



BIS JOURNAL

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАНКОВ №3 (46) 2022



16

Анатолий АКСАКОВ
Государственная Дума РФ
**Банки в условиях
иностраннх санкций**



30

Вячеслав КАСИМОВ
Московский кредитный банк
**Эффект разорвавшейся
бомбы**

38

Владимир ЛАПТЕВ
Фонд развития программной
инженерии
**Бег на месте.
Репозитории в России**

78

Дмитрий МАХАЕВ
Эксперт
**Вопрос XXI века.
Про SOC и ГосСОПКА**

108

Борис СТОЛПАКОВ
Историк криптографии
**Расшифруй письмо
царевны Софьи**

ИМПОРТОЗАМЕЩЕНИЕ. КУЙ ЖЕЛЕЗО, ПОКА ГОРЯЧО!





Форум

Россия 2022

13–15
сентября

г. Санкт-Петербург

гостиница Кортъярд Санкт-Петербург Центр

XX МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ

по проблематике
инфраструктуры
открытых ключей
и электронной подписи



**Регистрация
открыта**

Подробности
на pki-forum.ru

Оператор



+7 (495) 921-42-44

info@avangardpro.ru

pki-forum.ru



Денис БАТРАНКОВ
член редколлегии BIS Journal

Тема импортозамещения на слуху давно, но особенно актуальной она стала в 2014 году, после активизации международных санкций. Тогда страна и начала потихоньку готовиться. И всё же уход иностранных производителей с нашего рынка стал громом среди ясного неба. Отказ лидеров сферы ИБ помогать России своей экспертизой многих застал врасплох. Компании Cisco, IBM, Forcepoint, Fortinet, Microsoft, Palo Alto Networks и другие просто отказались работать по уже оплаченным контрактам. А ведь их оборудование и софт защищали от современных угроз сети огромного количества российских компаний.

К счастью, в России есть и свои компании с международной экспертизой: Vi.zone, Group-IB, Лаборатория Касперского, Ростелеком-Солар, Positive Technologies и другие. Их продукция и эксперты востребованы сегодня как никогда. Я знаю, что многим сотрудникам этих компаний пришлось оказывать срочную помощь предприятиям и организациям, пострадавшим от атак после прекращения работы иностранного оборудования.

При этом компаний, оставшихся один на один с новыми угрозами, ещё очень много. Что же им делать? Сегодня мы обсудим наши первоочередные действия, связанные с уходом иностранных производителей. Уже накопился опыт и статистика используемых методов взломов, и мы подсветим задачи, на которых стоит сфокусироваться. В текущей ситуации парадигма защиты изменялась: теперь, чтобы минимизировать ущерб, нужно хотя бы вовремя обнаружить взлом.

Раньше в контексте большого бизнеса на безопасность не особенно смотрели, в итоге выяснилось, что 9 из 10 компаний взломаны и не знают об этом. По информации аналитических лабораторий, хакеры в среднем проводят в сети 200 дней до того, как начинают наносить вред.

Люди нередко хорошо знают, как правильно поступать, но почему-то часто откладывают это на потом: поменять пароли, сделать бэкапы, составить актуальную логическую и физическую схему сети, разобраться в адресном пространстве, внедрить двухфакторную аутентификацию, хотя бы для VPN, нанять людей, вывести часть функций на аутсорсинг...

И сегодня наступило то самое время, когда не надо откладывать. Пора действовать!

ОБЩЕСТВЕННЫЙ РЕДАКЦИОННЫЙ СОВЕТ

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

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Велигура А.Н. — председатель комитета по банковской безопасности Ассоциации российских банков, руководитель комитета по безопасности НП «НПС», CISA, кандидат физико-математических наук
Виноградов А.Ю. — специалист Службы информационной безопасности КБ Максима (ООО)
Вихорев С.В. — советник генерального директора по информационной безопасности IT Expertise
Дзержинский Ф.Я. — независимый эксперт
Зубков А.Н. — генеральный директор ООО «Медиа Группа „Авангард“», директор Фонда содействия развитию безопасных информационных технологий (ФСРБИТ)
Курило А.П. — советник по вопросам ИБ ФБК и FBK CyberSecurity, кандидат технических наук
Левиев Д.О. — председатель Совета НП «Партнёрство специалистов по информационной безопасности»
Мельников С.Ю. — заместитель генерального директора ООО «Лингвистические и информационные технологии», доктор физико-математических наук
Некрасов И.В. — главный редактор журнала
Одувалов М.В. — 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. — руководитель департамента информационной безопасности факультета информационных технологий Финансового университета при Правительстве РФ, 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
Сабанов А.Г. — заместитель генерального директора АО «Аладдин РД»
Сумманен К.Т. — директор по управлению проектами — вице-президент, Банк ВТБ (ПАО), кандидат физико-математических наук
Хайретдинов Р.Н. — директор по росту компании Bi.ZONE

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: **Victor Miller-Gausa**
Фото в номере: **Unsplash.com, Pixabay.com**
Цветокорректор: **Наumenko М.Б.**

УЧРЕДИТЕЛЬ-ИЗДАТЕЛЬ

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

Зарегистрирован 13 августа 2010 года Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). 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 18.07.2022. Тираж 5000 экз. Заказ № 742022. Цена договорная. Отпечатан в типографии «Московский Печатный Двор», 123298, г. Москва, 3-я Хорошевская 18, корп. 1, офис 201А

© BIS Journal, 2022



НОВОСТИ

5 Технологии, криминал, кадры

АКТУАЛЬНЫЕ МНЕНИЯ

- 8 **Об указе Президента РФ**
Сергей Вихорев (ИТ-Экспертиза)
Верной ли дорогой идёте, товарищи?
- 11 **Об инсайдерах**
Олег Седов (BIS Journal)
Инсайдеров всё больше
- 14 **О господдержке**
Алексей Войлуков (Ассоциация банков России)
Вывести всех на аутсорсинг!



РЕГУЛЯТОРЫ

- 16 **От первого лица**
Анатолий Аксаков (Государственная Дума РФ), Тимур Аитов (ТПП РФ)
Стратегии прорыва
- 22 **Банк России**
Алёна Игнатъева (BIS Journal)
Критичная не равно критическая
- 24 **Банк России**
Александр Виноградов (КБ «Максима»), Анастасия Николаева (AKTIV CONSULTING), Дмитрий Левиен (НП «ПСИБ»)
«Выполнить не представляется возможным»

БАНКИ

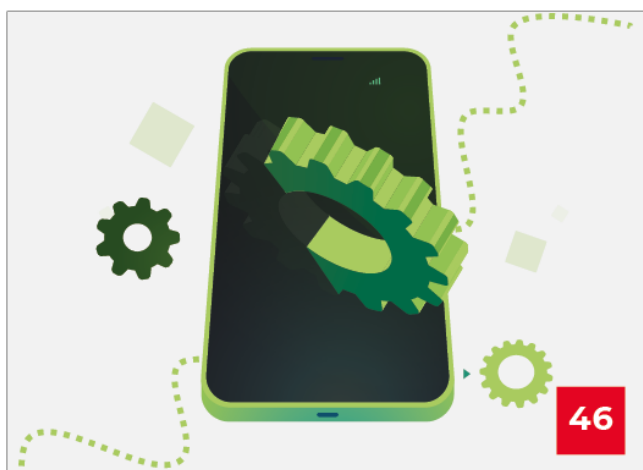
- 26 **Что делать?**
Денис Батранков (BIS Journal)
В первую очередь
- 30 **Собеседник**
Вячеслав Касимов (Московский кредитный банк)
Кто первый создаст Next Generation Firewall?
- 34 **Антифрод**
Василий Окулесский (эксперт ИБ)
Антифрод сегодня
- 38 **Репозитории**
Владимир Лаптев (Фонд развития программной инженерии)
Бег на месте или так надо?
- 42 **Облака**
Александр Долбнев, Андрей Иванов (Yandex.Cloud)
Облака в пейзаже
- 46 **ФинТех**
Юрий Кардюков (eKassir)
Зачем банкам подключаться к открытым API?
- 49 **Импортозамещение**
Сергей Шалимов (Аладдин Р.Д.)
Замещение горы
- 52 **Аутентификация**
Алексей Сабанов (Аладдин Р.Д.)
Учитывать при выборе





УГРОЗЫ И РЕШЕНИЯ

- 56 **Антифрод**
Сергей Парфёнов (Фаззи Лоджик Лабс)
«Нас не догонят!»?
- 58 **Моделирование кибератак**
Максим Пятаков (CtrlHack),
Владимир Соловьёв (АО «ДиалогНаука»)
**Русский хакер. Белый хакер.
Робот-хакер**
- 60 **Электронная подпись**
Павел Смирнов (КриптоПро)
**Архивное хранение электронных
документов с ЭП**
- 62 **Кадры**
Евгения Колодина, Ксения Минакова
(ГК «ЦИБИТ»)
Кадры решают всё
- 64 **Требования регуляторов**
Алексей Парфентьев (СёрчИнформ)
Время перемен



ИНФРАСТРУКТУРА

- 66 **Деловые мероприятия**
Николай Кольский (BIS Journal)
**«Надо глубже планировать, глубже
бюджетировать, и всё получится»**
- 68 **Деловые мероприятия**
Корней Реут (BIS Journal)
CISO Форум — 2022
- 70 **Деловые мероприятия**
Павел Никифоров (BIS Journal)
Positive Hack Days 11
- 72 **Деловые мероприятия**
Николай Кольский (BIS Journal)
**Конференция «Информационная
безопасность банков»**
- 75 **Деловые мероприятия**
Марк Новоначный (BIS Journal)
Форум DLP+ 2022
- 78 **ГосСОПКА**
Дмитрий Махаев (эксперт ИБ)
Вопрос XXI века
- 83 **Open Source**
Александр Герасимов (эксперт ИБ)
ИБ-решения по модели Open Source
- 84 **Облака**
Павел Иванов, Михаил Левашов
(Финансовый университет при
Правительстве РФ)
Новые смыслы



СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

88 Утечки

Андрей Жаркевич (ООО «Антифишинг»)
Ваше благородие, госпожа утечка



ОБРАЗОВАНИЕ И КАРЬЕРА

91 Олимпиады

Артём Зубков (ФСРБИТ)
Связь поколений как фундамент
будущего

93 Рынок труда

Ксения Трохимец (hh.ru)
Проблема дефицита ИБ-специалистов
обостряется



ЗА РУБЕЖОМ

94 Образование и карьера

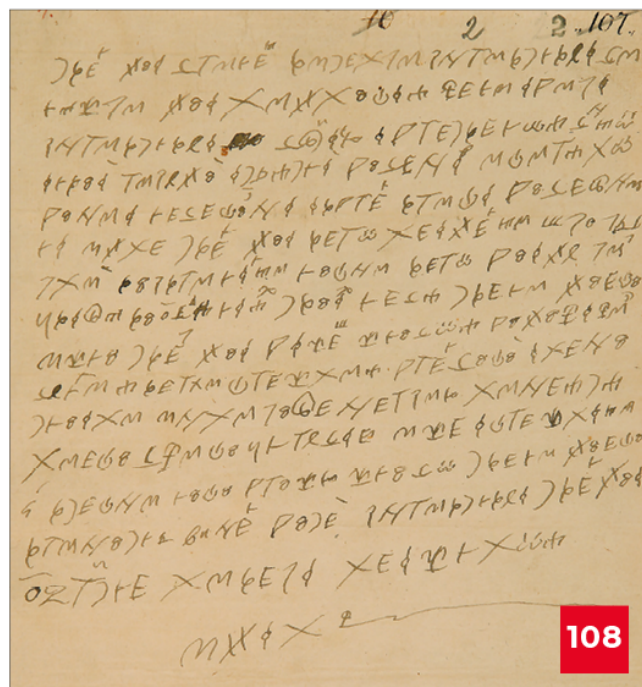
Марина Бродская (BIS Journal)
Для чёрного колледжа наступили
чёрные дни

97 Обзор ИноСМИ

Анна Катанкина (BIS Journal)
Министры, вымогатели, герои...

100 Их нравы

Екатерина Рачкова (Банк ВТБ)
Хавала



СУБЪЕКТЫ

104 История

Борис Столпаков (историк криптографии)
Математизация криптографии
в событиях и лицах

108 История

Борис Столпаков (историк криптографии)
Письма и бумаги императора Петра
Великого

112 Заметки безопасника

Александр Игонин (BIS Journal)
В шаге от аутсорсинга

АНАЛОГ SWIFT НА БЛОКЧЕЙНЕ

Центр технологий распределённых реестров СПБГУ сообщил о старте работы над децентрализованной международной системой межбанковских финансовых сообщений с использованием блокчейн-технологий. Разработчики планируют заменить ею SWIFT в каждой стране-участнице.

Пресс-релиз гласит, что «это независимая система, которая не может извлекать прямую финансовую выгоду и создавать ограничения для отдельной страны или организации».

«Решение даст всем участникам мировой банковской системы новый

инструмент, который позволит с высокой степенью надёжности обмениваться финансовыми сообщениями. При этом банки смогут не опасаться негативных последствий, а государства смогут проводить более самостоятельную политику», — пояснил директор Центра технологий распределённых реестров СПБГУ Дмитрий Шишмаков.

По плану каждая страна будет хранить часть программного кода и БД, становясь совладельцем системы. Центр технологий распределённых реестров СПБГУ при этом должен стать оператором системы.



ЧИПЫ ПРИЕДУТ ИЗ КИТАЯ

Чипы для карт «Мир» могут приехать из Китая. На сегодняшний день это единственный способ приобрести микропроцессоры для изготовления пластиковых карт платёжной системы «Мир».

По словам директора организационно-правового департамента АО «НСПК» Олега Тишакова, дефицит карточных чипов «никуда не делся» и по-прежнему остаётся серьёзной проблемой. Поставщики микропроцессоров из европейских стран перестали работать с российской

платёжной системой, а азиатские производители приостановили выпуск чипов из-за пандемии.

Сегодня НСПК ищет новых поставщиков. «На территории Китая нашли уже несколько поставщиков, сейчас мы находимся в процессе их сертификации», — рассказал Олег Тишаков. — Таким образом мы пытаемся минимизировать риски того, что на новых карточках не будет чипов. Кроме того, мы как оператор платёжных систем решили продлевать сроки действия карточек, которые уже выпущены на сегодняшний момент. И они будут работать до момента замены их новыми карточками — это касается платёжной системы «Мир», а карты международных платёжных систем Visa и Mastercard — до окончания срока их действия».

Маловероятно, что проблема дефицита микропроцессоров будет решена в ближайшее время, хотя бы потому, что процедура сертификации китайских компаний для работы с Россией не быстрый процесс.



ОПЛАТА ПО QR

До конца года на миллионе устройств эквайринга от «Сбера» появится возможность производить оплату с помощью сервиса «SberPay оплата по QR». А в 2023 году банк собирается оснастить этой технологией весь парк своих POS-терминалов.

Оплата с помощью сервиса «SberPay оплата по QR» (в один клик) доступна владельцам как «яблочных» гаджетов, так и «андроидов».

«Оплата таким методом проходит быстрее, чем стандартное сканирование QR-кода на кассе. Данный способ оплаты абсолютно безопасен, так как персональный QR-код каждый раз обновляется, поэтому его не получится скопировать, чтобы совершить платёж. При этом оплата пройдёт даже без доступа в Интернет», — рассказали в финучреждении.



ТРЕНД НА ДИПФЕЙКИ

ФБР сообщает о росте числа жалоб на дипфейки в заявках на вакансии, связанные с ИТ-«удалёнкой». С помощью дипфейк-технологий «соискатели» создают видеоролики, изображения и аудиозаписи, используя украденную личную информацию, после чего пытаются выдать себя за другого человека.

Так, в Бюро поступили жалобы на подмену голоса во время онлайн-интервью: если во время собеседования видно лицо человека, то его движения губ часто не полностью совпадают со звуком.

Известно и то, что злоумышленники уже пытались попасть на должности, подразумевающие доступ к клиентским данным, финансовой информации, а также корпоративным БД.

Эксперты ФБР попросили жертв (включая компании, получившие такого рода дипфейки) сообщить любую информацию, которая поможет идентифицировать мошенников через центр жалоб на интернет-преступления.

«ГИДРЕ» ОТСЕКЛИ ПЕРВУЮ ГОЛОВУ

Мещанский районный суд Москвы арестовал Дмитрия Павлова по делу о сбыте наркотиков в особо крупном размере (часть 5 статьи 228.1 УК РФ). Ему грозит от 15 до 20 лет лишения свободы. Неделями ранее Федеральное ведомство уголовной полиции Германии закрыло самую торговую площадку Hydra Market.

Минюст США также предъявил Павлову обвинения в распространении наркотиков и администрировании серверов «Гидры», а Минфин США ввёл санкции против ресурса.

Дмитрий Павлов при этом отрицал сотрудничество с Hydra Market. Он утверждал, что не знал, кто именно хостится на арендованных у «Промсервиса» серверах.



КРИПТОСУДЫ СТАНОВЯТСЯ ПОПУЛЯРНЫМИ

Количество судебных разбирательств, так или иначе связанных с криптоактивами, за год выросло в полтора раза. 954 дела возбудили по уголовным статьям, 365 — гражданские дела, 141 — банкротные и только 71 — административные.

Чаще прочего коины фигурируют в делах, связанных с оборотом наркотиков. Среди других уголовных разбирательств — отмывание денег. Замыкают топ незаконные организации и проведение азартных игр.

В гражданско-правовых спорах на первом месте — требования о взыскании необоснованного обогащения при покупке криптовалюты.

Банкротных же «криптодел» в прошлом году стало в два раза больше. В делах о банкротстве коины упоминаются в качестве имущества, и поэтому для доказательства владения ими необходимо предоставить документы.



УГЛУБЛЁННОЕ РАССЛЕДОВАНИЕ

Bank of the West, имеющий более 600 отделений в США и являющийся на данный момент 32-м в списке самых крупных финорганизаций страны, впервые зафиксировал множество подозрительных попыток снятия средств в прошлом ноябре. Тогда руководство банка объединилось с правоохранителями для проведения углублённого расследования.

Проверка всей сети банкоматов завершилась в апреле. Выяснилось, что кто-то «подсадил» скиммеры на определённое количество устройств.

«Установленное в банкомате скимминговое устройство мешало проведению обычной операции с дебетовой картой и позволяло злоумышленнику украсть номера карт, PIN-коды, имя и адрес жертвы», — гласит официальное заявление банка. «Украденная информация могла быть использована для создания поддельных дебетовых карт и кражи средств».

Представители Bank of the West уверяют: использование украденных данных о картах быстро пресекается, а все взломанные счета контролируются специалистами.

ОБНАЛЬЩИКИ КРУПНОГО КАЛИБРА

Сотрудники экономической полиции Санкт-Петербурга пресекли деятельность группы лиц, занимавшейся обналичиванием средств клиентов. Всего с 2016 года до момента поимки мошенникам удалось обналичить около 800 млн рублей.

Злоумышленники создали несколько подконтрольных фирм и через их корпоративные счета снимали денежные средства в финорганизациях с помощью банковских карт.

«Обнальщики находили физических и юридических лиц, заинтересованных в обналичивании своих доходов и уходе от уплаты налогов. По договорённости с клиентом безналичные денежные средства переводились на расчётные счета аффилированных фирм, а затем обналичивались. За свою работу „банкиры“ брали 15% от обналичиваемой суммы. За шесть лет противоправной деятельности злоумышленники „заработали“ порядка 120 млн рублей, обналичив около 800 млн рублей», — говорится в сообщении ведомства.

