШУ ВАС предоставить мне возможность обратиться через вашу газету к своим друзьям и знакомым в США и в странах Арабского Востока с тем, чтобы объяснить им причины, побудившие меня, после того, как я с таким трудом добился американского гражданства, порвать с Соединенными Штатами Америки и просить политического убежища в СССР.

Меня зовут Виктор Норрис Гамильтон. Мне 44 года. В 1940 году я окончил американский университет в Бейруте, во время войны служил в Арабском легионе, а затем перебивался случайным заработком. Работая в вечернем колледже в Бенгази, я встретил американку Лилли Белл Драйк. Когда через год мы поженились, она позвала меня в США. Должен сказать, я ехал в Америку, как в землю обетованную: мы верили, что Америка — страна больших возможностей для каждого, кто способен и может много работать. И сожаления, я и не подозревал, какие испытания готовила мне жизнь.

Начать с того, что, несмотря на диплом, я не мог получить место преподавателя в школе — у меня не было американского гражданства. Кроме того, в штате Джорджия, где мы поселились, на меня араба, смотрели, как на человека второго сорта — ведь кожа у меня смуглая. Несколько лет я работал швейцаром и коридорным в отелях.

Брак с Лилли давал мне некоторые преимущества в приобретении

и потом понял, военное и политическое значение.

Лекция прошла хорошо, по окончании ее Масквелл устроил небольшой прием. Среди гостей там оказался адмирал, фамилия которого я не знаю и по сей день. Он предложил мне свое содействие в поступлении на государственную службу.

По его рекомендации меня подвергли тщательной проверке и направили в специальную школу с иодовым названием «Темпо-Никс». В школе изучали основы разведывательного дела, криптографии и методы раскрытия шифров. Все предыдущее оказалось подготовкой к работе в американской разведке.

В июне 1957 года, после успешной сдачи экзаменов, меня вместе с другими выпускниками направили на работу в Национальное агентство безопасности (НАБ) в Административном центре НАБ в Мериленде. Я был зачислен экспертом в Ближневосточный сектор отдела, носившего название «Алло», что значит «Все другие страны». Сектор «занимается» ОАР, Сирией, Ираком, Ливаном, Йорданией, Саудовской Аравией, Йеменом, Ливией, Марокко, Тунисом, Турцией, Ираном, Грецией и Эфиопией. В задачи сотрудников «Алло» входит изучение и раскрытие шифрованной военной связи этих стран, а также расшифровка этих корреспонденций, поступающей в дипломатические представительства этих стран в любой точке земного шара.

США придает особое значение перехвату радиотелефонных переговоров, телеграфной и почтовой переписки дипломатических представителей ближневосточных стран, аккредитованных в Вашингтоне. Национальное агентство безопасности читает шифры всех этих стран, что является прямым результатом криптоанализа. Вместе с тем НАБ получает и оригиналы их национальных шифров из каких-то секретных источников. Это означает, что кто-то ворует для американцев шифры ближневосточных стран. Я собственными глазами видел в НАБ фотокопии шифров, например, сирийского генерального штаба, а также инструкцию с грифом «секретно» о пользования этими шифрами.

Мне дополнительно известно, что государственный департамент и министерство обороны систематически читали, анализировали и использовали в своих интересах шифрованную переписку посольств Объединенной Арабской Республики в европейских странах с правительством ОАР в Каире.

Я, например, имел на своем столе всю дешифрованную переписку Каира с посольством ОАР в Москве по вопросам, связанным с пребыванием в СССР в 1958 году правительственной делегации ОАР по поводу закупки нефти в Советском Союзе. Всю эту переписку НАБ передавал в государственный департамент, как передает постоянно дешифруемые инструкции министерства иностранных дел ОАР

или не хочу, но помогаю созданию серьезной опасности для района, с которым я связан и по рождению, и многими годами жизни, и друзьями, и родными.

Руководители НАБ внимательно следят за настроениями своих работников. В НАБ царит атмосфера мрачной подозрительности, недоверия к людям, работающим в форте Мид. Во всех отделах негласная слежка, бесконечные проверки и перепроверки всех действий и, по возможности, мнений работников. Никто никому не доверит, руководство поощряет доносы друг на друга. Каждое высказанное суждение, случайное замечание доходит до специальных работников, занимающихся обеспечением внутренней безопасности НАБ. С этой политической системой, с ее цепкой всеохватывающей паутиной столкнулся и я в конце своего пребывания в НАБ. Сильное подозрение органов внутреннего контроля НАБ вызвала моя просьба разрешить восстановить отношения с родственниками в Сирии. Я хотел послать им письмо. Этого было достаточно, чтобы меня начали считать ненадежным. Видимо, американцы не могли забыть, что я араб, т. е. с их точки зрения «несмысленный». Их неприязнь, часто переходившая в прямую враждебность, обострилась тем, что за короткий срок я получил повышение по службе, обйдя некоторых своих коллег. Мое положение становилось все более тяжким, и мне пришлось уйти из национального агентства безопасности.