Возбуждено уголовное дело по части 2 статьи 172 УК РФ «Незаконная банковская деятельность». В рамках обысков изъяты банковские карты, печати подконтрольных организаций, мобильные телефоны, компьютеры, а также документы финансово-хозяйственной деятельности.



FINANCIAL TIMES: КУРС НА ЮЖНУЮ АМЕРИКУ

По сообщению Financial Times, с начала весны наблюдается отток предпринимателей и айтишников из России. В том числе в страны Южной Америки. Точное число мигрировавших «на юга»,



однако, неизвестно — местные статистические службы не выделяют этих специалистов в отдельную категорию.

Профессор ICESI Владимир Рувински отметил, что за последние месяцы в южноамериканские страны приехали «сотни» российских граждан. Причины — по мнению эксперта — «смягчённые правила въезда и неоднозначное отношение к западным санкциям».

Рувински считает, что многие айтишники более не могут продолжать деятельность в России и поэтому ищут выход на новые рынки. По его мнению, речь идёт о «новой волне миграции».

По данным ФСБ, за первый квартал текущего года из РФ выехали более 3,8 млн человек. Чаще прочего — в Грузию, Турцию, Казахстан, Финляндию, Армению и Эстонию.

«ОРГАНИЗОВАННОЕ СОКРАЩЕНИЕ БИЗНЕСА»

Президент Microsoft Брэд Смит заявил, что его компания собирается и дальше сворачивать бизнес в РФ — до минимума или полного прекращения деятельности. «Мы работаем там всё меньше и меньше, пока там ничего не останется или почти ничего», — сказал он.

Смит добавил, что Microsoft не бросит своих российских сотрудников — им окажут своевременную помощь.

Cisco также объявила о постепенном уходе из России и Беларуси. Техкомпания начнёт «организованное сокращение бизнеса» и напрямую свяжется с клиентами для урегулирования финансовых вопросов, в том числе для возврата предоплаты за услуги.

Сотрудникам российских и белорусских филиалов Cisco пообещала «поддержку в это тяжёлое время».



НЕДОСЧИТАЛИСЬ 170 ТЫСЯЧ АЙТИШНИКОВ

На заседании комитета Совета Федерации по социальной политике замглавы МВД Игорь Зубов сообщил, что из-за массового отъезда айтишников за рубеж в России наметился их дефицит.

«В связи с санкционными режимами у нас имел место отток ИТ-специалистов, причём существенный, в ряд стран. Степень нуждаемости определяется экспертами примерно в 170 тысяч, а в целом в отрасли занят один миллион человек», — уточнил он.

Кроме этого, Зубов призвал поддержать закон об упрощённой выдаче ВНЖ иностранным ИТ-специалистам, обсуждаемый в эти дни Совфедом.

Ранее глава Минцифры Максют Шадаев заявлял о возвращении 80% уехавших с конца февраля россиян (преимущественно ИТ-специалистов). Сообщалось, что эта цифра была определена «по SIM-картам».

НАШЛИ СВОЁ МЕСТО

Банк «Открытие» до конца года переведёт 800 своих разработчиков, аналитиков и других ИТ-специалистов в ООО «Дискавери Лабс».

Созданная два месяца назад, «Дискавери Лабс» получит развитие как «центр разработки инновационного ПО компаний группы». В неё уже вошла часть финтех-стартапа Mission: Luna, а также сотрудники покинувших Россию иностранных ИТ-компаний.

Mission: Luna, в свою очередь, планировала запустить летом «Полезный и человеческий сервис для повседневных финансов», но ЦБ исключил маркетплейс из реестра операторов финплатформ. В «Открытии» заявили, что «отказались от проекта, поскольку в текущих условиях реализовать его невозможно».

ВЕРНОЙ ЛИ ДОРОГОЙ ИДЁТЕ, ТОВАРИЩИ?

ЭССЕ О ПРОБЛЕМАХ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ В СВЯЗИ С ИЗДАНИЕМ УКАЗА
ПРЕЗИДЕНТА РФ ОТ 01.05.2022 № 250



Сергей ВИХОРЕВ
советник
генерального
директора
ООО «ИТ-Экспертиза»

В последнее время, с началом специальной военной операции, а также приостановки деятельности в России иностранных поставщиков, НКЦКИ¹ ФСБ России фиксирует многократный рост компьютерных атак. По данным экспертов, число кибератак на российские компании в первые месяцы 2022 года выросло в четыре раза по сравнению с тем же периодом 2021 года². Усложнение ландшафта угроз и новые реалии рынка требуют комплексного подхода к кибербезопасности, включающего расширенные системы обнаружения и реагирования на сложные кибератаки. Оперативно реагируя на сложившуюся ситуацию, президент издал 1 мая 2022 года Указ, направленный на усиление информационной безопасности на объектах критической информационной инфраструктуры. Для этого предлагается создать (возродить?) государственную систему защиты информации. Указ касается многих: от таких гигантов, как «Росатом», «Газпром», «Русгидро», РЖД, до каждого юридического лица, являющегося субъектом КИИ и подпадающего под действие Федерального закона от 26.07.2017 № 187-ФЗ.

Указ уже вступил в силу, однако проблемы с его реализацией есть. И именно об этом я хотел бы поговорить. Но прежде давайте немного вспомним историю.

ЭКСКУРС В НЕДАЛЁКОЕ ПРОШЛОЕ

Сначала было слово, и слово это было ПД ИТР³. И было всё хорошо! Каждый знал, что делать и как делать, потому что в стране была чёткая

¹ Национальный координационный центр по компьютерным инцидентам.

² <https://habr.com/ru/news/t/657473>

³ Противодействие иностранным техническим разведкам — термин, который в социалистические времена включал в себя и информационную безопасность. Впоследствии, когда СССР был развален и все стали «друзьями», был заменен на термин ПД ТСР — противодействие техническим средствам разведки, но сути это не изменило.

линия партии. Партия сказала: «Надо», — все ответили: «Есть»! Да, были времена, были и люди... А потом, как сказано в детективном фильме «Чёрный принц», пришёл гегемон⁴, и всё пошло прахом. Да, 90-е не очень хочется вспоминать, но это наша история, и без её осмысления мы вряд ли двинемся дальше. Разруха в промышленности (пропустим), дефицит товаров (пропустим), внешнее управление (а это пропустить нельзя), изменение юридического ландшафта (признание верховенства частной собственности). В результате государство частично потеряло контроль над стратегически важными направлениями развития и секретами. И это был период разбрасывания камней. Но даже в это сложное время государство блюдёт свои интересы и пытается обеспечить защиту своих секретов. Выходит постановление Правительства № 912–51 О создании ГСЗИ⁵. Опять всё чётко и ясно, но только для гостайны.

Ну, слава богу, этот период мы прошли. А тут, аккурат, мы начали отстаивать своё право называться РОССИЕЙ и теперь вошли в период собирания камней. В нашем приземлённом мире ИБ-шников всё, что надо защищать, мы называем скромно: объект критической информационной инфраструктуры. А на самом деле ведь это объекты национального достояния. Представьте, не сможет работать КамАЗ или 1-я ЦКБ? Сложно будет! Да и на внешнем фронте не так всё благополучно. Эти информационные хрущи просто достали! К сожалению, нельзя их всех собрать в ведро и сжечь...

А теперь о тех проблемах, которые, на мой взгляд, возникнут при реализации указаний Президента РФ.

⁴ Гегемон — лицо, государство или общественный класс, осуществляющие лидерство (гегемонию).

⁵ Постановление Совета министров — Правительства РФ от 15.09.1993 № 912–51 «Об утверждении Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от её утечки по техническим каналам».

КАДРЫ РЕШАЮТ ВСЁ!

Одним из главных направлений по совершенствованию информационной безопасности Указ определяет создание во всех организациях специальной структуры, обеспечивающей решение данных вопросов. А для придания должного веса этой проблеме предлагает возложить на заместителя руководителя организации полномочия по обеспечению информационной безопасности (читай — управление такой структурой). При этом персональная ответственность за обеспечение информационной безопасности в организации остаётся непосредственно за руководителем организации.

Таким образом, нам нужны руководители, способные правильно организовать процесс обеспечения информационной безопасности, и спецы, способные правильно эксплуатировать систему защиты информации объекта критической инфраструктуры.

Ну, со вторыми, наверное, проблему решить можно, правда, надо учитывать, что к ним предъявляются специальные требования по компетенции⁶. Будем надеяться, что многочисленные кафедры информационной безопасности различных вузов смогут подготовить достаточное количество специалистов. А вот с первой категорией — проблема. Думаю, что трёхлетний стаж здесь будет маловато.

Во-первых, для эффективной работы надо хорошо знать не только основы информационной безопасности, но и специфику отрасли, в которой работает организация. А это за 1–3 года не узнаешь. Во-вторых, нужен простой житейский опыт. Только обладая таким опытом, можно принимать взвешенные решения, которые могут затрагивать различные аспекты. Такой опыт в 25–28 лет ещё не приобретается. Такой опыт характерен для более солидных личностей, лет 45 (знаю по своему опыту), когда знания, помноженные на жизненный опыт, позволяют мыслить стратегически и принимать верные решения, основанные на глубоком анализе обстановки. А много ли у нас на сегодня серьёзных 45-летних специалистов, способных взять на себя полномочия заместителя руководителя организации и нести персональную ответственность за обеспечение информационной безопасности? Не уверен. А потребность — большая, ведь объектов критической информационной

⁶ Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования», п. 12.

**УКАЗ****ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ****О дополнительных мерах по обеспечению информационной безопасности Российской Федерации**

В целях повышения устойчивости и безопасности функционирования информационных ресурсов Российской Федерации п о с т а н о в л я ю:

1. Руководителям федеральных органов исполнительной власти, высших исполнительных органов государственной власти субъектов Российской Федерации, государственных фондов, государственных корпораций (компаний) и иных организаций, созданных на основании федеральных законов, стратегических предприятий, стратегических акционерных обществ и системообразующих организаций российской экономики, юридических лиц, являющихся субъектами критической информационной инфраструктуры Российской Федерации (далее — органы (организации):

а) возложить на заместителя руководителя органа (организации) полномочия по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты;

б) создать в органе (организации) структурное подразделение, осуществляющее функции по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, либо возложить данные функции на существующее структурное подразделение;



Указ Президента РФ от 01.05.2022 № 250

инфраструктуры — много. Целых 13 сфер деятельности.

Где брать таких специалистов? Проблема!

А сроки построения всей государственной системы защиты информации очень напряжённые. Не получилась бы здесь профанация, когда к управлению процессом обеспечения информационной безопасности придут дилетанты. По всей вероятности, в подготавливаемом Правительством РФ типовом положении о заместителе руководителя органа (организации), ответственного за обеспечение информационной безопасности, целесообразно определить

критерии к компетенции таких ответственных работников, а может быть, даже предусмотреть аттестацию таких специалистов по аналогии с руководителями РСО.

ИНТЕРЕСЫ БИЗНЕСА И ГОСУДАРСТВА

Здесь же ещё одна проблема — деньги. Подразделения по обеспечению безопасности информации — это всегда затратные (читай убыточные) подразделения для собственника бизнеса. Конечно, когда речь заходит о федеральных органах исполнительной власти, вышших исполнительных органах государственной власти субъектов РФ, государственных фондов, государственных корпораций (компаний) и иных организаций, созданных на основании федеральных законов, можно обойтись директивным решением, и они будут вынуждены создавать такие подразделения. А что делать с остальными, в том числе и обычными юридическими лицами? Обязать их создавать такие подразделения — это означает, что государство вмешивается в процесс хозяйственной деятельности собственника, что, в принципе, недопустимо.

Значит, надо найти баланс между интересами собственника бизнеса и государства. Надо как-то убеждать собственника в необходимости таких действий, социальной ответственности бизнеса и необходимости принимать определённые меры. Директивным давлением здесь проблемы не решишь. Давайте не будем забывать, что по закону именно субъект КИИ проводит категорирование, определяет, есть у него объекты КИИ или нет⁷. Такое положение дел может привести к тому, что у нас формально не будет объектов критической информационной инфраструктуры (нет объекта — нет подразделения, нет «бесполезных» затрат для бизнеса). По всей вероятности, надо предусмотреть какие-то льготы и преференции со стороны государства, которые могли бы заинтересовать руководителей бизнеса экономически создавать специальные подразделения по обеспечению информационной безопасности и проводить комплекс мер по защите информации. Либо создавать чёткую юридическую основу таких структур, подкреплённую жёстким репрессивным механизмом, что, конечно, в современных условиях нежелательно.

Кстати, возлагая персональную ответственность за обеспечение информационной

безопасности на руководителей организаций, хотелось бы знать, сколько это «в граммах»? Декларация ответственности — это ещё не ответственность. Ну возложили, ну не сделал. И что? С работы не снимешь — я сам хозяин, взыскание объявишь — ну чёрт с ним, зато прибыль больше, пожурили — да и ладно.

ИМПОРТОЗАМЕЩЕНИЕ И СРОКИ

Об этом уже говорено-переговорено. А сколько различных конференций проведено на эту тему! И между тем Президент РФ ставит чёткий и конкретный срок: с 1 января 2025 г. органам (организациям) запрещается использовать средства защиты информации, странами происхождения которых являются иностранные государства, совершающие в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия, либо производителями которых являются организации, находящиеся под юрисдикцией таких иностранных государств, прямо или косвенно подконтрольные им либо аффилированные с ними. Казалось бы, речь только о средствах защиты информации. Но если посмотреть на проблему шире, то окажется, что многие существующие сейчас системы защиты информации используют встроенные в операционные системы и СУБД механизмы защиты информации. Более того, нормативные документы требуют в приоритетном порядке применять именно средства защиты информации, встроенные в программное обеспечение и (или) программно-аппаратные средства значимых объектов⁸.

Следовательно, с 01.01.2025 запрещается использовать в том числе и все зарубежные ОС и СУБД. Готова ли наша промышленность к таким радикальным мерам? Буду рад, если это так, однако... И между тем, как говорил известный политический деятель: «Наши цели ясны, задачи определены. За работу, товарищи!»⁹

Написав всё это и ещё раз внимательно перечитав, задался вопросом: а прав ли я в своих рассуждениях? И засомневался. Поэтому передаю вам, коллеги, право дать своё заключение.

⁸ Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», п. 27.

⁹ Заключительные слова выступления на XXII съезде Коммунистической партии Советского Союза (1962) её руководителя, Первого секретаря Никиты Сергеевича Хрущёва.

⁷ Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Ст. 7.



ИНСАЙДЕРОВ ВСЁ БОЛЬШЕ

И С ЭТИМ НАДО ЧТО-ТО ДЕЛАТЬ...

Человеческий фактор всегда был в группе риска. Те, кто верит, что в работе служб ИБ ничего не изменилось, безусловно, правы. ИБ всегда жили в состоянии стрессов, противодействия атакам и предотвращения инцидентов. Но сейчас всё в крайностях, всё без компромиссов и многократно усилено.

ТАКОЕ ВРЕМЯ

Согласно скучному определению из Wikipedia, «Инсайдер (англ. insider) — это член группы людей, имеющей доступ к информации, недоступной широкой публике. Инсайдер противопоставляется внешнему специалисту, который может обеспечить всесторонний теоретический



Олег СЕДОВ
член экспертного
совета BIS Journal

анализ, а инсайдер обладает информацией из первых уст».

В корпоративной же среде принято считать, что инсайдер — это плохой парень с мутными целями, который вообще не должен был попасть в компанию. Служба безопасности не должна таких пропускать. Она, как правило, и не пропускает, но, в отличие от роботов, люди имеют обыкновение меняться. И не просто меняться, а меняться неожиданно. Ещё вчера лояльный сотрудник сегодня — под воздействием внутренних или внешних причин — в корне изменяет к ней своё отношение. Внутренними причинами может послужить увлечение молодой подружкой с завышенными запросами или непредвиденные расходы на врачей для родных и близких. За примерами внешних причин тоже далеко ходить не надо, достаточно открыть новостную ленту или вспомнить про растущие цены в магазинах. Не многих, но кого-то это мотивирует... к кражам баз данных. Громкие сливы последних месяцев — это только вершина айсберга, и, к сожалению, нужно быть готовыми к тому, что таких утечек корпоративных секретов станет много.

Очень много.

Что поделаешь... сегодня такое время — время крайностей и отсутствия компромиссов. Сейчас многие находятся под давлением и внутренних, и внешних причин одновременно, что может приводить к изменениям в поведении, мотивации, лояльности компании. Недаром говорят, что люди приходят в компанию (в бренд), а уходят от людей (коллег и руководителя). Тот, кто имел опыт разочарования в работодателе, прекрасно знает, насколько это трудный период и непростой выбор решения. Нельзя работать в компании и быть против неё. Это кратчайший путь к стрессам, болезням и многочисленным конфликтам, в том числе и с самим собой. Но сейчас не то время, когда стоит ожидать от людей взвешенных, а не эмоциональных поступков.

СИНДРОМ ОСТАПЧУКА

Говорят, что жизнь нужно прожить так, чтобы твоим именем назвали диагноз. Ещё свежа в памяти история февраля 2022 года, когда Тарас Остапчук пытался потопить яхту российского олигарха, которую холил и лелеял долгие годы. Это как пример политизированной мотивации и изменений в поведении внутренних сотрудников.

Они сами не всегда способны осознавать, к каким колоссальным последствиям могут приводить их действия. Коллеги из пражского офиса

Microsoft рассказывали, что через них проходила история одной европейской компании, в которой работал молодой сотрудник ИТ-департамента. Каждое утро он начинал с чтения статей на экстремистском ресурсе и выражал им свою поддержку, переводя раз в неделю символическую сумму (5–7 €). И делал это с завидной регулярностью с корпоративного аккаунта. Но «Белые хакеры» — так называемые борцы за справедливость — взломали рупор экстремизма и передали европейским спецслужбам базу зарегистрированных на ресурсе лиц. В разработку взяли две группы: тех, кто изредка отмывал через ресурс существенные денежные суммы, и тех, кто делал это помалу, но с завидной регулярностью. В итоге счета компании, где мирно работал наш герой, заблокированы, партнёры и контрагенты под подозрением в соучастии, в офисе хозяйничают офицеры спецслужб, а ключевые сотрудники в поисках новой компании обновляют резюме, особо отмечая графу «стрессоустойчивость».

Феерическая глупость с бюджетом 5 € в неделю, с одной стороны, и колоссальные финансовые и репутационные потери для бизнеса — с другой.

Не будет большим преувеличением сказать, что проявления признаков «синдрома Остапчука» сегодня могут найтись у многих...

ДОБРОВОЛЬНОЕ ИНСАЙДЕРСКОЕ РАБСТВО

Как понять рядовому сотруднику, что его гаджет инфицирован? С вероятностью 90% никак! Но для того, чтобы гаджет стал частью преступной бот-сети, его нужно взломать и заразить соответствующим ПО. Делают это не люди, а роботы, и, судя по запрашиваемым в сети ценам на аренду ботов для реализации DDoS-атаки, дела в этой сфере идут успешно.

Но сейчас стало ещё проще. Например, можно найти предложения добровольно стать киберпартизаном. То есть добровольно установить у себя на гаджете вредоносное ПО, которое сделает тебя участником бот-сети для совершения атак на вражеские ресурсы. Для тех, кто в этом сомневается, могу показать коммерческие предложения, когда за добровольную установку такого ПО владельцам гаджетов предлагают заплатить денег. Условия и суммы — самые разные.