Однако разрыв с разведкой не

НАШ СПРАВОЧНИК ОТ Д

СЛУША

РАДИО 24
Первая программа перт по злым (с истического труд Фрагменты из пюу 13.19 — Выступлен еспии алески горк — Н. Г. Чернышев копозиция. 16.10 мольском лагере тр 17.00 — «Потчи Ри бссед». «Олеми з У микрофона амес ния управления от ки и электрификации СССР Н. Н. Озеров. ный концерт. 19.00 мне в жизни». Р 20.00 — Декада по нального искусства. лена». Музыкальный — «Над сном олус Музыкальная передача Вторая программа нсчем на попрос епей». 10.00 — Зе шерт. 10.45 — «В Передача «Робот у А. Колосов — «Песни юнна. 13.00 — Вы ечеником Безруков ейной консертот «Счастые Алы Си: А. Шипкова. 13.55 — ретты Б. Теренти счастия». 16.30 — зыка и поэме Пуш рафский фронт». I ням наше знамя дидата историческе Михайлов. 17.40 радиостанция. Юно Школа передового сного хозяйства» овец оебуретским — В кафе «Молод перт неспит. 22.30 сказы советских пи

СМОТРИТЕ

ТЕЛЕВИДЕНИЕ

Иллюстрация 3. Фрагмент газетной публикации, фото с сайта kommersant.ru

было поместить в книге исторические материалы, связанные с мировой криптографией, начиная с древнейших времён, чуть ли не от Адама. Что вполне естественно, так как тайнопись — это разновидность письменности, а со словом и его записью или звуковым воспроизведением связано всё развитие человечества. В результате Кан уволился из газеты и занялся исключительно книгой. Надо сказать, что руководство АНБ было не в восторге от развивавшегося книжного проекта и пыталось ему помешать. Но покровители проекта оказались сильнее. Да и без серьёзной поддержки газетчику трудно было освоить новый для него массив информации. Учитывая слабую компетенцию Кана в чисто профессиональных вопросах, американские криптографы помогали ему в переводах с немецкого, в изложении рассекреченной информации, в правках текста. Наконец, в начале 1966 г. объёмистая рукопись книги была представлена издателям. Разумеется, издатели передали рукопись компетентным правительственным органам для проверки. Понятно, что проверка была

тщательной. В окончательном виде рукопись «похудела» в объёме, так как пришлось удалить часть материалов, в том числе раздел, повествовавший о взаимоотношениях АНБ с британским Центром правительственной связи. Отметим, что в книгу не вошла и большая часть истории взлома немецкой шифрмашин «Энигма», ведь соответствующие материалы рассекретили лишь в 1970-х годах.

ПУТЬ К ЧИТАТЕЛЯМ ОТКРЫТ

Долгожданная книга «Взломщики кодов» (The Codebreakers) вышла в свет в 1967 г. (илл. 4).

В ней впервые подробно и доступно был изложен обширный исторический материал, связанный с криптографией. Разумеется, прежде всего с точки зрения интересов США. Ныне эта книга хорошо известна читателям во многих странах, в том числе в России. Немало читателей связывали и связывают своё знакомство с криптографией именно с «Взломщиками кодов», хотя с той поры появилось значительное число популярных публикаций о засекречивании связи и информационной

безопасности. Вероятно, неслучайно совпадение по времени публикаций книги Кана в США и серии популярных статей «Тайны тайнописи» (в 1966–1970 годах) в издававшемся миллионными (!) тиражами советском журнале «Наука и жизнь».

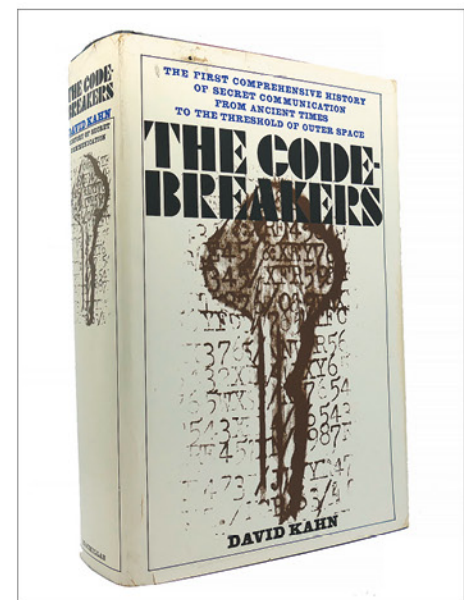


Иллюстрация 4. Обложка первого издания книги

«СВЕТ МОЙ, БРАТЕЦ ВАСЕНКА...»

О ЧЁМ ЖЕ ПИШУТ ЦАРЕВНЫ?

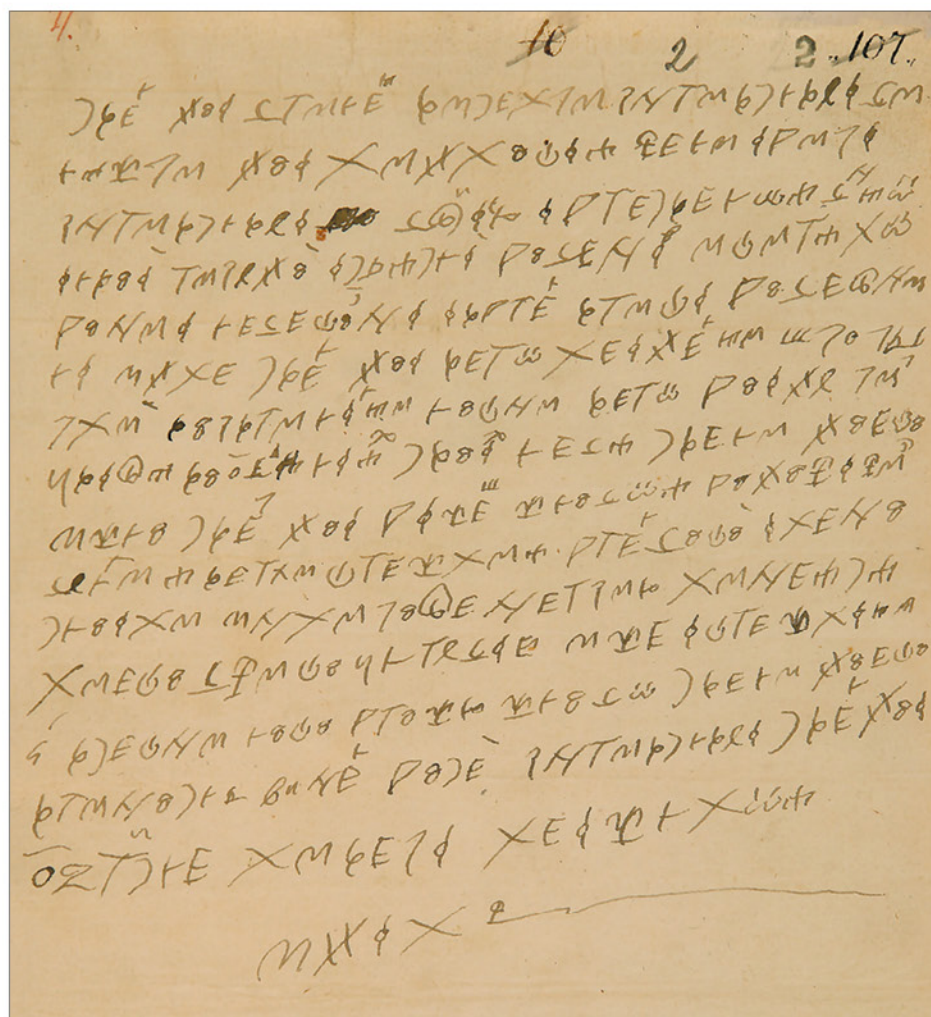


Иллюстрация 1. Письмо царевны Софьи Алексеевны князю Василию Голицыну

Пришла пора дать расшифровку письма правительницы России царевны Софьи Алексеевны князю Василию Васильевичу Голицыну, приведённого в № 3 за 2022 г. (илл. 1).

«ПОДАЙ ТЕБЕ ГОСПОДИ И ВПРЕДЬ ВРАГА ПОБЕЖДАТИ»

«Свет мой, братец Васенка, здравствуй, батюшка мой, на многие лета. И паки (снова — Б.С.) здравствуй, Божиею и пресвятыя Богородицы, и твоим разумом и счастьем победив агаряны.

Поддай тебе Господи и впредь враги побеждати, а мне, свет мой, веры не иметца, что ты к нам возвратишься. Тогда веры пойму, как увижу во объятиях своих тебя, света моего. А што, свет мой, пишешь, шштобы я помолилась, будто я верно грешная пред Богом и недостойна, однако же дерзаю надеяться на его благоутробие, аще и грешная. Ей, всегда того прошу, чтобы света моего в радости видеть. По сем здравствуй, свет мой о Христе, на веки несчетны. Аминь».

Письмо написано во время похода русских войск к Крыму в 1689 г.

Василий Васильевич Голицын возглавлял этот поход. Заметим, что опрометчиво было бы судить о царевне-правительнице и о её взаимоотношениях с князем Голицыным по приведённым здесь строкам письма.