Совершенно немыслимый выбор для трезво и критически мыслящего человека! Но время крайностей способно заглушить здравый смысл. Во-первых, нет никаких гарантий, что кибератака будет направлена именно на те ресурсы, на

которые ориентировался и «всё спланировал» наш «доброволец». А во-вторых, нет никаких гарантий, что владелец бот-сети не использует эту сеть для реализации любых криминальных сценариев по своему усмотрению, не ставя никого из добровольных участников в известность. Но ответственность, пусть даже только моральная, за причастность останется на тех, кто добровольно решил в этом участвовать!

ЧЁРНЫЙ СЛЕД

Коротка человеческая память. Например, мы с радостью стали забывать, как уходили на «удалёнку» в условиях пандемии. Это было не быстро, а мгновенно и принудительно. Никого не спрашивали о готовности и желании. Первыми были проданы ноуты и планшеты среднего ценового диапазона, а потом ушли с прилавков и премиум-модели. В тех условиях никому не удалось разместить корпоративный заказ на технику, чтобы создать комфортные условия для домашней работы сотрудников. Этот снимок (фото) был сделан в марте 2020 года на мокром московском асфальте. Даже секонд-хенд пользовался небывалым спросом. В другое время при покупке ноутбуков, бывших в употреблении, следовало отформатировать жёсткий диск и установить свои программы. Иногда для этого приглашали специалистов. Но в условиях пандемии никакой специалист, кроме доктора, на крик о помощи не отзывался. Поэтому все действовали одинаково: если ноут работает, то так и оставим, иначе дети не смогут утром подключиться к онлайн-урокам в школе, а вечером поработают родители.

Это значит, что уже тогда в домашних условиях была создана теневая ИТ-инфраструктура с сомнительным контролем за политикой безопасности, patch management и удалёнными обновлениями ПО. Именно тогда галопировал вектор атак на домашних пользователей и компрометацию их устройств. Известны эпизоды онлайн-заказов плотских утех на дом при регистрации с корпоративных аккаунтов. Расчёт злоумышленников был прост: рано или поздно эти гаджеты с инфицированным ПО окажутся в корпоративном периметре. О разнообразии криминальных сценариев можно только догадываться.

Но сейчас на унаследованные после пандемии риски, исходящие из сомнительной домашней ИТ-инфраструктуры, накладывается другая напасть — политически перегретая мотивация. И с этим надо как-то жить и управлять, а не игнорировать.



Фото. В период пандемии ноутбуки стали дефицитом. Объявление на асфальте, март 2020 г.

ЧТО-ТО НАДО С ЭТИМ ДЕЛАТЬ...

В одном из интервью Рори П. Рида, занимавшего тогда пост главного исполнительного директора и президента в подразделении Dell, отвечающего за мировые продажи, журналист спросил, использует ли компания DLP-функционал. «У нас нет DLP. Мы работаем с сотрудниками», — ответил Рори. С тех пор прошло уже немало лет, и мир заметно изменился. Мне кажется, если бы пришлось отвечать на подобный вопрос сегодня, то, возможно, к работе с сотрудниками добавился бы и DLP-функционал. И не только средства DLP. С тех пор отношение к ним заметно изменилось. В умелых руках сотрудников ИБ-подразделений это уже не средство поиска внутренних нарушителей, мониторинга или слежения за сотрудниками. Это тонкие и деликатные инструменты, которые не позволяют хорошему парню сделать глупость.

Это трудное дело — работать с сотрудниками, находящимися в состоянии напряжения. Это значит, что нужна тёплая и комфортная атмосфера для работы с коллегами. Именно с коллегами, а не с кадрами или сотрудниками! Сейчас очень важно сохранить команды, их коллективный дух. Иногда для этого поможет обновлённый взгляд на команду. Он позволяет выявить новые ценности коллег. Сейчас как никогда могут быть уместны выплаты премиальных бонусов за прошлый год. Мотивация — это не только про HR или ИБ. Это скорее про партнёрство ИБ с HR. Мы все должны выйти из этой ситуации обновлёнными, образованными, прокачанными... И стрессоустойчивыми.



**Алексей
ВОЙЛУКОВ**
вице-президент
Ассоциации банков
России

ВЫВЕСТИ ВСЕХ НА АУТСОРСИНГ!

ПОЧЕМУ СЛУЖБЫ ИТ И ИБ БАНКОВ ОСТАЛИСЬ БЕЗ ГОСПОДДЕРЖКИ?

В настоящее время кредитные организации испытывают значительную нагрузку на подразделения информационной безопасности (ИБ), связанную в том числе со значительным уровнем киберагрессии со стороны недружественных стран. По информации Банка России, количество кибератак в финансовом секторе с 24 февраля 2022 года выросло в 22 раза. Участники рынка сообщают об увеличении мощности DDoS-атак в 2–3 раза, некоторые из них непрерывно атакуют ресурсы на протяжении 12–14 часов с силой более 700 тысяч запросов в секунду.

НАГРУЗКА РАСТЕТ НА ФОНЕ ДЕФИЦИТА КАДРОВ

Нагрузка на службы ИБ увеличивается также в связи с уходом ряда вендоров с рынка Российской Федерации, прекращением действия технической поддержки и сервисов подписки, повышением стоимости средств защиты информации и аппаратных комплексов и форсированным импортозамещением. Всё это дестабилизирует работу по обеспечению информационной безопасности и требует дополнительных финансовых затрат и усилий.

Особую значимость приобретает вопрос дефицита ИТ-кадров в финансовом секторе. В настоящее время он увеличивается за счёт оттока специалистов в профильные ИТ-компании, в том числе зарубежные. Наличие установленных государством преференций в компаниях ИТ-сектора только усиливает этот переток, в том числе из кредитных организаций.

Все эти факторы требуют применения компенсационных и иных мер поддержки не только для служб ИБ кредитных организаций, но и для всего ИТ-направления банков в целом.

ГОСПОДДЕРЖКА ПРОХОДИТ МИМО БАНКОВ

Эффективными мерами поддержки ИТ-отрасли и ИТ-специалистов являются меры,

предусмотренные Указом № 83¹. Льготные кредиты для организаций по ставке не более 3%, двухлетние каникулы по налогу на прибыль, освобождение от государственного и муниципального надзора и контроля на срок до 3 лет оказали бы существенное положительное влияние на кредитные организации, инвестирующие значительные ресурсы в разработку ИТ-решений и цифровых сервисов. А бюджетное финансирование улучшения жилищных условий сотрудников и повышения их заработной платы вкупе с отсрочкой от призыва на военную службу смогло бы остановить или существенно замедлить отток ИТ-кадров из банковского сектора.

В настоящее время эти меры поддержки распространяются исключительно на ИТ-компании. В этой связи Ассоциация направила в Государственную думу Федерального собрания Российской Федерации и Правительство Российской Федерации инициативу о распространении мер, предусмотренных Указом № 83, на организации финансового сектора, осуществляющие деятельность в области информационных технологий².

Дополнительно в целях решения проблемы дефицита ИТ-специалистов Ассоциацией также предложены меры по поддержке сотрудников служб ИТ и ИБ кредитных организаций:

- ♦ освобождение от уплаты НДФЛ сроком на три года;
- ♦ выделение бюджетных средств на предоставление льготных потребительских кредитов;
- ♦ отмена НДФЛ с материальной выгоды по льготным кредитам.

¹ Указ Президента Российской Федерации от 02.03.2022 № 83 «О мерах по обеспечению ускоренного развития отрасли информационных технологий в Российской Федерации».

² В том числе деятельность по разработке, внедрению и доработке цифровых сервисов и продуктов, отечественного программного обеспечения, программно-аппаратных комплексов, созданию и поддержке инфраструктуры, занимающиеся экспертной поддержкой в сфере ИТ, в том числе с целью реализации политики импортозамещения (в части реализации ИТ-проектов).



ДЕЙСТВИЯ АБР, БАНКА РОССИИ И МИНЦИФРЫ

Банк России уже поддержал эту инициативу, Ассоциация продолжит её реализацию совместно с Минцифры России.

Минцифры России также предложило альтернативное и более оперативное решение, связанное с проведением кредитной организацией реорганизации и выделением отдельного юридического лица, осуществляющего деятельность в сфере ИТ, для получения им всех мер поддержки. Такой подход может быть реализован кредитными организациями после консультаций с Банком России и получения ими методологической помощи по выделению собственных служб ИТ и ИБ в отдельное юридическое лицо³ с последующим оказанием им соответствующих услуг банкам на основании аутсорсинга.

При этом и сам вопрос аутсорсинга ИТ и ИБ требует дополнительной проработки. В настоящее время в Государственной думе Федерального собрания Российской Федерации находится на рассмотрении проект Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации», регламентирующий вопросы использования услуг аутсорсинга ИТ и облачных услуг финансовыми организациями. В соответствии с этим

³ С присвоением им кода ОКВЭД, требуемого действующими государственными программами поддержки ИТ-отрасли.

законопроектом требования к порядку привлечения поставщиков услуг аутсорсинга, в том числе по защите информации и операционной надёжности, будут устанавливаться дополнительно актами Банка России.

Ассоциация деятельно участвует в обсуждении ИТ-аутсорсинга для кредитных организаций. Для этого создана специальная проектная группа с участием представителей банков, Банка России и вендоров программного обеспечения. Ассоциация рассчитывает, что такой комплексный подход позволит создать оптимальное решение для всех участников аутсорсинга ИТ-функционала.

Несмотря на значительный вклад банковского сектора в цифровизацию экономики и обеспечение кибербезопасности финансового пространства, в настоящее время не реализованы системные меры поддержки ИТ- и ИБ-направлений кредитных организаций. Учитывая, что именно на банках лежат функции обеспечения бесперебойности и безопасности предоставления финансовых услуг, защиты денежных средств населения и бизнеса, крайне важно принять все возможные меры для распространения инструментов государственной поддержки ИТ на кредитные организации.



Анатолий АКСАКОВ
депутат Государственной думы
РФ, председатель Совета
АБР, член Национального
финансового совета ЦБ



Тимур АИТОВ
эксперт BIS Journal, член Совета ТПП
РФ по финансово-промышленной
и инвестиционной политике, зампред
комиссии по цифровым финансовым
технологиям

СТРАТЕГИИ ПРОРЫВА

БАНКИ В УСЛОВИЯХ МЕЖДУНАРОДНЫХ САНКЦИЙ

Структура момента такова, что раздел «Регуляторь» в BIS Journal не может быть представлен прямыми высказываниями ни со стороны Госдумы РФ, ни со стороны Банка России. «Мы ещё не готовы... идёт рабочий процесс... формируется позиция, готовятся документы...» Тем не менее про Анатолия Аксакова нельзя сказать, что он таится от общественности. Публикуем его беседу с нашим экспертом Тимуром Аитовым¹.

Тимур Аитов. Тема нашей беседы — банки в условиях международных санкций, стратегии прорыва. Первый вопрос: как нам совершить этот самый прорыв? Наши банки подверглись беспрецедентным санкциям, но выстояли, ситуация всё-таки под контролем. И что же? Наши разработчики по-прежнему говорят: «Нам ещё надо немного доделать, чтобы получились аналоги западного ПО...» Министры говорят: «Дайте нам ещё 2–3 года, и мы проблемы с импортозамещением решим окончательно». А кто-то под сурдинку советует: «Может, нам перейти от импортозамещения к импортоопережению?» То есть всё достаточно сумбурно. Как к этому относиться, можно ли достичь прорыва, есть ли у вас собственный рецепт?

Анатолий Аксаков. Прежде всего надо помнить, что Россия входит в пятёрку ведущих стран по цифровизации финансовых процессов. К сожалению, это опережение опиралось в основном не на наши разработки, хотя и наши тоже активно внедрялись, особенно крупнейшими банками. Тем не менее в 2018 году был принят закон, который ориентировал не только финансовую сферу, но и всю экономику на переход на отечественные программные продукты и «железо», чтобы сделать нашу ИТ-сферу максимально независимой от американских систем.

— Тема импортозамещения и раньше звучала...

— В 2014 году её подняли, в 2018 году был принят закон с довольно жёсткими сроками — первой отсечкой установили 2021 год. Но под напором обстоятельств и наших компаний, не верящих в санкции, срок передвинули сначала на 2023 год, потом на 2024, а сегодня оказалось, что всё это надо было делать вчера.

Конечно, конкурировать с крупнейшими ИТ-компаниями, например американскими, мы вряд ли сможем, даже с китайской Huawei, но при этом мы имеем большой задел в виде молодых людей, которые учились в наших вузах, часто уезжали за границу, способствовали там продвижению западных компаний и довольно неплохо зарабатывали. Некоторые из них вернулись с богатым опытом и оригинальными идеями и готовы помочь родной стране в продвижении технологий. И такой задел людского потенциала большой.

ДВА ПУТИ

Мы можем пойти двумя путями. Первый — ориентироваться на новые формы развития ИТ-технологий в стране: небольшими группами. Не всегда величина структуры определяет качество работы, которая в ней осуществляется. Сейчас будет тренд на создание малых групп до 100 человек, пусть даже до 1000, но ориентированных на прорывные, генерирующие идеи, причём идеи, способные обесценить всё то, что есть сегодня у ведущих компаний мира.

Такие группы будут поддерживаться государством, финансироваться, по крайней мере, на начальных этапах. Но не всё должно финансироваться, быть бесплатным, люди должны создать ситуацию максимальной конкуренции, и не только внутри страны, между собой, но и с внешним миром. Вот для таких групп мы будем создавать условия — льготы, стимулы, которые помогут этим мозгам проснуться и работать как в своё удовольствие, так и на пользу стране.

Второе направление — это концентрация ресурсов на проекты, решающие очень масштабные, узловые задачи, в том числе и в сфере ИТ-технологий. У нас есть такой опыт. Например, реализация плана ГОЭЛРО, который в своё время дал мощный толчок к развитию СССР, атомный проект, когда нам было необходимо срочно создать свою атомную бомбу, чтобы противостоять

¹ Беседа Тимура Аитова и Анатолия Аксакова в полном объёме по ссылке <https://mediametrics.ru/articles/view.html?id=69705>.

американскому диктату. Такой опыт, безусловно, надо использовать, и мы будем это делать.

ОРГАН ТИПА ГОСПЛАНА

— Но кто будет ставить чёткие цели, формулировать текущие задачи? Похоже, нам нужен орган типа Госплана, можно назвать его центром стратегического планирования. Вы сказали, что чиновники постоянно переносят сроки. Да, действительно, министерства составляют список компаний, которые должны пройти импортозамещение к 2022 году, потом меняют дату на 2024 год, а что эти компании связывает между собой — проекты, материальные возможности, интеллектуальный потенциал — это, похоже, никого не волнует. Госплан в своё время взаимоувязывал между собой десятки тысяч разных составляющих, поэтому масштабные проекты, целые отрасли и работали как часы, а сегодня такого обстоятельного планирующего органа нет.

— У нас есть Министерство экономического развития.

— Простой пример. Минпромторг выпустил наш отечественный процессор «Эльбрус», но под него нет прикладного ПО. Кто это пропустил? Почему так получилось?

— У нас экономика не настолько большая и сложная, чтобы ею так управлять. Сейчас есть искусственный интеллект, мощные компьютеры, которые позволяют проанализировать данные, тенденции и, исходя из анализа ситуации, могут выработать предложения для стратегического развития.

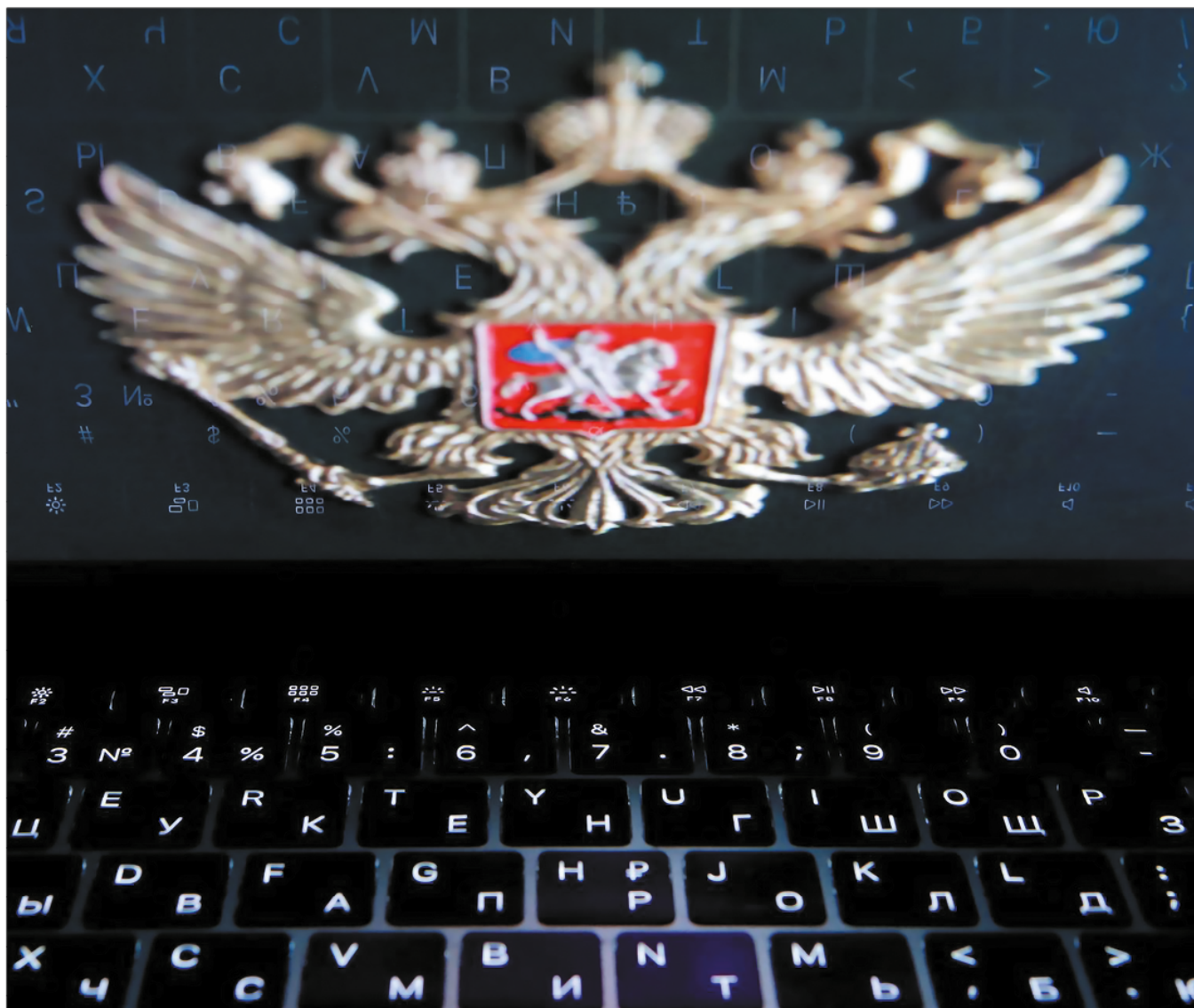
— Но кто-то должен делать выбор, принимать или не принимать эти предложения, корректировать их, доводить до рабочего состояния. Кто?

— Безусловно, должен быть центр принятия таких решений, на мой взгляд, центр стратегического развития. Но не тот, что был разработан теоретически, а именно Центр стратегического развития страны, определяющий направление движения экономики, концентрирующий научные и практические умы, чтобы они вырабатывали план реализации этих наработок, используя искусственный интеллект, международный опыт... Такой центр нам нужен, причём он должен быть не общественным, а государственным, его решения должны утверждаться Президентом или Госдумой. А дальше это уже закон, и его надо выполнять в безусловном порядке.



КНУТ И ПРЯНИК

— Наши разработчики сегодня жалуются, мол, банки мало берут российского ПО, как заставить их брать? А заказчики говорят: «Вы не то нам сделали, нам нужен вертикально интегрированный софт, когда стена, а вы нам какие-то кусочки предлагаете». То есть одним нравится, другим не нравится... Как в такой ситуации поступить, с чего начать — финансировать разработчиков, чтобы они делали то, что нужно, или заказчиков, чтобы они создавали спрос? Или просто заставлять покупать российское, как сегодня и происходит? Если вспомнить Китай, то они сначала создали инфраструктуру, которая поддерживает активность компаний, в том числе IT- и банков, а потом уже заставили переходить на китайское. Как нам



сегодня поступать, чтобы было правильно, кого финансировать — покупателей или производителей?

— Кнут и пряник — самая эффективная пара. Должен быть пряник в виде покупателя, у которого есть деньги и который приобретает эти услуги и технологии.

— И кнут в виде закона?

— А он есть. Мы приняли закон в 2018 году, установили отсечку 2021 год для внедрения российского ПО. Я сам собирал банкиров, Минцифры, силовиков — всех заинтересованных и проводил дискуссию: почему закон не выполняется? Банки оправдывались, что нет у нас такого ПО и сроки нереальные, а на самом деле сами не профинансировали эту работу вовремя и в нужном объеме, поэтому мы и не можем реализовать задачи, поставленные в законе.

Срок передвинули на два года. Банки готовы покупать отечественное. Пряник для производителя появился. И кнут в виде закона есть. Я с айтишниками встречаюсь в неделю по несколько раз, они идут и идут с интересными идеями, понятно, не все идеи реализуемы, но сам факт того, что их

очень много — и по управлению логистикой, и по организации контроля за движением всех наших товаров, и как организовать расчёты, в том числе без SWIFT... Это свидетельствует, что потенциал есть, и он уже пробивает себе дорожку, потому что кнут и пряник сошлись в интересах.

ПРО МАЛЫЕ БАНКИ

— В стране много малых банков. Чего им ждать в будущем, на что надеяться, как проводить импортозамещение? Денег у них нет, в долги влезать — прямая дорога к разорению, государство тоже вряд ли поможет... А может, пришло время создать централизованную инфраструктуру, которой они будут пользоваться? ЦБ уже что-то подобное делает, например, НСПК с картой «Мир», сервис быстрых платежей, «Семафор» запустил, КУС — знай своего клиента. Как дальше поступать с малыми банками, если они нужны стране? Кстати, нужны ли?

— Сколько их должно быть, определяет рынок. С моей точки зрения, они вполне могут оказывать услуги, закрывая

ниши, где крупным банкам неинтересно работать. У нас же есть микрофинансовые организации — они работают без банковской лицензии и не умирают, несмотря на все сложности с фондированием, функционируют себе и даже процветают.

Так и малые банки должны найти свою нишу. Но уверен, они не могут выпасть из общего процесса цифровизации. Да, для этого у них не хватает денег, и тут я согласен, ЦБ должен создавать инфраструктуру, которая позволит и поможет им закрывать ниши, где крупному бизнесу неинтересно работать.

Мы приняли закон 211-ФЗ о маркетплейсе, многие банки являются его участниками. Сейчас мы внесли в Госдуму законопроект, предусматривающий, что маркетплейсами могут пользоваться не только физические лица, но и предприниматели, то есть это такая платформа, через которую вы видите перечень услуг, оказываемых в том числе малыми и средними банками. И если вам кажется, что тут услуги более дешёвые и предпочтительные, то почему бы не воспользоваться этим маркетплейсом? Крупные банки туда не идут, у них другие каналы распространения информации. Так что такая инфраструктура уже создана, в том числе по инициативе ЦБ.

— Крупным банкам такие инициативы не очень-то нравятся. Тот же сервис быстрых платежей... Помните, один крупный банк, который мы называем зелёным, долго игнорировал предложение вступить в эту систему.

— Мы приняли закон, по которому все обязаны работать в этой системе.

— Он заплатил несколько штрафов и только потом вступил...

— Система быстрых платежей уже предусматривает использование не только физическими лицами, но и малыми предприятиями. Но такой процесс со стороны ЦБ, на мой взгляд, должен быть более интенсивным с учётом нынешней ситуации.

ЗАМЕНА ПО

— Есть острый вопрос, который банкиры активно обсуждают в кулуарах: про замену ПО. Они говорят: дорого. А если заставят менять и, соответственно, все резко начнут менять, появятся риски потери непрерывности бизнеса, и эти риски могут быть выше, чем риски санкционных отключений. И что происходит? Сегодня у всех банков программные продукты куплены много лет назад, а ключи на эти продукты закуплены на много лет вперёд, и практически все научились обходить ограничения по обновлениям — когда техподдержка пропадает, получают обновления через третьи руки. Что этим банкирам сказать: не торопиться или торопиться, не откладывать замену ПО? Напомню, что даже наш ЦБ использует западное программное обеспечение, у него Oracle стоит как катастрофоустойчивый кластер, и, по моим данным, пока не собираются его менять. Как быть с заменой ПО?

— Мы значительно облегчили и смягчили законодательство, чтобы зарубежная продукция могла замещаться

комплектующими, ремонтироваться, поддерживаться за счёт параллельного импорта. Если такая схема поможет сохранить действующее ПО, почему бы и нет.

Мы приняли решение, что ПО можно использовать до срока окончания его лицензии, а дальше заменять новым, опирающимся на отечественные разработки. Мы понимаем сложность ситуации, и никто не собирается брать вас за горло и душить. Но при этом генеральная линия, установка на переход на отечественное ПО остаётся, и если кто-то думает, что можно с помощью отговорок от этого уйти, то он ошибается.

ВТБ уже полностью перешёл на отечественное ПО, и многие другие банки начали этот процесс. Не так быстро, как хотелось бы, но жизнь заставляет, и вот увидите, у нас появится много своего интересного. ИТ по ментальности ближе к азиатским странам, а мы, хоть и не азиаты, но с раскосыми глазами...

ПРО ИСЛАМСКИЙ БАНКИНГ

— Хороший повод для вопроса про исламский банкинг. Было время, вы эту тему активно поддерживали, а сейчас, похоже, интерес к ней пропадает, хотя, казалось бы, в условиях санкционных ограничений — это шанс, новые возможности, крупные клиенты, выход на новые рынки?

— Тема давно дискутируется, но без особого движения, видимо, из-за религиозного контекста, решили не смешивать религию и финансы. А не так давно меня пригласил на празднование Курбан-байрам один из руководителей нашего мусульманского сообщества Альбир хазрат, он сам из Чувашии, мы с ним давно дружим. И вот на праздничном деловом ужине мы и обсуждали возможности возрождения дискуссии о реализации исламских финансов у нас в стране.

Я пригласил специалистов, устроил видеоконференцию, там были и работники Минфина, Центрального банка, другие люди, близкие к госвласти и компетентные по этому вопросу. Тема реанимировалась, расширилась, особенно с учётом интереса со стороны арабских, азиатских стран. Мы создали рабочую группу, она узкая, не хотим балагана и политизации, чисто деловой разговор, нужно конкретно сформулировать, что мешает альтернативным, в том числе и исламским, финансам работать в России. Планируем оформить предложения и представить их в виде правовой инициативы в Госдуму.

По крайней мере то, что я услышал на встрече, звучало разумно, там ничего противоречащего нашему финансовому законодательству нет, просто некоторые моменты необходимо отрегулировать, откорректировать. По моему замыслу это должно разместиться в отдельном разделе «Альтернативные финансы», и все, кто захочет в этой сфере работать, будут читать закон и принимать решение.

О КРИПТОВАЛЮТАХ

— Многие просили задать вам вопрос о криптовалютах. Почему ЦБ так негативно к ним относится? К тем же стейблкоинам, цена которых привязана к биржевому товару, понятна и прозрачна. С другой стороны, настороженность ЦБ понять можно. Например, в Венесуэле вы-

пустили El Petro, стейблкоин, и он первое время очень хорошо шёл, 4 млрд долларов они собрали, а сейчас подпали под санкции, американцы дотянулись до всех криптобирж, и цена El Petro упала ниже нижнего предела. Сможет ли криптовалюта быть тем инструментом, который поможет нам преодолевать санкционные ограничения, достаточно ли объёма для такой большой страны и что ждёт нас в этом отношении, какие законы будут приниматься?

— Текущая ситуация на крипторынке говорит о том, что ЦБ скорее прав, поскольку рынок обрушился, в том числе просел и Bitcoin, и если бы мы легализовали криптовалюты законодательно, то число россиян, вложивших в них свои деньги, было бы намного больше — десятки миллионов, тем более что в последние годы Bitcoin всё время рос. Поэтому правильно сделали, что не легализовали, но в то же время мы обязаны принять закон, который регулирует этот рынок.

Я бы сконцентрировался на активах. Мы приняли закон о цифровых финансовых активах, и они выпускаются по благословению Центрального банка. Три платформы, способные выпускать такие активы, уже зарегистрированы: Норильского никеля, Трансмашхолдинга и Сбербанка. На подходе ещё два банка со своими платформами.

Мы создали очень узкую рабочую группу (там ЦБ, Минфин, те, кто уже зарегистрировал платформы, те, кто собирается, и другие профессионалы), потому что вокруг таких новых вещей столько болтунов, политиков, шушеры всякой болтается, которая не только фон создаёт, но и большие проблемы. Всё, что уже наработали, мы оформили в законопроект и вынесли на обсуждение, например, налогообложение таких активов у нас будет принято в ближайшее время, оно будет похоже на налогообложение работы с ценными бумагами, там всё достаточно похоже.

Что касается криптовалют, здесь всё сложнее, я вообще сторонник легализации этого процесса, но под очень жёстким регулированием. Должна быть одна биржа или один институт, который покупает, продаёт, осуществляет все операции, обеспечивает выпуск кошельков, на которых хранятся криптовалюты, и очень жёсткое регулирование по вхождению в этот рынок: тестирование, квалификация понимания, что такое криптовалюта, риски, связанные с её оборотом.

Говорят, что стейблкоины привязаны к конкретному продукту, на самом деле привязка очень относительная. Например, платформа Норильского никеля позволяет выпускать активы, обеспеченные добываемой платиной, превращаемой в слитки, и тут вопросов нет, материальное обеспечение этих активов очевидно. А когда компания говорит, что у неё обеспечением является такой-то биржевой актив, зачем мне покупать эту бумажку, если гарантий того, что там есть реальное обеспечение, никаких? Это же частная валюта.

— Я имел в виду, что ЦБ будет её эмитировать.

— В нашем правовом пространстве, которое мы сейчас формируем, это цифровые финансовые активы, ЦБ это делает.

— ЦБ собирается эмитировать цифровой рубль, это тоже похоже на криптовалюту, просто стейблкоин будет ценой в 1 рубль.

— Да, это похоже на криптовалюту, но реально её объём и движение будет полностью регулироваться Центральным банком, он будет обеспечивать стабильность цифрового рубля, его равноценность наличным и безналичным деньгам, находящимся в банках. Цифровой рубль сейчас находится в разработке, в его тестирование вовлечены 12 банков, в конце года они должны подготовить прототип цифрового рубля, который будет запущен в оборот в 2023 году. По крайней мере, по планам Центрального банка. Мы в этом направлении активно, уверенно работаем и, мне кажется, абсолютно правильно действуем. И последняя ситуация на рынках, когда биржи, работавшие у нас, начали уходить, подтвердила правоту ЦБ, что крипторынок находится под значительным — не всеобщим, конечно, — контролем американских спецслужб, и если захотят, они прикроют этот рынок одним махом.

— Они и начали это делать, вводя ограничения в отношении счетов россиян...

— Да, некоторые уже не могут работать со своими криптовалютами из-за санкций. В таком контексте декларации о том, что распределённая система частных денег независима от влияния, не подтверждаются фактами.

— Так помогут ли нам криптовалюты бороться с санкциями или это пустой звук, ведь масштаб криптоинструментов не такой большой, если смотреть по капитализации?

— Три триллиона долларов.

— Bitcoin — меньше триллиона, Ethereum — половина Bitcoin, остальные ещё меньше.

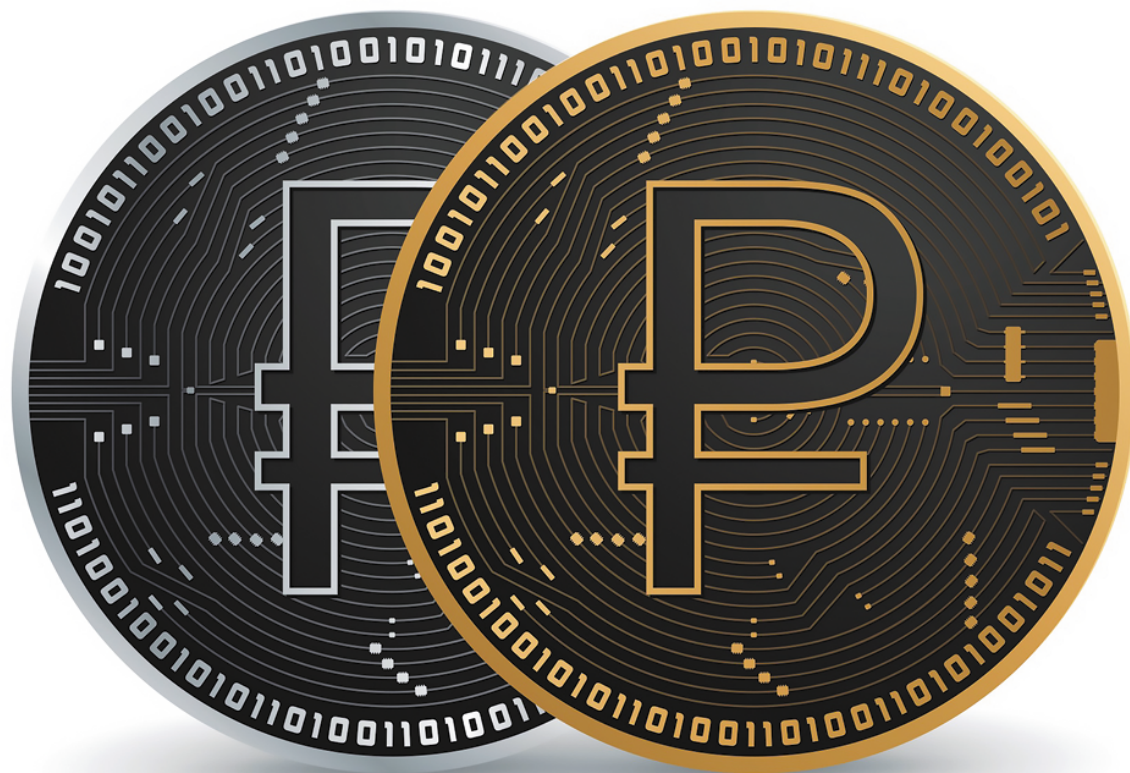
— Если честно, мне давно некоторые компетентные люди говорили о том, что и Bitcoin, и другие находятся под контролем известных зарубежных спецслужб. Если они и не запустили их изначально, то, по крайней мере, активно контактировали с некоторыми разработчиками.

КУРС ДОЛЛАРА

— Раз уж мы про деньги начали говорить, давайте обсудим курс доллара и рубля. Каким должен быть этот курс, что его определяет сегодня?

— О том, как будут развиваться валютные процессы, пока не готов делать серьёзных заявлений. Понятно, что нам необходимо определиться со своими партнёрами, прежде всего с теми, кто не хочет зависеть от решений американского Госдепа или европейского центрального банка, очень сильно подверженного влиянию политических решений. Нет гарантий, что эти политические решения не будут применены к Китаю, Индии или любой другой стране.

Поэтому будет вырабатываться общая валютная политика. Создана рабочая группа во главе с М. С. Орешкиным, помощником Президента РФ, в неё вошли серьёзные люди, включая председателя Банка России, и эта группа должна выработать предложения. Плюс будут более активно вестись межгосударственные контакты с Китаем, Индией, Бразилией, Южной Африкой в рамках БРИКС, чтобы выработать подходы к



использованию национальной валюты, которая обеспечит взаиморасчёты между этими странами, а дальше она может пойти и по более широкому использованию. В СССР был переводной рубль, здесь, возможно, появится валюта БРИКС. Причём, если Индия, Китай, Россия, Бразилия и ЮАР договорятся, это будет очень серьёзная альтернатива доллару и евро, по сути, удар по ним. Так что поживём — увидим.

При этом могу сказать, что в Евразийском союзе, куда входят азиатские страны, мы в большей мере будем переходить на рубль и на расчёты в национальных валютах. С Китаем сейчас резко начал расти оборот в рублях, вижу последние сообщения, что и немцы, и ряд других стран начали платить рублями за газ, это говорит о том, что рубль становится в определённом смысле международной валютой.

— Будем надеяться, что процесс в этом направлении будет только развиваться.

— Индия, Китай — это самодостаточные страны. Благодаря сложившейся ситуации в мире они получают дополнительный толчок к укреплению своих геополитических позиций. Мы и раньше уделяли этому внимание, но не активно, а теперь будем им помогать, потому что мы в этом заинтересованы, мы уже в тиски зажаты и должны находить варианты более глубокого сотрудничества с этими странами, в том числе и технологического сотрудничества.

— Вы имеете в виду какую-то общую цифровую валюту?

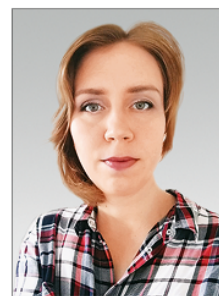
— Есть цифровой юань, сейчас появится цифровой рубль, насчёт рупий пока не готов говорить, но там тоже хорошие айтишники, поэтому допускаю, что и цифровая рупия появится, а с ней и совместные предприятия базового производства — станки, оборудование — либо на территории Индии, либо на нашей с участием индийских работников... У нас рабочей силы всё равно меньше. Так что интеграция с Азией пойдёт намного быстрее.

Я обратил внимание, что наш товарооборот с Китаем с февраля на март вырос на 40 процентов — это при всех разговорах о том, что китайцы не очень-то нам помогают. Они же предприимчивые люди, и их и наш малый бизнес быстро переориентировались и начали наращивать взаимооборот в очень больших объёмах. Уверен, что и Европа развернётся в нашу сторону. Просто иногда меня удивляют действия их политиков. Бить своими решениями по своему же народу — этого Европа, конечно, долго терпеть не будет. Сегодня она работает по команде из-за океана, но так не может быть всё время.

— Спасибо за интересную беседу, за ваши мнения, мысли и важную информацию. От души желаю вам успеха, здоровья, благополучия, и так держать!

КРИТИЧНАЯ НЕ РАВНО КРИТИЧЕСКАЯ

О НОВЫХ ТРЕБОВАНИЯХ БАНКА РОССИИ К ОПЕРАЦИОННОЙ НАДЁЖНОСТИ



**Алена
ИГНАТЬЕВА**
эксперт BIS Journal

В конце апреля Банк России опубликовал два новых положения, описывающих требования к операционной надёжности в целях обеспечения непрерывности банковских услуг для кредитных организаций — 787-П от 12.01.2022 и финансовых — для некредитных финансовых организаций — 779-П от 15.11.2021. Под действие норм попали кредитные и небанковские кредитные организации, НПФ, страховые и брокерские компании, депозитарии, финмаркеты, биржи. Оба документа начинают действовать с 1 октября 2022 года.