О ПИСЬМАХ СОФЬИ АЛЕКСЕЕВНЫ

Это одно из двух известных шифрованных писем Софьи Алексеевны (илл. 2) Голицыну за время того крымского похода. Расшифровка писем опубликована Н.Г. Устряловым ещё в 1858 г.

Отметим, что письма зашифрованы на одном и том же ключе — искусственном алфавите. Это шифр простой замены. Оба письма носят личный характер, в них практически отсутствует деловая информация. Деловой можно признать лишь фразу во втором письме:

«Борису не побыть ли в Белогороде, также и Овраму, сверхъ того, как ты, радость моя, изволишь».

Из истории похода можно понять, что здесь речь идёт о военачальниках — боярине Борисе Петровиче Шереметеве и думном дворянине Аврааме Хитрово.

Случалось, царские письма перехватывали. В том же письме указано: «Почты от нас, светъ мой, посланы три. Четвёртой Шошинъ. Порадей, батюшка мой, чтобъ его окупить или на размену отдать».

Здесь упомянут Матвей Шошин, подъячий приказа Большой Казны. Он доставлял В.В. Голицыну письма от Ф.Л. Шакловитого во время крымского похода и побывал в плену. Крупный государственный деятель, глава царской охраны Фёдор Леонтьевич Шакловитый имел шифрованную переписку с Голицыным и пересылал ему шифрованные письма Софьи Алексеевны. Вероятно, Софья Алексеевна в деловой переписке применяла другие шифры.



Иллюстрация 2. Царевна Софья Алексеевна (работа XIX в.)



Иллюстрация 3. Царь Фёдор Алексеевич (работа XIX в.)

ОРГАНИЗАЦИЯ СВЯЗИ ПОХОДНОГО ШТАБА С МОСКВОЙ

Для обеспечения связи войск и московского правительства во время крымских походов 1687 и 1689 годов были организованы специальные почтовые станции. Гонцы имели возможность отдохнуть и сменить лошадей. Уже в 1687 году действовало 17 станций. Согласно реестру почтовой корреспонденции, в 1689 г. в штаб В. В. Голицына доставили 67 почтовых отправок из Москвы. Для каждого отправления указаны состав почты (перечислены все упаковки с их печатями) и сдавшее почту лицо, указано время отправления из Москвы (число и час). Кроме регулярной почты, через почтовые станции следовали личные гонцы главнокомандующего В. В. Голицына. Всего за полгода он направил в Москву 58 личных гонцов с тайнописными посланиями.

РЕШЕНО КИЕВ НЕ ОТДАВАТЬ

Крымские походы русских войск 1687 и 1689 годов заслуживают более подробного упоминания. Ведь их проведение

стало своеобразной оплатой принадлежности Киева России.

Как известно, 13-летняя Русско-польская война, в которую вынужденно вступила Россия, согласившись принять в свой состав Украину, завершилась перемирием на 13 с половиной лет в 1667 г. Тогда Россия удержала за собой левобережную (по Днепру) Украину, но Киев, лежавший на правом берегу, должен был вернуться в польское владение через два года, предоставленных для вывода русского гарнизона. Шляхте, утратившей свои владения в левобережной Украине, Россия выплатила из казны 200 тысяч рублей компенсации. Понятно, что Киев имел и имеет сакральное значение для русских, поэтому царская власть решила город не отдавать и за ценой, кровью или деньгами, не постоять.

ДИПЛОМАТИЧЕСКАЯ АКТИВНОСТЬ МОСКВЫ

Время шло, дипломатия работала. Надо сказать, что дипломатическая активность Москвы после царя Алексея Михайловича даже усилилась. Хотя постоянных дипломатических

представительств было ещё мало, потребность в них компенсировали приезды посольств. В царствование Фёдора Алексеевича только в июле 1677 года Москва одновременно принимала четыре посольства. А ведь иногда посольства состояли из нескольких сот человек. При правительнице Софье Алексеевне в 1686 году за границу выезжала российская дипломатическая делегация, вполне сравнимая с Великим посольством 1697–1699 годов. Она объехала 11 государств.

Московские дипломаты закрепили продвижение России и на Дальний Восток. В 1689 году трудами Фёдора Алексеевича Головина был заключён Нерчинский договор с Китаем.

ЕВРОПЕЙСКАЯ ОДЕЖДА И ГЛОБУС

Особенно активно и успешно Россия вошла в европейскую политику при Василии Васильевиче Голицыне, возглавлявшем Посольский приказ в 1682–1689 годах.

Его, как и Ф. А. Головина и значительную часть сотрудников Петра I, выдвинул царь Фёдор Алексеевич (илл. 3).



Иллюстрация 4. Портрет В.В. Голицына (работа XIX в.)

При В.В. Голицыне служащие Посольского приказа переоделись в европейскую одежду, а над главным из каменных корпусов Посольского приказа, вполне в духе времени, вознёсся огромный глобус, символизировавший весь земной шар.