В СТОРОНУ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА

Указанные положения тесно взаимосвязаны с 683-П и 757-П в части определения защищаемой информации и технологических участков технологических процессов и с 716-П — в части технологических процессов и требований к управлению риском.

Пока неисполнение указанных положений никаких страшных последствий для финансовых организаций не несёт, разве что в ходе надзора может быть выписано предупреждение. Однако если проанализировать ряд последних законодательных инициатив ЦБ, то можно заметить, что рынок планомерно движется в сторону риск-ориентированного подхода.

Наиболее вероятен сценарий, при котором в перспективе двух-трёх лет для всех финансовых организаций будет введён риск-профиль, содержащий в себе оценки аудиторов и ЦБ, показатель доли несанкционированных переводов, жалоб клиентов и информацию о компании в СМИ. На его основе будут формироваться требования к размеру резервов, которые организация должна сформировать. Чем выше риск-аппетит, тем их объём будет больше. В этом случае невыполнение требований к операционной надёжности может послужить одной из причин для увеличения размера резервов.

НОВОЕ ОПРЕДЕЛЕНИЕ — КРИТИЧНАЯ АРХИТЕКТУРА

Положения 787-П и 779-П вводят новое определение — критичная архитектура (не путать с критической информационной инфраструктурой в терминах 187-ФЗ «О безопасности критической информационной инфраструктуры»), элементы которой должны учитываться и контролироваться финансовой организацией.

И если для критической информационной инфраструктуры достаточно учитывать ПО, оборудование, линии связи и базы данных, то в рамках критичной архитектуры необходимо иметь детальное описание технологических процессов и технологических процессов входящих в них технологических участков. Формулировка получается запутанная, легче объяснить её на примере. В приложении к 787-П есть одиннадцатый технологический процесс — дистанционное банковское обслуживание. Одним из технологических участков этого процесса является учёт совершённых операций. Учёт операции, в свою очередь, тоже состоит из процессов, которые организация должна описать (в какие формы, заносится та или иная информация, куда дублируется, какие контроли проходит и т.д.).

Кроме этого, нужно контролировать людей, не только сотрудников, непосредственно обеспечивающих защиту информации, но и других участников этого процесса, в том числе подрядчиков. И если с уборщицей тётей Машей всё просто: достаточно не пускать её одну в серверную и не разрешать вносить туда ведро с водой, то контроль подрядчиков, имеющих логический доступ к инфраструктуре, часто выполняется формально. Ярким примером такого подхода является взаимодействие со сторонними разработчиками. Контроль кода и ограничение доступа, как правило, выполняют только крупные компании, в то время как в небольшом бизнесе разработчики зачастую получают постоянный, практически бесконтрольный доступ в рабочий контур. Что они там делают, проверяет в лучшем случае система DLP, которая есть только у небольшого процента организаций. Про поставщиков SMS/PUSH-сервисов обычно тоже не задумываются, несмотря на то что те имеют прямой доступ к информации, содержащейся в уведомлениях (информация об операциях, остатке на счёте, одноразовые пароли и т.п.) и контактными данными клиентов.

Схематично критичную архитектуру можно изобразить следующим образом (рисунок 1).

Состав объектов информационной инфраструктуры определён в национальном стандарте ГОСТ Р 57580.1–2017 и включает:

- ♦ аппаратное обеспечение;
- ♦ сетевое оборудование;
- ♦ сетевые приложения и сервисы;
- ♦ серверные компоненты виртуализации, программные инфраструктурные сервисы;

КРИТИЧНАЯ АРХИТЕКТУРА 787-П, 779-П								
Технологические процессы (ТП)								
Люди	Объекты информационной инфраструктуры	Участники	Каналы связи	Технологические участки (ТУ)				
				ТУ1	ТУ2	ТУ3	ТУ4	ТУ5
				ТП1ТУ1... ТПНТУ1	ТП1ТУ2... ТПНТУ2	ТП1ТУ3... ТПНТУ3	ТП1ТУ4... ТПНТУ4	ТП1ТУ5... ТПНТУ5

Рисунок 1. Схематичное изображение критичной архитектуры

♦ операционные системы, СУБД, серверы приложений;
♦ АС и приложения, реализующие технологический процесс.

Об участниках технологических процессов я уже упоминала выше — это вовлечённые в процесс иные кредитные и некредитные финансовые организации, а также поставщики услуг (провайдеры, хостеры, поставщики услуг технической поддержки, операторы услуг информационного обмена и т.п.).

В область действия положений 787-П и 779-П попадают только каналы связи, по которым осуществляется передача защищаемой информации (сведений, содержащихся в распоряжениях, персональных данных, информации, необходимой для авторизации клиентов и удостоверения их прав, ключевой информации, информации о совершённых операциях). К ним можно отнести каналы связи между сервисами организации и клиентами, кредитной организацией и банками-корреспондентами, Банком России (в рамках его платёжной системы), операторами платёжных систем, удостоверяющим центром, предоставляющим ключи для аутентификации. А вот канал связи, который используется организацией для направления сведений в ФОИВ (например, сведения о работниках в ПФР или сдачи отчётности в налоговую), под действие положений не попадает.

Технологических участков для каждого процесса всего пять:

- ♦ идентификация и аутентификация клиентов;
- ♦ подготовка, приём и передача электронных сообщений;
- ♦ удостоверение права клиентов распоряжаться денежными средствами либо активами;
- ♦ осуществление операции и её учёт;
- ♦ хранение электронных сообщений и информации об осуществлённых операциях.

НАБОР ДОКУМЕНТОВ

Отмечу, что для каждого технологического процесса требуется не только детальное описание, но и целый набор документов, часть из которых хоть и не заявлены в положениях, но явно вытекают из требований:

- ♦ документ, определяющий целевые показатели операционной надёжности;
- ♦ документ, определяющий методику фиксации, контроля и анализа показателей деградации технологических процессов;

- ♦ порядок учёта и контроля критичной архитектуры;
- ♦ порядок управления критичной архитектурой на всех стадиях жизненного цикла;
- ♦ политика управления рисками информационной безопасности и информационных систем, в том числе при взаимодействии с поставщиками услуг;
- ♦ методика сценарного анализа в части возможной реализации информационных угроз;
- ♦ документы, описывающие организационные и технические меры в отношении работников и подрядчиков, связанные с возможностью злоупотребления предоставленными полномочиями доступа;
- ♦ правила взаимодействия с участниками технологических процессов в части актуализации информации об информационных угрозах;
- ♦ документы, содержащие описание мер, направленных на реализацию требований к операционной надёжности;
- ♦ модель угроз в отношении критичной архитектуры.

ДО 1 ОКТЯБРЯ

Таким образом, чтобы полноценно выполнять требования положений 787-П и 779-П, до 1 октября финансовым организациям необходимо:

- ♦ провести инвентаризацию и актуализацию технологических процессов, возможно, скорректировать существующие процедуры учёта и контроля активов;
- ♦ разработать/актуализировать большой объём внутренних нормативных документов, часть требований к которым являются новыми даже для кредитных организаций, которые уже привели свою деятельность в соответствие положению 716-П;
- ♦ назначить ответственных лиц для организации процесса управления риском операционной надёжности, с учётом возможного конфликта интересов;
- ♦ выстроить процессы в соответствии с принятыми документами.

Учитывая приближающийся сезон отпусков, необходимость вовлечения в эти задачи работников практически всех подразделений, а также непростую процедуру согласований в финансовых организациях, лучше не откладывать эти работы в долгий ящик.



Александр ВИНОГРАДОВ
специалист службы ИБ
КБ «Максима»



Анастасия НИКОЛАЕВА
ведущий консультант по ИБ
AKTIV CONSULTING



Дмитрий ЛЕВИЕВ
председатель Совета
НП «ПСИБ»

«ВЫПОЛНИТЬ НЕ ПРЕДСТАВЛЯЕТСЯ ВОЗМОЖНЫМ»

ОБОСТРЕНИЕ МЕЖДУ БУМАЖНОЙ И РЕАЛЬНОЙ ИБ

В конце первого квартала 2022 г. обеспечение информационной безопасности в организациях Российской Федерации перешло на усиленный режим работы, а вопросы реальной информационной безопасности вышли на первый план. Большое количество сетевых атак, отсутствие технической поддержки от значительного числа зарубежных производителей программного обеспечения и программно-аппаратных решений привели к резкому росту числа уязвимых автоматизированных информационных систем, в том числе в кредитно-финансовой сфере. С этого момента Планы на обеспечение непрерывности деятельности и (или) восстановления деятельности в случае возникновения нестандартных и чрезвычайных ситуаций стали реальны.

ТЕКУЩАЯ СИТУАЦИЯ

Кредитно-финансовая сфера является самой зарегулированной в области информационной безопасности, и огромное количество нормативной базы по обеспечению информационной безопасности имеет статус находящихся на исполнении, которое в настоящее время выполнить невозможно.

Вопросы модернизации существующей инфраструктуры в настоящий момент требуют полного пересмотра как поставщиков новых решений, так и поставщиков решения к существующей инфраструктуре (параллельный импорт).

Оценка выполнимости требований сопровождения текущих решений рассматривается далее с учётом наличия параллельного импорта.

ИСХОДНАЯ ПОЗИЦИЯ

Как известно, 04.06.2020 Банк России утвердил Положение № 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».

Через год, 20.04.2021, данным регулятором было утверждено Положение № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций».

Напомним, что в указанных Положениях устанавливаются требования к уровню соответствия с ГОСТ Р 57580.2–2018 не ниже четвёртого в 719-П:

- ♦ пункт 2.4. для операторов по переводу денежных средств;
- ♦ пункт 3.7. для банковских платёжных агентов, осуществляющих операции платёжного агрегатора;
- ♦ пункт 4.5. для операторов услуг информационного обмена;
- ♦ пункт 6.8. для операторов услуг платёжной инфраструктуры;

и не ниже третьего в 757-П:

- ♦ пункт 1.7. для некредитных финансовых организаций, реализующих усиленный и стандартный уровни защиты информации;

Таким образом, некредитным финансовым организациям, операторам по переводу денежных средств, банковским платёжным агентам (субагентам), операторам услуг информационного обмена, операторам услуг платёжной инфраструктуры следует реализовать требования к обеспечению защиты информации при осуществлении переводов денежных средств и/или деятельности в сфере финансового рынка, применяемых в отношении автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, и реализовать уровень защиты информации согласно требованиям ГОСТ Р 57580.1–2017 путём внедрения технических средств защиты и разработки организационно-распорядительной документации.

Однако в связи с санкциями и прекращением деятельности в России зарубежных компаний-поставщиков программного

и аппаратно-программного обеспечения реализация мер, указанных выше, а именно выполнение требований к уровню соответствия с ГОСТ Р 57580.1–2017, становится невозможным.

Ситуацию усложняет тот факт, что список покидающих российский рынок компаний постоянно меняется. Этот процесс может затрагивать не только коммерческие, но и open-source-решения.

Согласно ГОСТ Р 57580.1–2017 в организации должно быть введено в эксплуатацию следующее программное и аппаратно-программное обеспечение, а также обеспечена регламентация его настроек, проведение контрольных мероприятий.

Процесс 1. Обеспечение защиты информации при управлении доступом. Внедрение системы, реализующей централизованное управление правами доступа и учётными записями пользователей в различных информационных системах (IDM). Технические меры: УЗП.9, УЗП.18. Организационные меры: УЗП.2, УЗП.3, УЗП.4, УЗП.12.

Процесс 2. Обеспечение защиты вычислительных сетей. Внедрение аппаратно-программного межсетевого экрана с функцией IDS и IPS. Технические меры: СМЭ.1, СМЭ.3, СМЭ.6, СМЭ.7, СМЭ.14, СМЭ.16, СМЭ.17, СМЭ.18, СМЭ.19, СМЭ.20, ВСА.2, ВСА.4, ВСА.5, ВСА.8, ВСА.9, ВСА.10. Организационные меры: КЗИ.1, КЗИ.2, КЗИ.3.

Процесс 3. Контроль целостности и защищённости информационной инфраструктуры. Внедрение программного обеспечения, служащего для осуществления диагностики и мониторинга сетевых объектов информационной инфраструктуры, позволяющего сканировать сети, компьютеры и приложения на предмет обнаружения возможных уязвимостей в системе безопасности, оценивать и устранять уязвимости (сканер уязвимости). Технические меры: ЦЗИ.1, ЦЗИ.2, ЦЗИ.3, ЦЗИ.4, ЦЗИ.5, ЦЗИ.6, ЦЗИ.7, ЦЗИ.8, ЦЗИ.9, ЦЗИ.10, ЦЗИ.15, ЦЗИ.20, ЦЗИ.21, ЦЗИ.23, ЦЗИ.27, ЦЗИ.28, ЦЗИ.29, ЦЗИ.32, ЦЗИ.33, ЦЗИ.35, КЗИ.6. Организационные меры: ЦЗИ.12, ЦЗИ.13, ЦЗИ.14, ЦЗИ.18, ЦЗИ.19, ЦЗИ.22, РЗИ.3, КЗИ.1, КЗИ.2, КЗИ.3.

Процесс 4. Защита от вредоносного кода. Внедрение эшелонированных средств защиты от ВВК. Технические меры: ЗВК.1, ЗВК.2, ЗВК.3, ЗВК.4, ЗВК.5, ЗВК.6, ЗВК.7, ЗВК.8, ЗВК.9, ЗВК.10, ЗВК.11, ЗВК.12, ЗВК.13, ЗВК.14, ЗВК.15, ЗВК.16, ЗВК.17, ЗВК.18, ЗВК.19. Организационные меры: РЗИ.3, КЗИ.1, КЗИ.2, КЗИ.3, КЗИ.5.

Процесс 5. Предотвращение утечек информации. Внедрение системы предотвращения утечки информации (DLP-система). Технические меры: ПУИ.1, ПУИ.2, ПУИ.3, ПУИ.4, ПУИ.5, ПУИ.6, ПУИ.8, ПУИ.9, ПУИ.10, ПУИ.11, ПУИ.12, ПУИ.13, ПУИ.15, ПУИ.17, ПУИ.18, ПУИ.19. Организационные меры: КЗИ.1, КЗИ.2, КЗИ.3, КЗИ.5.

Процесс 6. Управление и анализ событий защиты информации. Внедрение системы для сбора и анализа событий информационной безопасности. Технические меры: МАС.1, МАС.2, МАС.3, МАС.4, МАС.5, МАС.6, МАС.8, МАС.9, МАС.10, МАС.11, МАС.12, МАС.13, МАС.14. Организационные меры: РИ.12, РИ.13, РИ.14, ПЗИ.5.

Процесс 7. Защита среды виртуализации. Внедрение системы виртуализации. Технические меры: ЗСВ.3, ЗСВ.6, ЗСВ.9, ЗСВ.10, ЗСВ.32, ЗСВ.33, ЗСВ.34, ЗСВ.36, ЗСВ.37, ЗСВ.38, ЗСВ.39, ЗСВ.42, ЗСВ.43. Организационные меры: РИ.4, РИ.6, КЗИ.2, КЗИ.3.

Процесс 8. Защита информации при осуществлении удалённого логического доступа с использованием мобильных (переносных) устройств. Внедрение системы Mobile Device Management. Технические меры: ЗУД.3, ЗУД.4, ЗУД.5, ЗУД.6, ЗУД.7, ЗУД.8, ЗУД.9, ЗУД.10, ЗУД.11, ЗУД.12. Организационные меры: ЗУД.1, КЗИ.2, КЗИ.3, КЗИ.5.

Процесс 9. Требования к защите информации на этапах жизненного цикла автоматизированных систем и приложений. Организационные меры: ЖЦ.1, ЖЦ.2, ЖЦ.3, ЖЦ.4, ЖЦ.5, ЖЦ.6, ЖЦ.7, ЖЦ.8, ЖЦ.9, ЖЦ.10, ЖЦ.11, ЖЦ.12, ЖЦ.13, ЖЦ.14, ЖЦ.15, ЖЦ.16, ЖЦ.17, ЖЦ.18, ЖЦ.19, ЖЦ.20, ЖЦ.21, ЖЦ.22, ЖЦ.23, ЖЦ.24, ЖЦ.25, ЖЦ.26, ЖЦ.27, ЖЦ.28.

ВЫПОЛНИТЬ НЕВОЗМОЖНО

Из вышесказанного следует, что выполнить четвёртый уровень соответствия ГОСТ Р 57580.2–2018 по объективным причинам не представляется возможным. Показатели оценки реализации организационных и технических мер защиты из числовых значений перешли с 1 (реализуется в полном объёме) на 0 (полностью не реализуется) и/или 0.5 (реализуется не в полном объёме). Таким образом, снижается качественная оценка уровня соответствия по каждому процессу системы защиты информации.

ОФИЦИАЛЬНОЕ ПОСЛАБЛЕНИЕ

В начале марта от Центрального банка поступило информационное письмо по снижению требований к обеспечению защиты информации, указанных в нормативных актах Банка России. Послабление от Центрального Банка будет действовать до 01.01.2023. В данном письме было сообщено, что в случае выявления нарушений требований нормативных актов Банка России, устанавливающих требования к обеспечению защиты информации, возникших в результате действий санкционных мер ограничительного характера, считается целесообразным применение компенсирующих мер защиты.

ОДНАКО

Однако специалисты информационной безопасности оказались не готовы к новым реалиям жизни и не смогли выполнить рекомендации, указанные в письме, по причине отсутствия согласованного бюджета подразделений информационной безопасности на приобретение нового программного и аппаратно-программного обеспечения. Сказалась также возросшая нагрузка на специалистов по информационной безопасности из-за отключения от технической поддержки внедрённого продукта, участвовавших в DDoS-атаках, проведения оценки рисков, связанных с установкой новых обновлений (так как «железо» может стать «кирпичом»). Кроме того, на российском рынке, к сожалению, пока сложно найти альтернативные решения, способные заменить большинство наименований иностранных программных продуктов и оборудования. А как известно, «бумажной безопасностью» закрыть реально работающий процесс нельзя.

ЧТО ДЕЛАТЬ?

Что можно порекомендовать ИБ-специалистам в данной ситуации:

- ♦ Регуляторам помочь с выбором реализации выполнения технических мер.
- ♦ Провести обучение ИБ-специалистов по компенсации реализации требований нормативных правовых актов Банка России.
- ♦ Перенести сроки выполнения четвёртого уровня соответствия ГОСТ Р 57580.2–2018 на год или лучше на два.

В ПЕРВУЮ ОЧЕРЕДЬ

ВАШИ ДЕЙСТВИЯ В СВЯЗИ С УХОДОМ ИНОСТРАННЫХ ПРОИЗВОДИТЕЛЕЙ



Денис БАТРАНКОВ
член редколлегии
BIS Journal

ВЫБРАТЬ КРИТИЧНЫЕ РЕСУРСЫ ДЛЯ ЗАЩИТЫ

Выделите критичные для вас ресурсы, которые должны быть постоянно доступны вашему бизнесу, и защищайте их. Важно, что именно бизнес должен указать техническому персоналу те моменты, на которых нужно сфокусироваться. В зависимости от бизнес-процесса для кого-то критичным будет один сервер, управляющий производством, а для кого-то — ноутбук генерального директора или главного бухгалтера. В каждом бизнесе своё. И главное — сфокусироваться на контроле самого важного. Чтобы сохранить работающие бизнес-процессы, нужно оценить, какое оборудование и какой софт уже не работает, что перестанет работать в ближайшей перспективе, чем их можно заменить, как сохранить имеющиеся. Важно, что ресурсом являются и ваши сотрудники — нужно сохранить ключевых сотрудников и их экспертный опыт.

Всё, что описано выше, входит в Business Impact Analysis (BIA). Согласно международным

стандартам, ваш вице-президент по безопасности должен курировать этот процесс и на уровне бизнеса задавать recovery time objectives (RTOs) и recovery point objectives (RPOs), планируя стратегию защиты на основе этих чётких параметров. Самые срочные задачи описаны ниже.

СДЕЛАТЬ БЭКАПЫ И ХРАНИТЬ ИХ ОТДЕЛЬНО ОТ СЕТИ

Если проанализировать взломы последних месяцев, частая причина невозможности восстановить бизнес заключалась в том, что атакующий уничтожал не только рабочие системы, но и их архивы. Сделайте бэкапы и отделите их от сети физически, чтобы их гарантированно невозможно было уничтожить. Атака криптолокера на норвежскую сталелитейную компанию Norsk Hydro вызвала остановку всего бизнеса в 40 странах мира: производства алюминия, складов, офисов продаж. После атаки у них работала только облачная почта в Office 365. И именно через почту они смогли быстро скоординировать

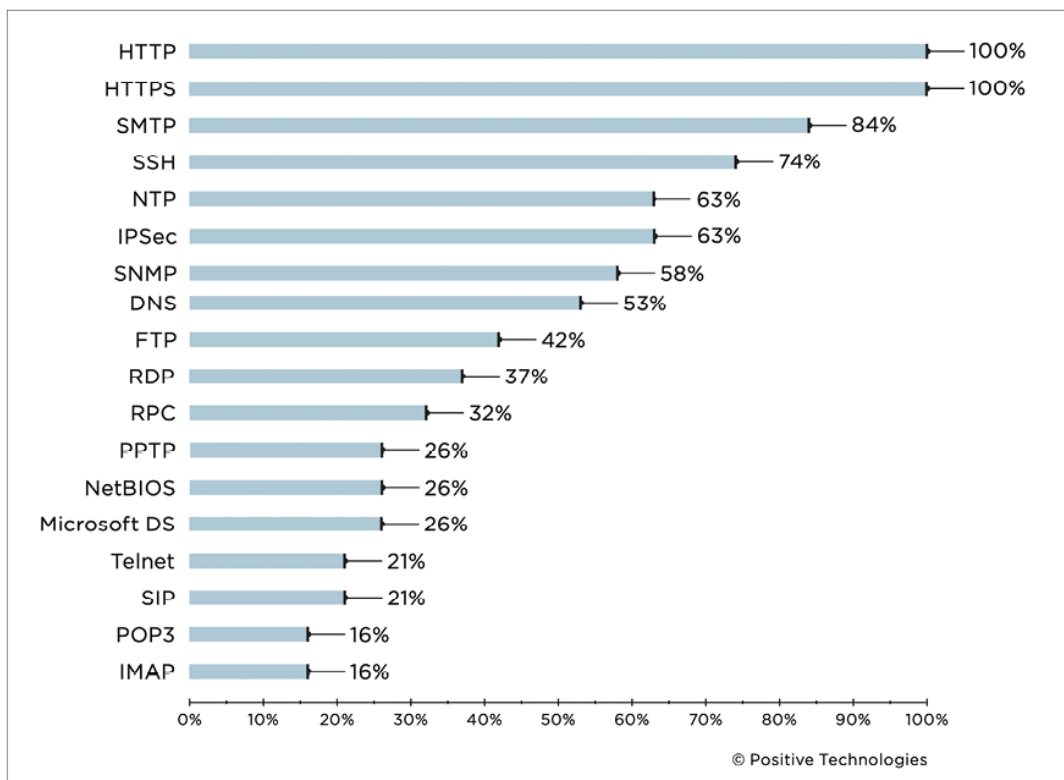


Рисунок 1. Любые выставленные в интернет ресурсы подвергаются атакам (источник: ptsecurity.com/upload/corporate/ru-ru/analytics/vulnerabilities-corporate-networks-2020-rus.pdf)

усилия и восстановить из архивов данные, серверы и рабочие станции. Правда, это заняло несколько месяцев.

ЗАКРЫТЬ НЕНУЖНЫЕ ВНЕШНИЕ РЕСУРСЫ И УЯЗВИМОСТИ

♦ Часто компании даже не знают о своих сервисах, доступных всему интернету, а также об их уязвимостях. Взломы последнего времени показали, что внешние ресурсы — самый частый способ проникновения в сеть: электронная почта, веб-сайты, сервисы управления. Любые выставленные в интернет ресурсы: веб-серверы, VPN-шлюзы, почтовые серверы, DNS-серверы, каналы связи — могут подвергнуться атакам (рис. 1).

♦ Согласно отчёту компании Positive Technologies, подбор учётных данных остаётся основным способом проникновения во внутреннюю сеть: результаты пентестов 2020–2021 года показали, что в 71% случаев этот способ проникновения оказался успешным (рис. 2).

♦ Множество взломов последнего года было выполнено через уязвимости Exchange, Citrix, CMS Joomla. Для проактивного выявления и устранения уязвимостей такого типа необходимо использовать и внедрить сканеры безопасности и процесс управления уязвимостями.

♦ Стоит обратить внимание на новый класс продуктов Attack Surface Management и на услуги класса Advanced Border Control. Необходимо назначить ответственного за каждый ресурс, чтобы в случае инцидента знать, к кому обращаться.

♦ Если у вас используется удалённый доступ к сети, всегда используйте двухфакторную аутентификацию, причём желательно российско-го производителя.

♦ Внешняя поверхность атаки может быть расширена еще и за счет ваших собственных удаленных сотрудников, которые могут быть атакованы, работая дома. Если они подключатся с зараженного устройства, то вы рискуете. VPN-шлюз должен устанавливать туннель с удалённым сотрудником через системы фильтрации трафика и проверки защищённости сотрудника, чаще всего реализованные в UTM/NGFW.

ЗАЩИТИТЕСЬ ОТ DDOS

♦ Часто публичные ресурсы нужны для работы, и сегодня их пытаются вывести из строя. По мнению большинства экспертов, атаки в 2022 г. в основном проводят политически мотивированные пользователи сети Интернет без специальных знаний в ИТ-технологиях. Их атаки не отличаются сложностью и легко блокируются доступными программно-аппаратными продуктами и сервисами защиты. Важно, чтобы такие средства у вас вообще были.



Рисунок 2. Подбор учётных данных остаётся основным способом проникновения во внутреннюю сеть (источник: ptsecurity.com/upload/corporate/ru-ru/analytics/positive-research-2022-rus.pdf)

♦ Чтобы подготовиться к DDoS-атакам на сервисы компании, установите нужное оборудование у себя или у провайдера либо подключите сторонние сервисы защиты от DDoS.

♦ При наличии веб-сервера на уровне веб-приложений часто используются решения класса WAF — они тоже умеют блокировать DDoS.

♦ Уже несколько раз звучали угрозы отключить Россию от интернета. Проанализируйте, а лучше проведите киберучения: будут ли работать бизнес-процессы при отключении страны от интернета?

ПЕРЕХОД НА РОССИЙСКИЕ АНАЛОГИ

♦ К атакам типа «выведение из строя» относятся и риски ухода иностранных поставщиков. Необходимо проанализировать, в чьей юрисдикции находится каждый поставщик программного и аппаратного обеспечения, и подготовить меры по переходу на локального поставщика в случае отказа от поддержки.

♦ Рекомендуется перейти из иностранных облачных сервисов IaaS, PaaS, SaaS, FaaS на их российские аналоги.

♦ Одна из угроз доступности внешних сервисов — отзыв сертификатов SSL/TLS. Проверьте, кто выдал вашим сервисам текущие SSL/TLS-сертификаты, и подготовьтесь к худшему сценарию, когда ваш сертификат отзовут.

ХАРДЕНИНГ

♦ Проанализируйте прошлые инциденты в вашей компании, и вы сразу поймёте, что вам надо улучшить в защите.

♦ Во многих операционных системах и приложениях есть дополнительные настройки безопасности. Включите их. Для каждой

операционной системы есть специальное описание, как это можно сделать, — hardening.

- ♦ Ваши критичные ресурсы должны быть заперты как можно дальше от возможных взломов, поэтому необходимо провести сегментацию сетей.

- ♦ Сейчас самое время провести инвентаризацию учётных записей и сменить пароли, чтобы не сомневаться в том, что сотрудники не скомпрометировали их.

- ♦ Проверьте, что у вас хорошо реализована двухфакторная аутентификация как минимум для VPN, — к сожалению, существуют техники её обхода.

- ♦ Двухфакторная аутентификация должна быть не только при доступе из внешних сетей, но и для доступа из одной внутренней сети в другую. Проверьте, что она включена везде. Это сдерживает скорость перемещения злоумышленников между сетями и даёт возможность службе безопасности обнаружить несанкционированную работу в сети.

- ♦ Сегодня важно убедиться, что процесс собственной разработки не использует публичные библиотеки исходного кода, которые могут быть исправлены злоумышленником. Стоит посмотреть, какие продукты класса SAST или DAST помогут вам в этом. Используйте фреймворк SLSA, технологию RASP и методики ФСТЭК к 76 приказу.

АУДИТ ЗАРАЖЕНИЙ

По статистике компании Positive Technologies, 9 из 10 компаний не знали, что они уже заражены. В связи с этим замечанием рекомендуется проверить, что ваша компания в данный момент ещё не заражена и не содержит компьютеров или сетевых устройств, где установлены уже известные виды вредоносного программного обеспечения. Для этого рекомендуется заказать внешний аудит. Возможно, вы можете использовать для этого экспертизу вашего центра мониторинга, blue team или read team. Нередко в компаниях есть свои группы реагирования на инциденты, собственный центр

управления кибербезопасностью (SOC) или внешние эксперты используются через сервисы MDR или MSS. Ваши эксперты периодически должны проверять вашу сеть на наличие признаков вторжений — этот процесс называется threat hunting.

ОБУЧЕНИЕ СОТРУДНИКОВ

- ♦ Современные атаки часто используют социальную инженерию, фишинг, watering hole, методы горизонтальных перемещений и взломы цепочки поставок. Проведите обучение сотрудников, чтобы они знали о возможных атаках социальной инженерии и о том, как правильно реагировать, если звонят из «службы безопасности». Часто сначала ломают вашего друга или партнёра, а затем через него проникают в вашу сеть, пользуясь доверием. Технологии дипфейк позволяют подменить и голос, и видео, поэтому риски могут быть с разных сторон.

- ♦ Оповестите сотрудников о том, на что обращать внимание при работе с поступающей электронной почтой, общении по телефону и почему опасно впускать в офис незнакомых.

- ♦ Чтобы любой сотрудник компании, в том числе любой сторонний человек, смог оповестить вашу компанию об инцидентах, распространите публично хоть какие-то контакты: куда можно обращаться в подобных случаях. Обычно это имейл или телефон дежурной смены центра управления безопасностью, центра реагирования на инциденты (SOC, CSIRT) либо техподдержки.

- ♦ Обменивайтесь информацией с коллегами по отрасли, проверяйте, как бы вы справились с инцидентом, который случился у соседей. Ведите статистику собственных инцидентов и отражайте во внутренних документах, как вы с ними справились.

- ♦ Обновите планы реагирования на основные типы инцидентов (DDoS, шифрование данных, взлом сайта, кража логинов и паролей сотрудников и клиентов, отказ оборудования), проверьте, доведены ли они до сведения всех сотрудников. Выясните, какие есть возможности для замены оборудования.

- ♦ Необходимо проинструктировать сотрудников или провести для них киберучения по действиям при атаке криптолокера, DDoS, краже конфиденциальных данных, остановке производства. В случае реального инцидента учиться будет некогда.

СЕГМЕНТАЦИЯ СЕТИ

- ♦ Сегментация — это не просто разделение на подсети или VLAN, это ещё и чёткие правила доступа на межсетевом экране (любого

Сегодня важно убедиться, что процесс собственной разработки не использует публичные библиотеки исходного кода, которые могут быть исправлены злоумышленником. Стоит посмотреть, какие продукты класса SAST или DAST помогут вам в этом

поколения) в каждый сегмент для каждого сотрудника и каждого приложения, которые ему требуются для работы.

♦ Знаю, что для многих правила по имени сотрудника или по его роли — новинка. Однако, если секретарь директора может по SSH подключаться в ЦОД, возникает вопрос к сотрудникам службы безопасности: зачем они написали правило на firewall, которое это разрешает?

♦ Успешные атаки внутри сети также не обходятся без подбора учётных записей: этот метод использовался в 93% успешных атак, по исследованию компании Positive Technologies. Используйте двухфакторную аутентификацию и identity firewall между внутренними сегментами, а также поведенческий анализ, чтобы отличить преступника от собственного сотрудника, работающих под одним аккаунтом.

♦ Существуют разные поколения межсетевых экранов. Избавьтесь от старинных правил на межсетевых экранах по портам TCP и UDP и напишите правила по конкретным приложениям, ведь по одному порту может ходить множество приложений. Не полагайтесь только на прокси-серверы, которые защищают только веб-трафик, — атакуют ещё по DNS, ICMP и по другим приложениям.

♦ Единственное, что хоть как-то сдерживает сегодня злоумышленника, — это контроль трафика ваших приложений. Однако правила по приложениям важно правильно настроить: если у вашего NGFW критерием правил всё равно являются порты TCP и UDP, после взлома одного сервера в ЦОД злоумышленник легко перемещается между серверами по разрешённым вами же соединениям. Например, если вы разрешили доступ по порту 80, думая, что там будет только HTTP, после расследования взлома большим откровением для вас станет, что там ходил SOCKS5.

♦ Иногда заказчики жалуются, что у текущих устройств защиты недостаточно производительности или неудобно встроить контроль приложений архитектурно, чтобы включить контроль приложений между внутренними сегментами сети. Нужно помнить, что контроль приложений и аккаунтов пользователей можно реализовать и в NGFW, и в системах класса NTA/NDR, которые подключаются к сети в режиме прослушивания на SPAN-порт или через устройства TAP.

МОНИТОРИНГ ПЕРИМЕТРА И СОТРУДНИКОВ, РАБОТАЮЩИХ ДИСТАНЦИОННО

Многим компаниям нужно начать контролировать исходящие из сети соединения на предмет

перемещения вредоносного контента и подключения к известным вредоносным адресам в Интернете и для сотрудников в офисе, и для сотрудников, работающих из дома. Для этого все их соединения нужно категорировать как через общеизвестные базы URL-категорий, так и через базы Threat Intelligence, специальные блокировщики DGA-доменов, «песочницы» и методики анализа контента приложений. Такие техники контроля исходящих соединений есть в решениях NGFW, SOAR, ZTNA, UTM, NTA и NDR.

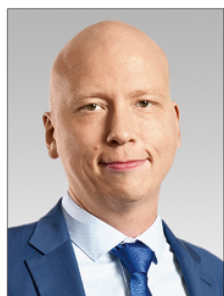
МОНИТОРИНГ ВНУТРЕННЕГО ТРАФИКА

Парадигма защиты поменялась. Взламывают даже такие бренды, как Sony, BMW, Facebook, LinkedIn, Garmin, RuTube. Проникнуть сегодня можно в любую компанию — невозможно заранее предугадать неизвестные уязвимости, как невозможно защититься от всех ошибок пользователей. По статистике Forrester, предприятия тратят в среднем 37 дней и \$2,4 млн на обнаружение и устранение последствий взлома.

Вдобавок после проникновения злоумышленник чаще всего работает от имени сотрудника компании, совершенно легитимными утилитами. Выявить злоумышленника сегодня можно только по поведению и по его ошибкам: он будет сканировать сеть, перемещаться между сегментами, повышать привилегии, подключаться к своим серверам управления. Подключения изнутри наружу к внешним серверам можно увидеть на периметровых устройствах защиты. Перемещение между сегментами увидеть гораздо сложнее — нужно контролировать работу таких протоколов, как RPC, SMB, Kerberos, RDP, SSH, а ещё инкапсулированных внутри VLAN, VXLAN или GENEVE. Для контроля внутреннего трафика сегодня применяются решения класса NTA/NDR. Именно сетевой трафик — ахиллесова пята взломщика: в сетевом трафике спрятать своё поведение невозможно, даже если он зашифрован.

ВЫПОЛНИТЕ ТО, ЧТО НЕОБХОДИМО

Люди нередко хорошо знают, как правильно поступать, но часто откладывают это на потом: поменять пароли, внедрить двухфакторную аутентификацию хотя бы для VPN, сделать бэкапы, нанять людей, вывести часть функций на аутсорсинг, осуществить харденинг, составить актуальную логическую схему сети, разобраться в адресном пространстве... И сегодня наступило то самое время, когда надо действовать!

**Вячеслав КАСИМОВ**

директор
департамента
информационной
безопасности
Московского
кредитного банка
(МКБ)

КТО ПЕРВЫЙ СОЗДАСТ NEXT GENERATION FIREWALL?

ВЯЧЕСЛАВ КАСИМОВ ПРОГНОЗИРУЕТ
ЭФФЕКТ РАЗОРВАВШЕЙСЯ БОМБЫ

Директор департамента информационной безопасности Московского кредитного банка (МКБ) Вячеслав Касимов в интервью BIS Journal дал свою оценку текущих реалий рынка информационной безопасности и поделился мнением о вопросах формирования киберкультуры и кадровой политики в организации.

О ТРЕНДАХ

— Как вы оцениваете текущую ситуацию в сфере информационной безопасности банков? Какие основные тенденции видите на рынке?

— Основной тренд — это повышенная активность хактивистов, которые организуют DDOS-атаки на различные предприятия, в том числе финансовой сферы, что доставляет всем большую головную боль. И если крупные банки уже давно адаптировались к такого рода активности, то малые кредитные организации определённо чувствуют себя не очень комфортно. При этом мы видим, что организаторы DDOS-атак развиваются. С одной стороны, это развитие заключается в том, чтобы находить технически грамотных людей, которые смогут отыскать дополнительные лазейки для повышения эффективности их DDOS-атак. С другой стороны, наблюдается тренд на то, чтобы производить и доставлять до организаций в РФ так называемые криптолокеры — это тот софт, который умеет запускаться на компьютере или сервере и шифровать весь жёсткий диск, делая, таким образом, недоступным этот сервер. И всё это на фоне отказа от привычных зарубежных средств защиты информации.

Всё это приводит к дискомфортной ситуации по той причине, что не все отечественные решения умеют справляться с криптолокерами. И это, кстати, серьёзная проблема. Обычно, если осуществляется удалённый доступ, то у защищаемой стороны есть время на то, чтобы идентифицировать это проникновение и, приняв необходимые меры, выбить злоумышленников

из инфраструктуры. А в случае с криптолокерами времени нет, потому что счёт идёт на минуты и распространение происходит очень быстро. Думаю, единственный правильный вариант в такой ситуации — придерживаться идеологии подводной лодки: если один отсек затопило, то она всё равно плывёт дальше. Я имею в виду необходимость тщательно организовывать межсетевое экранирование, в том числе между рабочими станциями пользователей, в текущих реалиях это must have.