«РАЗГОВОР ШЁЛ НА ЛАТИНСКОМ ЯЗЫКЕ...»

Вот что доносил о своём первом визите к главному российскому дипломату французский посланник:

«Я думал, что нахожусь при дворе какого-нибудь итальянского государя. Разговор шёл на латинском языке обо всём, что происходило важно тогда в Европе; Голицын хотел знать моё мнение о войне, которую император и столько других государей вели против Франции, и особенно об английской революции; он велел мне поднести всякого сорта водок и вин, советуя в то же время не пить их... Дом Голицына был один из великолепнейших в Европе».

ДИПЛОМАТИЧЕСКИЕ МАНЁВРЫ В. В. ГОЛИЦЫНА

Контакты с Францией, союзницей Турции и Крымского ханства, были важны для России. Ведь именно Турция, а не Польша контролировала правобережье Днепра с севера уже за много вёрст до днепровских порогов и также претендовала на левобережье. Десятилетняя война России с Турцией

завершилась в 1681 г. Бахчисарайским миром на 20 лет с признанием Киева и левобережья до запорожских земель за Россией. Всё же, учитывая все риски и выгоды, Россия вступила после долгих переговоров в «Священную лигу» европейских государств и, согласно договору, заключённому с Австрийской империей, Венецией и Польшей, обязалась помочь им в войне с Турцией.

КИЕВ НАШ

От России требовалось не допустить помощи турецким войскам со стороны крымского хана. Взамен Польша согласилась подписать «Вечный мир» с Россией, уступив при этом Киев за 146 тысяч рублей серебром. Мирный договор был подписан в Москве в апреле 1686 г. Так Киев утвердился за Россией юридически. На илл. 4 приведён известный портрет князя В.В. Голицына вместе с томом русско-польского мирного договора, закрепившего Киев за Россией.

МНОГОВЕКОВАЯ ОПАСНОСТЬ

Конечно, обязательства России в «Священной лиге» были тяжелы, ведь их выполнение означало новую войну с Турцией. Впрочем, русское государство, на протяжении столетий ощущавшее опасность с южного направления, всегда готовилось к обороне.

По возможности возводили укрепления и строили крепости, которые затем превращались в города. Так возникли Орёл и Курск, а в конце XVI и начале XVII веков — Белгород и Харьков. На илл. 5 приведена реконструкция путей грабительских набегов с крымского направления и указаны сторожевые города, построенные к середине XVII столетия.

Неся колоссальные материальные потери, Россия постоянно и вынужденно тратила силы и средства на защиту от опустошительных нашествий. Главными, конечно, были людские потери. За пять веков, до 1730-х годов, многие сотни тысяч, если не миллионы русских пленников прогнали по этим дорогам в Крым. Выживших продавали на невольничьих рынках. Огромные территории на плодородных землях вдоль путей набегов вынужденно пустовали.

ЗНАКОМЫЕ НАЗВАНИЯ

Осенью 1680 г. вышел указ царя Фёдора Алексеевича о строительстве нового города Изюм с крепостью и земляным валом. Уже в 1681 г. крепость была построена под руководством генерал-поручика Григория Ивановича Косагова. Расположение Изюма на илл. 5 можно найти в точке слияния рек Оскол и Северский Донец. Одновременно с его строительством по берегам Оскола и Северского Донца создавалась линия укреплений с городками Балаклея, Купянск... Не правда ли, знакомые названия?

ВЫПОЛНЯЯ ПРИНЯТЫЕ ОБЯЗАТЕЛЬСТВА...

Выполняя принятые обязательства, сам В.В. Голицын возглавил два демонстративных похода русских войск к Крыму в 1687 и 1689 годах. Вероятно, они потребовали огромных финансовых затрат, что стало дополнительной платой за передачу Киева России. Но эти походы показали и силу российской армии, состоявшей уже в основном из полков нового строя: солдатских, драгунских, гусарских и рейтарских.

Операции русских войск заслужили высокую оценку в Европе. Они были эффективны: уже первый поход вынудил турецкое командование снять войска с других фронтов и отправить их для защиты Константинополя, что обеспечило успех союзников.

ВПЕРВЫЕ ВЗЯТ ОЧАКОВ

Первый поход к Крыму из-за задержек со сбором войск начался лишь в середине мая 1687 г. Обоз воемной В.В. Голицыном 90-тысячной армии насчитывал более 100 тысяч возов с припасами. 2 июня подошли войска гетмана И.С. Самойловича (50 тысяч казаков), 22 июня обе армии достигли положения, отмеченного на илл. 5 рекой Конская. Осознав опасность, крымский хан Селим Гирей повелел своим войскам отступить вглубь ханства, отравить источники воды и выжечь степь. В таких условиях русское командование приняло решение об отступлении с 28 июня на северо-запад к Днепру, где и произошли боевые действия. На правобережье вскоре потерпела поражение Буджакская орда. Одновременно

корпус генерала Г. И. Косагова разгромил гарнизоны турецких крепостей в нижнем течении Днепра, впервые взял крепость Очаков и вышел к Чёрному морю.