Остальные тренды на рынке остались прежними. Был некоторый спад в активности мошеннических кол-центров, потом их активность опять резко возобновилась, и ситуация вернулась к уровням прошлого года.

БЛИЖНИЙ ПРОГНОЗ

— Во второй половине года чего ожидаете?

— Объективно будет рост доходов у ведущих отечественных производителей средств защиты информации, поскольку все денежные потоки, которые направлялись в адрес западных цепочек дистрибуции, переместятся в их сторону. Будут ли они инвестировать эти средства в собственное развитие, не знаю, очень надеюсь, что да.

Отмечу, что вообще ситуация складывается непростая, потому что некоторых классов систем защиты информации просто нет, например, Next Generation Firewall. Те, кто говорит, что они у нас есть, лукавят. С другой стороны, там, где наши производители преуспели и где были созданы отечественные средства защиты, у них нет конкурентов. Например, есть один известный производитель антивирусов, с которым в России никто, по сути, не конкурирует. Хотя справедливости ради стоит отметить, что попытки стали происходить, и это радостная тенденция.

Я думаю, что во втором полугодии всё будет сосредоточено на том, чтобы частично импортозаместиться, где это возможно, то есть завершить начатые весной процессы. Вторая

тенденция — это явная направленность подразделений информационной безопасности в организациях на то, чтобы использовать open source.

О НОВЫХ ТЕХНОЛОГИЯХ

— Если говорить о новых технологиях, применяемых в ИБ (блокчейн, VR, ИИ, роботы и тому подобные), какие из них вы считаете результативными и почему?

— Блокчейн — это, как правило, просто транспорт, и весь хайп вокруг него уже сошёл, я думаю. И в области ИБ — это тоже не та технология, которая хорошо ложилась бы под какие-то задачи. Я бы сказал, что это отложенный в сторону механизм, про который помнят, потому что, возможно, он когда-то пригодится.

Технология VR также слабо применима в информационной безопасности. А вот что касается искусственного интеллекта и роботов — это действительно полезные технологии. Так, нейронные сети успешно используются в антифрод-системах и для выявления аномалий в произвольных потоках событий. Например, есть SOC, который получает много информации от разных источников и затем её обрабатывает. Для дифференциации событий и выявления инцидентов создаются правила, но процедуры их создания долгие, они занимают годы. Поэтому использовать ИИ и нейронные сети для выявления событий, очень похожих на инциденты, — это хорошая идея.

Один из механизмов для такого рода идентификации создан в МКБ, мы планируем его интегрировать с нашим SOC. И в самом SOC — достаточно далеко идущие планы в отношении того, что делать в дальнейшем с точки зрения использования ИИ.

Роботы — это отличная история для операционных процессов, я сейчас говорю не об ИБ, а в целом об автоматизации в ИТ. Их эффективно использовать всякий раз, когда нужно какую-то работу упростить и за счёт этого снизить koszty. Например, заменить рутинный труд операторов при повторяющихся монотонных операциях: от обработки сканов документов до ввода типовых реквизитов платёжных поручений.

С точки зрения ИБ здесь есть целый класс решений под названием SOAR — это системы, которые позволяют автоматизировать реагирование на инциденты. Например, происходит подозрительная активность учётной записи одного из пользователей. Эту подозрительную активность можно первично обработать вручную (заблокировать), а можно автоматизировать. И здесь вполне применимы роботы.

В итоге получаем ситуацию, когда 50% новых технологий неплохо укладываются в рабочие

Многие технологии будут перспективными, хотя бы потому, что части классов решений нет в природе, а там, где есть всего один-единственный вендор, ниша тоже имеется. Поэтому в текущих условиях перспективно практически всё

процессы, 50% — либо со скрипом, либо — на полочку.

— Какие технологии обеспечения ИБ являются перспективными, по вашему мнению?

— Если бы мы были в ситуации год назад, то я уверенно сказал бы: всё, что касается качественного мониторинга и качественной идентификации каких-то инцидентов, — это мегаперспективные истории. Но сейчас мы вынуждены очень быстро бежать, чтобы не остаться на месте. Моё личное мнение — та компания, тот отечественный производитель, который первый создаст Next Generation Firewall, получит эффект разорвавшейся бомбы и станет чемпионом. Они замучаются покупать серверы для того, чтобы обеспечить необходимое количество поставок этого Next Generation Firewall. И с высокой вероятностью часть крупных компаний будут это покупать в режиме shut up and take my money, без сомнений и без тестирования.

КУЙ ЖЕЛЕЗО, ПОКА ГОРЯЧО!

Вообще, хотел бы сказать, что у нас рынок не так чтобы сильно заполнен отечественными разработками и гарантированно есть куда развиваться. Многие технологии будут перспективными, хотя бы потому, что части классов решений нет в природе, а там, где есть всего один-единственный вендор, ниша тоже имеется. Поэтому в текущих условиях перспективно практически всё.

— И сколько на это замещение потребуются времени, по вашему мнению?

— Любое решение, которое используется в ИБ, имеет некоторую софтверную и аппаратную составляющие, то есть должен быть софт, который работает на каком-то железе. Если мы говорим про полное импортозамещение, то здесь первоочередная задача — производить процессоры, хоть сколько-нибудь сопоставимые с процессорами AMD и Intel. Это отдельная сложная задача, которая требует серьёзных инвестиций, поэтому сложно даже примерно прогнозировать сроки. Что касается софта, то здесь можно управиться за пару лет.

Очень важна просветительская деятельность, которая должна вестись не только в банках, но и на государственном уровне. Необходимо задействовать все доступные каналы, чтобы донести, что такое социальная инженерия

ОБ ОТКРЫТЫХ API

— Каковы угрозы открытому API и наиболее действенные методы обеспечения безопасности в открытых API?

— Набор методов для защиты API достаточно стандартный. Начинается всё с Security Software Development Life Cycle — это методология, позволяющая идентифицировать потенциальные уязвимости на ранних стадиях, например, с помощью специализированных анализаторов кода. Найденные уязвимости должны быть проанализированы специально обученными людьми либо самими разработчиками и устранены к моменту выпуска релиза.

Существует несколько разновидностей анализаторов, например, статические и динамические. Но совершенно нелишним для дополнительной проверки будет задействовать так называемых white-хакеров.

Если вернуться в ситуацию на год назад, то я бы сказал, что очень перспективный механизм, когда продукт в препрод-стадии и когда он уже запущен в прод, выдаётся на анализ сообществу за вознаграждение в рамках программ Bug Bounty. Кстати, насколько мне известно, сейчас нет российских программ Bug Bounty, и было бы хорошо создать такие.

Не следует забывать и о контроле настроек серверов, на которых функционирует Open API, и об устранении инфраструктурных уязвимостей. А для того чтобы убедиться, что открытое API действительно хорошо и безопасно работает, важно также обращать внимание не только на классическую информационную безопасность, но и на так называемую продуктовую безопасность, когда эксплуатируется особенность алгоритма реализации самого продукта, например, покупается товар со скидкой, но есть возможность его вернуть с полной стоимостью.

В целом, говоря об открытых API, важно помнить об их многоаспектности. Я бы посоветовал начинать со взвешенного анализа рисков, чтобы понять, какие изъяны в модели обслуживания, которое предлагается с открытым API,

можно найти. Дальнейшее развитие уже зависит от квалификации аналитиков, которые этим занимаются.

О СОЦИАЛЬНОЙ ИНЖЕНЕРИИ И КИБЕРКУЛЬТУРЕ

— Какова, на ваш взгляд, наиболее эффективная практика борьбы с социальной инженерией?

— Я искренне уверен, что наиболее эффективная практика — доводить каждого социального инженера до суда и справедливых вердиктов. Как только широкая общественность узнает, что любая подобная активность приводит к тюремному сроку, количество желающих этим заниматься резко снизится.

С точки зрения того, как не допустить, чтобы клиенты становились жертвами социальной инженерии, очень важна просветительская деятельность, которая должна вестись не только в банках, но и на государственном уровне. Необходимо задействовать все доступные каналы, чтобы донести до разных слоёв населения, что такое социальная инженерия и на что она направлена.

У банков, конечно, есть антифрод, но здесь приходится подключать людей, которые бы совершали контрзвонки, а у нас их априори меньше, чем «сотрудников» у мошеннических кол-центров. Мы звоним пожилым людям в тех случаях, если возникают подозрения, что они стали жертвами социальной инженерии. Но их очень сложно переубедить, потому что первые звонящие для них в приоритете. Действительно, есть серьёзные проблемы с тем, чтобы переубедить человека, который уже попал под психологическое воздействие социальных инженеров. Более или менее работает история, когда советуешь просто снять деньги и спрятать их куда угодно, только не переводить никому другому. Это даёт людям дополнительное время на осмысление произошедшего, и зачастую они выходят из-под влияния мошенников.

— Проблема киберкультуры в компании: как её формировать и сколько на это требуется времени?

— Для того чтобы её сформировать, нужно на многих уровнях объяснять людям, что такое информационная безопасность, зачем она нужна, каковы могут быть последствия тех или иных инцидентов. Это нужно делать не раз, особенно с учётом смены людей в различных подразделениях. По сути, это большая программа по обучению, которая должна реализовываться разными способами: дистанционные курсы, очные семинары и тренинги, повторяющееся обучение,

киберучения, учения, связанные с фишинговыми рассылками и так далее.

Я хочу обратить внимание на то, что уровень технической грамотности обычных пользователей и ИТ-персонала немного разный. Важно акцентировать внимание и разрабатывать отдельные обучающие курсы для ИТ и для других подразделений, потому что не все курсы одинаково полезны разным категориям работников. Мы, например, сейчас пытаемся запустить программу секьюрити-чемпионов, чтобы наши «агенты» были внутри ИТ и распространяли там хорошее, доброе, вечное и безопасное.

О КАДРАХ В ИБ

— Кадры в ИБ: как искать, учить, удерживать? Хотелось бы узнать вашу оценку кадровой ситуации в настоящее время.

— Для меня она несколько шокирующая. Уровень заработных плат, которые хотят люди с какими-то базовыми навыками, очень маленьким опытом и сомнительными перспективами дальнейшей работы в этой сфере, достаточно высок, и за последние 2–3 года он вырос в два раза. И я хорошо знаю, чем это вызвано. Есть ряд компаний, которые сыпали деньгами в большом количестве. И таких денежных волн в этой сфере за последние пять лет наблюдалось несколько. Это расшатало рынок в сторону того, что зарплатные ожидания сильно увеличились, поэтому сейчас ситуация непростая.

Есть разные варианты, как искать кадры. Например, с помощью записной книжки или на профильных конференциях и мероприятиях в рамках живого общения. Используем также обычный поиск на рынке, а также помогают советы коллег. Мы рассматриваем все эти варианты, потому что наши кадровые аппетиты растут из-за того, что бизнес развивается, количество ИТ-систем и ИТ-персонала увеличивается.

Как учить? Люди хорошо обучаются в процессе работы, иногда им помогает дополнительно обучаться некоторая ротация между подразделениями, например, администраторы хотят заниматься мониторингом или криптографы устали от генерации ключей и хотят чего-то большего, в связи с чем переходят в другие подразделения, чтобы администрировать другие системы. Здесь точно есть масса возможностей внутри крупных организаций.

В нашем банке, например, используется практика самостоятельного внедрения решения без активного привлечения интегратора. В процессе внедрения новых продуктов и даже их тестирования люди тоже учатся.

Учить людей можно как в рабочем процессе, так и с помощью специализированных курсов, в том числе онлайн. Например, навыки администрирования Windows и Linux хорошо приобретаются на базе онлайн-курсов. И хочу заметить, что это очень полезная вещь, потому что далеко не у всех студентов и выпускников есть навыки подобного рода.

Удерживать персонал помогают три фактора, по моему мнению. Первый — ставить интересные задачи, которые не превращают жизнь людей в рутину. Второй — не допускать выгорания людей. Третий — поддерживать адекватный уровень оплаты труда. Если человек сыт, одет, обут, у него есть крыша над головой и интересная работа, причём с соблюдением баланса личной жизни и этой работы, то в такой ситуации он не будет смотреть на рынок труда вообще. Задача менеджера — грамотно скомбинировать эти три фактора.

НЕМНОГО О СЕБЕ

— Всегда с удовольствием слушаю ваши выступления на конференциях, поэтому, если позволите, личный вопрос: как вы стали безопасником?

— Это забавная история. Я жил недалеко от МАИ, решил пойти туда на подготовительные курсы. Успешно сдал экзамены и поступил на не очень интересный для меня факультет — летательные аппараты. Одновременно мой школьный товарищ попросил помочь ему с поступлением в институт, то есть, говоря другими словами, выполнить задания за него. Времени было достаточно, и мне не составило труда составить компанию моему приятелю. Мы пошли в Московский государственный технический университет гражданской авиации. Изучали, какие там есть специальности, потому что ни он, ни я толком ничего не знали об этом. Увидели специальность «информационная безопасность». Я почитал описание, мне показалось это интересным, и я предложил подать документы на эту специальность. Всё шло хорошо, я сдавал экзамены за себя и за товарища, дошли до русского языка. Там была 25-бальная система, я задание выполнил успешно, а товарищ сдал на 4 балла из 25, поскольку в этот раз он решил справиться без моей помощи. Таким образом, я прошёл на бесплатное обучение и с тех пор начал погружаться в информационную безопасность. Не могу сказать, что университет мне дал очень много, но поскольку я совмещал работу и учёбу, то всё глубже уходил в сферу ИБ, и думаю, сейчас я здесь уже по-настоящему прижился.

Беседовала Оксана Дяченко

АНТИФРОД СЕГОДНЯ

ЗАМЕТНО ОТЛИЧАЕТСЯ ОТ АНТИФРОДА ВЧЕРА



**Василий
ОКУЛЕССКИЙ**
эксперт, кандидат
технических наук

Недavno состоялся Уральский форум — 2022 в новой концентрат-форме в Москве. Прошёл обмен мнениями, знаниями по самой разной тематике из области информационной безопасности финансовой сферы. Мнения разные, обсуждения порой очень горячие, но общий настрой приподнятый, боевой. Я хочу обратиться все-го к одному вопросу, который активно и жарко обсуждался на официальных площадках форума, в кулуарах, на стендах, — противодействие операциям без согласия клиентов. Именно так теперь называется борьба с мошенниками. Это довольно разные смыслы, но будем говорить, как учит нас регулятор.

И ВЧЕРА, И СЕГОДНЯ, И ЗАВТРА

По общему мнению участников, попытки обманывать клиентов банков были, есть и будут всегда, пока есть хоть какие-то эквиваленты денежных средств. Защититься от этого полностью невозможно, и универсальных «серебряных пуль» в природе не существует. Тем не менее защита клиентов должна быть, необходимо снижать вероятность операций, имеющих соответствующие признаки, совершенствовать механизмы возврата денежных средств клиентам, тем самым минимизируя риски потерь клиентов.

Очень много разговоров было о сборе данных об окружающей среде, о повышении осведомлённости клиентов и сотрудников банков, телекоммуникационных, страховых, ретейловых и прочих компаний. Были сформулированы новые данности.

Однако...

Если говорить о базовых понятиях, в первую очередь о рисках, то они остаются базовыми, независимо от внешних изменений:

- ◆ финансовые потери клиента;
- ◆ финансовые потери банка;
- ◆ снижение рейтинга банка;
- ◆ запрет на проведение операций с использованием систем ДБО;
- ◆ массовый отток клиентов;
- ◆ осложнение отношений с регулятором и т.д.

Проблемы, которые надо решать, как говорится, и вчера, и сегодня, и завтра, те же:

- ◆ проведение платежа без согласия клиента — это операция мошенническая или просто?

◆ Что такое признаки операции без согласия клиента в случаях атаки типа «социальная инженерия»?

◆ Как реагировать на появление признаков операции без согласия клиентов при онлайн-платежах, ведь это ещё не мошенническая операция?

◆ Какова юридическая значимость заключений ИИ?

Типовые векторы атак:

- ◆ атаки на инфраструктуру проведения платежей;
- ◆ атаки на программное обеспечение СДБО;
- ◆ атаки на клиентов с использованием социнженерии;
- ◆ атаки на сотрудников банка также с использованием социнженерии.

Основные «усилители» атак, как и сами люди, опять те же:

- ◆ страх;
- ◆ жадность;
- ◆ любопытство;
- ◆ недостаток осведомлённости и психологической устойчивости «клиента».

Наша работа борцов за безопасность платежей, как и раньше, имеет два пути (рис. 1):

- ◆ внедрение средств сбора и анализа средств платежа клиента и создание поведенческих профилей клиентов на основе ИИ для принятия решения о проведении платежа;

- ◆ повышение осведомлённости клиентов по всем возможным каналам.

ТАК ЧТО ЖЕ ПОМЕНЯЛОСЬ?

Так что же поменялось? Чем сегодня отличается от вчера? Предложу свой ответ:



Рисунок 1. Работа борцов за безопасность платежей по-прежнему имеет два пути

Тип атаки	Подготовительная работа	Атака - социнженерия	Проведение платежа	Обналичивание денежных средств
получение всех необходимых постоянных данных	предварительное получение клиентских данных	получение одноразовых данных для платежа	использование СППДС мошенника, переводы, оплата покупок в интернет-магазинах	перевод на кошелек, обналичивание в банкомате
получение всех необходимых постоянных данных	частичное получение неполных данных клиента	получение недостающих клиентских данных и одноразовых данных для платежа	использование СППДС мошенника	перевод на кошелек, обналичивание в банкомате
убеждение клиента о необходимости перевода д/с на "защищенные" счета	частичное получение неполных данных клиента	убеждение клиента самому перевести д/с	использование СППДС самого клиента	перевод на кошелек, обналичивание в банкомате
убеждение клиента в необходимости "содействия"	частичное получение неполных данных клиента	убеждение клиента взять кредит и перевести/отдать кредитные средства	использование СППДС самого клиента	получение наличных от самого клиента, перевод на кошелек, обналичивание в банкомате

Рисунок 2. Мы можем анализировать только электронные следы действий клиента

♦ повысилась общая тревожность общества, что помогает мошенникам иметь всё время постоянную актуальную тематику для атаки;

♦ постоянно меняются между собой весовые составляющие разных видов атак;

♦ в социальной инженерии очень быстро меняются темы «разговора» при остающихся прежних схемах атаки;

♦ отключились/переключились многие зарубежные «кол-центры»;

♦ возникли некоторые технические проблемы непосредственно с самими удалёнными каналами взаимодействия с клиентами, осложнились вопросы обеспечения доверия в каналах взаимодействия;

♦ мобильный банк всё чаще частично «возвращается» в интернет-банк;

♦ возросли риски отключения зарубежных облачных сервисов, используемых как для проведения платежей, так и для их контроля;

♦ для ряда банков работа финмониторинга стала «врастать» в антифрод;

♦ постоянно расширяется функциональность СБП, которая требует оперативной доработки мобильных сервисов в СДБО;

♦ недостаточно быстро внедряется технология 3DS2.0 в эквайринге.

Последнее время при обсуждении проблем СДБО всё сводится либо к психологии клиента (правая ветка), либо к бездействию телекома и банков (левая ветка). При этом задачи противодействия переводам денежных средств в основном решают коллеги из антифрода. А у них не так много доступных технических инструментов. Повышение осведомлённости — отдельная большая задача, о ней скажем пару слов ниже. Давайте попробуем посмотреть, как антифрод выглядит изнутри.