24 августа поход был прекращён царским указом, но на южных рубежах оставили войска численностью 5 и 7 тысяч человек «для бережения великороссийских и малороссийских городов». Ещё несколько полков получили приказ строить укрепления на реке Самара для следующего похода в Крым.

ВТОРОЙ КРЫМСКИЙ ПОХОД

Новый поход начался в конце февраля 1689 г. 112-тысячная русская армия при 400 орудиях с огромным обозом одной колонной двинулась через степи к Крыму. 15 мая произошло крупное нападение крымских татар, отбитое артиллерийским и ружейным огнём. При этом погибли сыновья крымского хана. 20 мая русские войска подошли к Перекопу, за ним далее простиралась безводная степь. Армия терпела лишения, да и продолжение похода вглубь Крыма не планировалось. Ханские посланники просили мира, уже не помышляя о получении от России денежных выплат, предусмотренных Бахчисарайским мирным договором. Командование понимало, конечно, что окончательное устранение набегов из Крыма тогда было невозможно и должно было остаться делом неблизкого будущего. Основная цель похода — сковывание сил противника — была достигнута, поэтому поход был прекращён и В. В. Голицын отступил от Перекопа, сохранив почти всю армию и возвысив международный авторитет России.

БЛАГОДАРНАЯ ПАМЯТЬ ПОТОМКОВ

Но истинные цели крымских походов были известны лишь очень узкому кругу лиц в России, что использовали их противники и конкуренты в борьбе за собственную власть. Как известно, вскоре правительство Софьи Алексеевны было свергнуто и В. В. Голицына сослали на Север, в Пинегу, где он и умер 25 лет спустя. Недооценённый современниками, он заслужил благодарную память потомков.

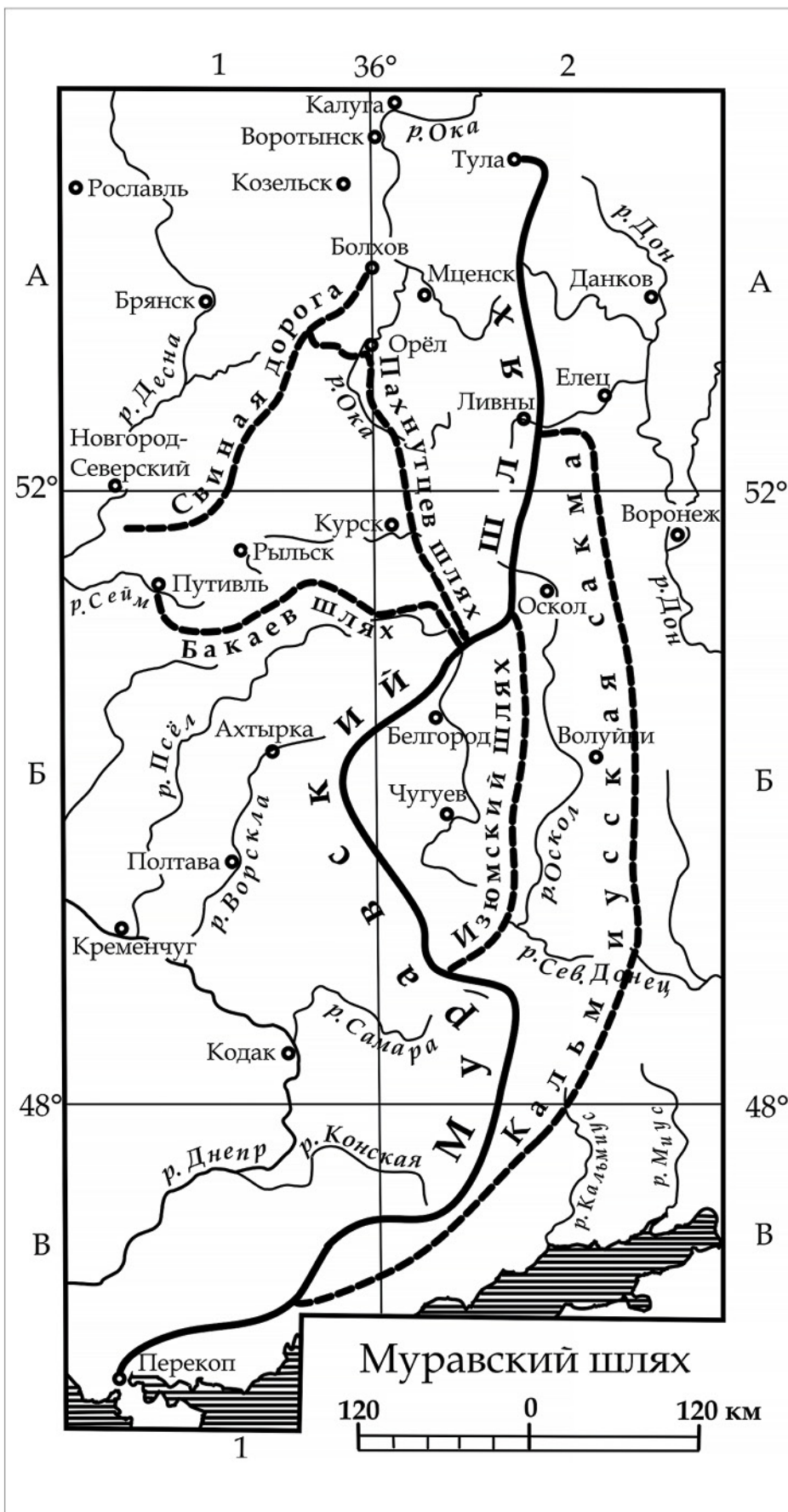
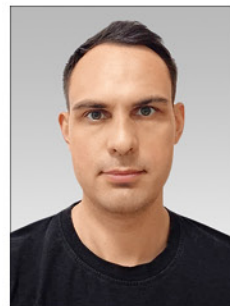


Иллюстрация 5. Пути крымских грабительских набегов

«ЕСТЬ В ГРАФСКОМ ПАРКЕ ЧЁРНЫЙ ПРУД...»

ИЛИ ОДИН РАЗ ВНЕДРИ, ПЯТЬ РАЗ ПОДДЕРЖИ



Александр ИГОНИН
эксперт BIS Journal

У большинства компаний постоянно появляются новые идеи и проекты, и от подразделений ИТ и ИБ как от инструментов бизнеса ожидается всецелая их поддержка. Если инициатива по-настоящему серьёзна и имеет большую важность для компании, на её реализацию могут быть выделены огромные средства, часть от которых, безусловно, идёт и на выполнение требований информационной безопасности.

Как это часто бывает, большие и серьёзные проекты нужно закончить «ещё вчера», и руководство готово к серьёзным затратам, чтобы это «вчера» наступило как можно быстрее: выделяют деньги на железо, софт, новую команду (или подразчика), призванных обеспечить должный уровень проектирования и внедрения. Порой в результате подобных грандиозных усилий получается создать действительно неплохую ИТ-систему. Что же может пойти не так?

К сожалению, очень часто «что-то не так» оказывается с поддержкой. Астрономические бюджеты без проблем тратятся на начальные стадии проекта, а после внедрения его просто кидают на плечи существующих ИТ- и ИБ-команд по принципу «Ну, мы тут внедрили, а вы там как-нибудь разбирайтесь». Практика показывает, что «как-то разобраться» в лучшем случае получается с трудом, а в худшем — не получается вообще.

При этом нужно отдавать себе отчёт в том, что поддержка — «удовольствие» весьма дорогое и продолжительное по времени. Нельзя просто выкопать большой пруд, засадить его лилиями и ожидать, что он всегда будет опрятным и цветущим: без регулярного обслуживания очень скоро цвести в нём будут только малопривлекательного вида водорос-

на обслуживание дополнительной инфраструктуры, и почти никогда — затраты подразделений ИБ на обеспечение требований безопасности. А между тем каждый новый источник данных и каждое новое правило в SIEM, каждый новый хост в сканере уязвимостей, каждый новый подключённый к средствам защиты информации элемент сети

требует регулярной проверки и, при необходимости, исправления обнаруженных проблем. И если проверка часто довольно хорошо поддаётся автоматизации, то вот анализ и исправление выявленных проблем обычно требуют человеческого вмешательства и могут занимать ощутимое время. А взять эти человеко-часы (а то и человеко-дни!) негде, потому что при планировании проекта эти затраты нигде не были учтены.

Вот и получается, что в проектных документах у нас нарисован красивый пруд, который спустя полгода после внедрения превращается в яму с водой, а спустя один-два года — в цветущую лужу с характерным болотным запахом. И как же так получилось?

Удивительный вопрос — насто-

ящая загадка, которая так и будет переходить из проекта в проект, пока затраты на поддержку и ИТ, и ИБ его составляющих не начнут учитываться на этапе планирования его бюджета. И затраты эти, к слову, весьма небольшие: их оценивают от 5 до 20 (а то и больше!) процентов в год от начальной стоимости внедрения.



ли. Точно так же и ИТ-системы без регулярной поддержки довольно быстро превращаются в болото. И задачи ИБ не исключение.

При планировании проекта часто учитываются расходы на поддержку оборудования и приложений у сторонних вендоров, гораздо реже — затраты собственных ИТ-подразделений

XII симпозиум **«Современные тенденции** **в криптографии»**

Тематика симпозиума включает следующие вопросы:

- исследование криптографических алгоритмов и протоколов, в том числе являющихся международными стандартами;
- эффективная реализация методов анализа криптографических алгоритмов и протоколов;
- оценка криптографической стойкости российских криптографических алгоритмов и протоколов;
- эффективная реализация российских криптографических алгоритмов и протоколов;
- математические аспекты криптографии;
- криптография в «Интернете вещей»;
- квантовая криптография и квантовые вычисления;
- постквантовая криптография;
- криптография и искусственный интеллект;
- криптографическая защита биометрических данных;
- другие актуальные и перспективные направления криптографии



ОРГАНИЗАТОРЫ



TK26



МИАН

ПРИ ПОДДЕРЖКЕ



ФСРБИТ

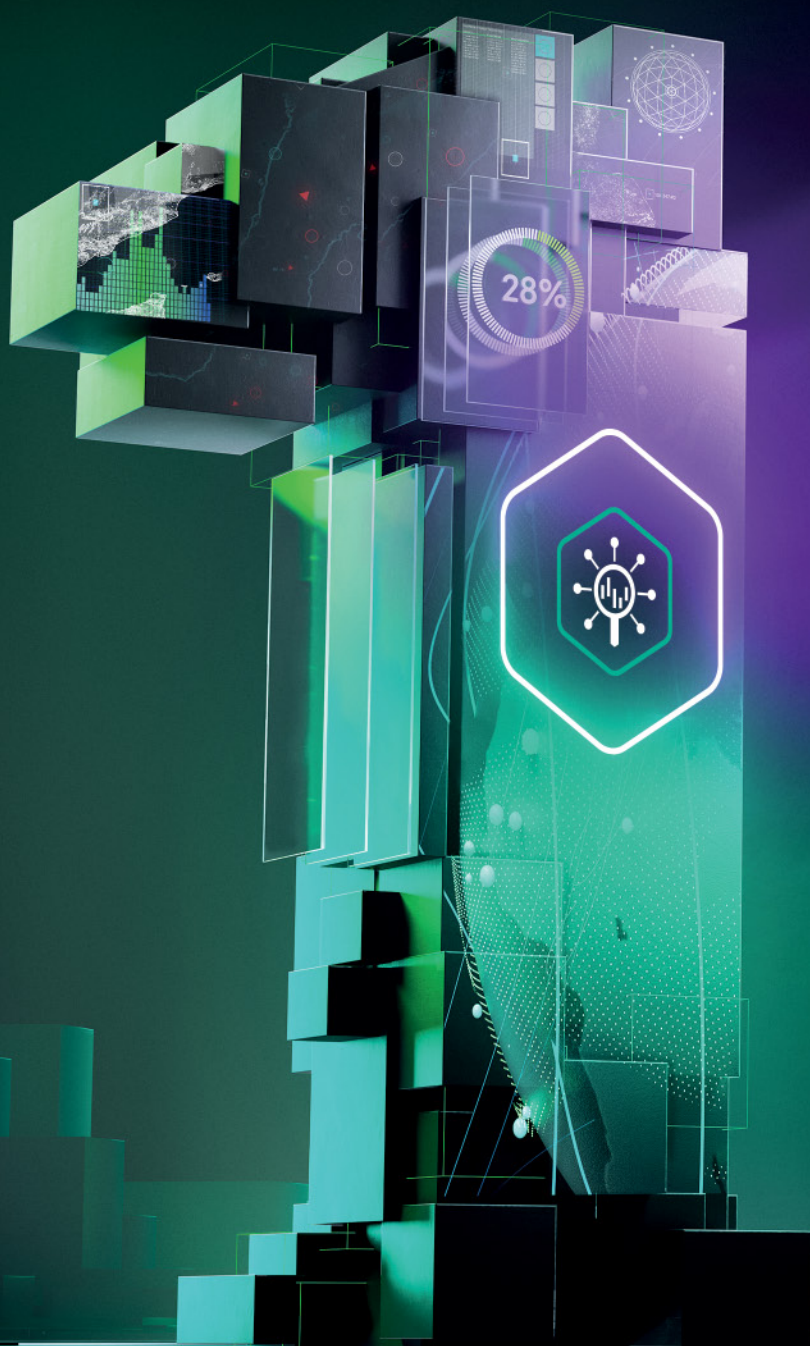
ОРГПОДДЕРЖКА



Kaspersky Unified Monitoring and Analysis Platform



Первоклассное SIEM-решение со встроенными
возможностями по обогащению и реагированию



kaspersky АКТИВИРУЙ
БУДУЩЕЕ