АНТИФРОД ИЗНУТРИ

Как правило, мы не видим непосредственно клиента, не видим его гаджеты, не видим, чем он в данный момент занимается. Мы можем анализировать только электронные следы его действий (рис. 2).

Это не полная картина, это только её часть, но она даёт возможность увидеть, какими данными могут располагать системы антифрода. В упрощённом виде данные в этих системах можно условно разделить на две большие группы — сеансовые данные и данные о предыдущей активности клиентов,

Сеансовые данные — геолокация, тип авторизации, время, серийный номер устройства, характеристики программного обеспечения средства платежа, признаки наличия вредоносного ПО, удалённого управления устройством и другие позволяют идентифицировать клиента, авторизовать его право управления денежными средствами. Анализ и использование результатов анализа таких данных позволяет отсеять действия, совершаемые с «чужого» средства платежа, но не более.

Данные о предыдущей активности клиентов могут содержать какие-то временные параметры проведения платежей, обычные суммы, назначения и адреса платежей, типовые места проведения платежей и т.д. Анализ этих данных позволяет сформировать некий типичный профиль поведения клиента и тем самым позволяет выявлять нетипичные платежи и строить какое-то дополнительное реагирование на него.

Очевидно, что в случаях с социальной инженерией, когда клиент сам переводит свои деньги злоумышленнику, этих данных для выявления признаков совершения операции без согласия

клиента недостаточно: формально клиент всё переводит сам. И вот здесь необходимы принципиально новые механизмы анализа поведения клиента. Это могут быть характеристики моторики клиента при наборе на клавиатуре или виртуальной клавиатуре данных платежа, особенности использования мыши при вводе данных и им подобных механизмов. И тут встают сразу две технических и масса этико-нормативных проблем: необходимо, во-первых, создавать инструменты сбора подобных данных, а во-вторых, создавать инструменты анализа этих данных, построенных на использовании искусственного интеллекта, с одной стороны, и юридического обеспечения использования ИИ — с другой.

ПРО ОСВЕДОМЛЁННОСТЬ КЛИЕНТОВ

Если обратиться к проблеме повышения осведомлённости, то ситуация выглядит довольно странно (рис. 3).

По известному принципу Парето основная масса наших клиентов, и это порядка 80%, абсолютно нормальные люди, которые стараются делать всё правильно и поэтому обычно не создают проблем ни себе, ни банкам. Есть обязательная составляющая около 10% (слева) супергипербезопасников, которые всё знают и всё делают лучше всех, и есть 10% (справа), которым всё всё равно. Наша обычная направленность «повышения осведомлённости» — это те самые 80%, которые проблем не создают, «леваки» эту работу игнорируют, потому что они «лучше знают», а «правакам» это всё равно. Более того, для «праваков» до сих пор срабатывают старые добрые уловки, например,

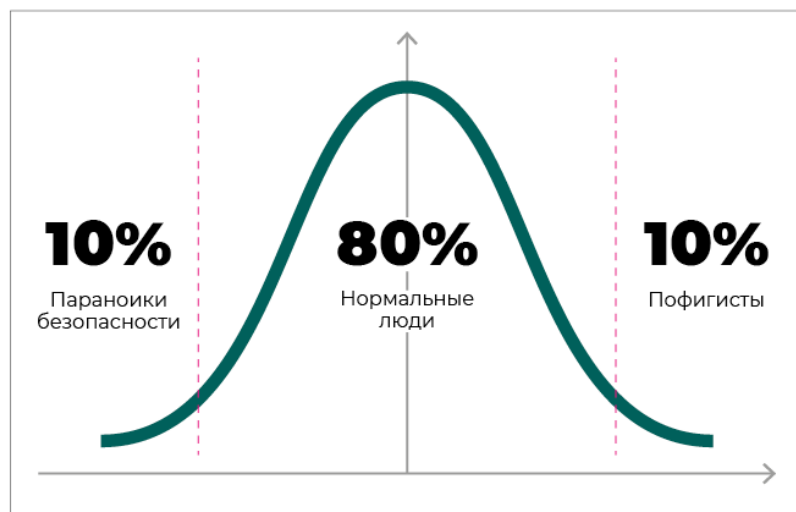


Рисунок 3. Осведомлённость надо строить с учётом отношения людей к правилам. Принцип Парето

картинка из архива (рис. 4) до сих пор срабатывает, и люди добросовестно вводят свои данные в эту форму:

ИТОГИ

Подведём итоги.

◆ Новые проблемы всегда создают новые возможности, и это обязательное условие успешного развития отрасли, они заставляют нас искать и находить новые решения, использовать самые передовые технологии.

◆ Во главе любых видов атак всегда стоит экономика методов, поэтому методы борьбы со злоумышленниками должны в первую очередь иметь экономическую основу, поэтому внедрение систем технической защиты периметра банковской организации, систем антифрод-мониторинга должны быть категорией «must have». При этом надо понимать, что внедрение таких систем — не панацея, а лишь бэкграунд системы безопасности СДБО.

◆ Настало время активно переходить на отечественные системы антифрода, и они не просто есть, но стали даже круче импортных.

◆ Обязательным условием успешной борьбы с мошенничеством в СДБО является постоянное совершенствование систем авторизации пользователей на основе постоянного расширения параметров аутентификации (системы анализа данных гаджетов клиентов на самые разные fingerprint, включая сим-карту, сам гаджет, его ПО, режимы работы, данные СП при веб-версиях ДБО), в том числе с использованием систем поведенческого анализа клиента на основе ИИ, что также серьёзно поможет выявлению случаев самопереводов.

◆ Обязательно внедрять механизмы дополнительного подтверждения при превышении уровня риска платежа.

◆ Совершенствовать системы выявления и пресечения деятельности «дропов» на основе решений ФинЦентра и антифрода НСПК, формировать российские облачные сервисы.

◆ Совершенствование систем контроля и защиты от утечек банковских и клиентских данных в самих банках, компаниях, обрабатывающих такие данные.

И удачи в нелёгкой борьбе за безопасность клиентов!

Сергей ВИХОРЕВ

советник генерального директора ООО «ИТ-Экспертиза»

А ОДИН В ПОЛЕ ВОИН?

ЭССЕ О ДОМОХОЗЯЙКАХ, МЫШАХ И АНТИФРОДЕ

ХОЗЯЙКА ЗРИТ В КОРЕНЬ

Антифрод — это важно. Но как-то однобоко мы подходим к этой проблеме. С одной стороны, повышение осведомлённости клиента. Правда, непонятно, насколько это эффективно. Ведь ещё незабвенный дедушка Крылов правильно заметил:

«Уж сколько раз твердили миру, Что лесть гнусна, вредна; но только всё не впрок, И в сердце льстец всегда отыщет уголок».

С другой стороны, мы стараемся определить всеми возможными способами, в том числе и с использованием искусственного интеллекта, причём по косвенным признакам, а то ли лицо, которому положено, совершило эту транзакцию. А в целом получается, что вектор наших усилий направлен только в одну сторону: клиент, совершающий сделку. Но ведь палка всегда о двух концах. И если есть «жертва», то всегда будет и «злоумышленник». Причём он не дурак, он мимикрирует, он подстраивается под ситуацию, он, в конце концов, ловит «хайп». И это важный элемент в мошеннических действиях по совершению операции без согласия клиента, который полностью выпадает из поля зрения антифрода.

А как борется с мышами хорошая хозяйка? Разве она пытается закрыть все дыры, через которые они лезут? Нет, она раскладывает отраву, чтобы уничтожить зло в корне.

О ПРОФИЛЕ ЗЛОУМЫШЛЕННИКА

И тут вырисовывается новое направление в борьбе с фродом. А не задуматься ли нам не о профиле клиента, а о профиле злоумышленника? Сложно? Да. Возможно? Да.

Давайте рассмотрим такую ситуацию. Положим, злоумышленник хочет либо получить данные клиента, либо убедить его перевести деньги на другой счёт. Он будет звонить потенциальной жертве и обрабатывать её. По всей вероятности, он будет использовать какой-то кол-центр или несколько разных сим-карт. При этом злоумышленник вряд ли будет бегать по городу, чтобы каждый раз сделать звонок из другого

места. Следовательно, можно выделить первый демаскирующий признак: местоположение злоумышленника, из которого либо идёт много звонков с одного или нескольких номеров, либо используют много разных сим-карт.

Пойдём дальше. Злоумышленник вряд ли будет звонить наобум (хотя и это не исключено, но это другой случай), ему нужно для начала иметь какую-то базу, где есть по крайней мере Ф. И. О. жертвы, её телефон и, лучше всего, банк, в котором у жертвы счёт или номер банковской карты. Такую базу злоумышленник, скорее всего, купит в даркнете. Не думаю, что таких баз у злоумышленника в один день будет «в работе» несколько. Следовательно, скорее всего, свои звонки он будет совершать клиентам одного банка. Это позволяет нам дополнить и расширить демаскирующий признак: местоположение злоумышленника, из которого либо идут много звонков клиентам одного банка с одного или нескольких номеров, либо используют для этих целей много разных сим-карт. Ну а дальше, используя современные методы геолокации (а может быть, и искусственного интеллекта), вполне реально вычислить «лёжку» злоумышленника.

А дальше всё просто: берём и ликвидируем «лёжку» и тем самым спасаем много-много дедушек и бабушек от возможности потерять свои средства. Заметьте, это не методы социальной инженерии, это не технические методы, это скорее аналитические методы. Мы должны не только анализировать действия клиента, но ещё и научиться анализировать действия злоумышленника. Иначе в вечной борьбе «действие — противодействие» мы всегда будем в отстающих.

А теперь вопрос. Это дело службы банка? Нет! Здесь уже зона ответственности силовых структур, операторов связи, аналитиков и прочая. Вот и получается, что проблема антифрода — это проблема скорее не банка, а внешних структур. Но и с банка ответственность не снимается. Всё-таки хорошая хозяйка в первую очередь постарается залить мышиную норку цементом с битым стеклом...

Андрей КУРИЛО

советник по вопросам ИБ ФБК и FBK CyberSecurity

Согласен с С. Вихоревым в том, что борьба с мошенничеством (возьмём пошире) — это далеко не проблема банков. Это дело государственное, так как в нём слишком много различных составляющих, слишком много центров управления отдельными компонентами, и государственные интересы, прямо обозначенные в Конституции РФ, пересекаются тут с интересами бизнеса.

А что касается формирования профилей преступника — вопрос хороший, однако мне кажется, что этот подход

труднореализуем, так как слишком высока неопределённость в такой задаче, сложно будет выработать решение на блокирование операции на основании не слишком точных данных.

С. Вихорев в ответ спросит: зачем блокировать транзакцию? Надо блокировать мошенника. И это правильно, но долго и непонятно, насколько эффективно. Ведь нужно будет доказать в суде, что задержанное лицо — мошенник. Иначе никак.

БЕГ НА МЕСТЕ ИЛИ ТАК НАДО?

ПОНЯТИЕ РЕПОЗИТОРИЯ И СИСТЕМЫ РЕПОЗИТОРИЕВ В МИРЕ И РОССИИ С ПОЗИЦИЙ ПРОГРАММНОЙ ИНЖЕНЕРИИ

Во всем мире использование репозиторий связано с сокращением трудозатрат разработчиков информационных систем, затрат на покупку и поддержание средств производства и эксплуатации информационных систем, времени создания новых систем и программных продуктов, а также обеспечения их качества в широком смысле.

Крупные финансовые структуры и разработчики финансовых информационных систем, как правило, имеют свои собственные репозитории, но при этом также пользуются услугами проверенных коллективных репозиторий типа GitHub для резервирования собственных разработчиков и повышения доступности привлечения новых талантливых разработчиков, для использования при необходимости отдельных дорогостоящих средств разработки, а также для использования других услуг репозиторий. Технические требования финансовых структур к современным репозиториям и качеству услуг в целом соответствуют требованиям к глобальным платежным системам.

Потребность в репозиториях для информационных систем и программных продуктов на всех этапах жизненного цикла известна давно, но необходимость иметь собственные российские репозитории стала по-настоящему понятна руководителям отрасли после санкций в марте 2022 года. На заключительной стратегической сессии по развитию электронной промышленности 21 марта 2022 года (<http://government.ru/news/44874>) прямо говорилось «...о необходимости создания государственного репозитория».

А что такое «репозиторий» в современном понимании программной инженерии, какие функциональные и технические требования предъявляются к современным репозиториям?

Мне запомнилось, как первый программист, ставший академиком в Советском Союзе, — академик Андрей Петрович Ершов в одном из своих выступлений в Новосибирском Академгородке дал понятие программиста в зависимости от того, сколько лет он занимается программированием и его квалификации. Программист, разрабатывающий программу на определенном языке и типе ЭВМ через рост квалификации поэтапно приходит в состояние аналитика-программиста, системного программиста, ученого-программиста. Идет накопление знаний, идет развитие понятия программиста.

Так и понятие репозитория и системы репозиторий информационных систем и технологий программного обеспечения вычислительной техники также развивается в рамках программной и системной инженерии. Сами понятия репозитория и системы репозиторий трактуются специалистами с различных точек зрения. Поэтому необходимо определиться с данными понятиями для того, чтобы четко формулировать технические требования к конкретным репозиториям и не смешивать все в одну кучу.

Термин «репозиторий» первоначально появился в стандарте открытых систем и также развивается по нескольким направлениям (https://www.altlinux.org/Репозитории_СПО).

Общедоступные репозитории используются как отдельными программистами, так и командами программистов, мелкими и крупными компаниями в повседневной жизни. Репозитории фактически присутствуют во всех современных платформах разработок программного обеспечения, они являются неотъемлемой частью информационных систем.

В настоящее время понятие репозитория в мире тесно связано с понятием фонда алгоритмов и программ, с проектированием архитектуры информационных систем, коллективными средами автоматизации программирования, с коммуникацией разработчиков, подбором программистов, обеспечением быстрой и безопасной разработки программ, поддержки и управления качеством информационных и программных систем, обеспечением информационной безопасности и доверенности программных систем на всех этапах жизненного цикла.

Без этих связанных понятий и функций понятие репозитория часто сводится к банальному понятию «облачного хранения файлов для коллективной работы через Интернет» или распределенной инфраструктуры разработки программного кода, включая библиотеки программ, с возможностью контроля версионности, дополненная функциями совместной работы над кодом, багтрекинга, автоматической проверки и тестирования, а также другими инструментами разработки и обеспечения целостности.

И, наконец, понятие репозитория прямо связано с понятием собственности, интеллектуальной собственности, авторской собственности, обеспечением взаимодействия покупателя и продавца на всех этапах подготовки и выполнения контракта.

Поэтому операторов репозитория можно классифицировать как по типу собственности (личная, международная, коммерческая, государственная), по функциональным характеристикам (перечислены выше), а также по технологической независимости от других стран и собственников.

В ряде развитых стран наряду с open source repository поддерживаются и финансируются:

- ♦ «открытые» межгосударственные репозитории программного обеспечения и знаний для коллективных научных исследований в различных областях науки (научные межгосударственные репозитории),

- ♦ коммерческие репозитории (типа GitHub компании Майкрософт или российские аналогичные минирепозитории на уровне банков или ИТ компаний, проект репозитория ФГИС «Реестр отечественного ПО» Минцифры для отечественных разработчиков, GitFlic),

- ♦ государственные репозитории программного обеспечения, разработанного и поддерживаемого за счет денег налогоплательщиков (типа code.gov, Национальный фонд алгоритмов и программ Минцифры, репозиторий ГОСТЕХ, несостоявшийся проект национальной программной платформы национального проекта Информационное общество ([https://www.tadviser.ru/index.php/Продукт:Национальная_программная_платформа_\(НПП\)](https://www.tadviser.ru/index.php/Продукт:Национальная_программная_платформа_(НПП)))).

Технологическая платформа (ТП) «Национальная программная платформа» (НПП) была

организационной формой, объединяющей ее участников для достижения поставленной цели — развития отечественной отрасли ПО.

В настоящее время Минцифры продолжает попытки реализации ряда проектов по созданию репозитория без учета обеспечения жизненного цикла программного продукта и уровня зрелости компании разработчика, это:

- ♦ репозиторий «Экосистемы разработки и тестирования программно-аппаратных комплексов в НИИ «Восход»;

- ♦ репозиторий ГОСТЕХ;

- ♦ новое положение по Национальному фонду алгоритмов и программ;

- ♦ инициативы создания «маркетплейсов» российских программных продуктов, магазинов мобильных приложений;

- ♦ концепция развития open source и создание оператора репозитория в рамках АНО «Открытый код» при поддержке Фонда развития ИТ;

- ♦ «Стратегия создания российского репозитория программных пакетов и библиотек, находящегося в юрисдикции и на территории Российской Федерации», которую Ассоциация документальной электросвязи должна была представить до конца 2021 года.

ФСТЭК России заказала две опытно конструкторские работы:

- ♦ по созданию доведенного ядра ОС Линукс;

- ♦ по «Разработке унифицированной среды разработки безопасного отечественного

BIS-КОММЕНТАРИЙ

МИНПРОМТОРГ ПОДДЕРЖАЛ...

BIS Journal попросил прокомментировать текущую ситуацию с отечественными репозиториями заместителя главы Минпромторга России Василия Шпака, одного из активных инициаторов их создания. После многочисленных звонков и почти двухмесячной переписки с сотрудниками пресс-службы Минпромторга был получен куцый официальный ответ. По сути это классическая ведомственная отписка — обтекаемая и малоинформативная. И это печально, вроде ведь одно большое дело делаем. Но, как говорится, спасибо и на этом. К следующему номеру постараемся найти более полную информацию.

Минпромторг поддержал идею создания доверенных ПАК, высказанную предприятиями отрасли.

Необходимость создания отечественного репозитория программных пакетов и библиотек (ПАК) обусловлена невозможностью влияния на политику использования зарубежных репозиториях. Минпромторг согласен, что наиболее серьезными рисками при производстве программного обеспечения, созданного на базе зарубежных репозиториях, становятся: встраивание недекларируемых возможностей, отсутствие контроля над жизненным циклом программного продукта и влияния на техническую политику разработки программного обеспечения, отсутствие механизмов, обеспечивающих совместимость с отечественными продуктами.

На текущий момент разработана и проходит согласование Стратегия создания российского репозитория программных пакетов и библиотек, находящегося в юрисдикции и на

территории Российской Федерации. Идея создания такой стратегии принадлежит предприятиям отрасли.

Основными целями создания российского репозитория являются:

- обеспечение условий устойчивого развития отечественной отрасли информационных и телекоммуникационных технологий;

- обеспечение необходимого уровня конкурентоспособности отечественных компаний на международном рынке;

- содействие созданию инфраструктуры разработки отечественного программного обеспечения, реализуемого на отечественных аппаратных платформах;

- обеспечение целостности, безопасности и устойчивости функционирования объектов критической информационной инфраструктуры Российской Федерации, включая объекты военного и государственного управления.

Пресс-служба Минпромторга

программного обеспечения». Репозиторий и его оператор также должны быть созданы к 2025 году.

♦ **доверенные репозитории** для создания и развития критически важных информационных систем государственного и военного назначения с грифом от уровня конфиденциально и ДСП до уровня гостайна (типа *forge.mil*).

В Российской Федерации действует Межведомственная концепция создания доверенной программно-аппаратной среды для автоматизированных систем управления (АСУ) органов военного и государственного управления (ОВГУ), которая определяет основные научно-технические и организационные принципы создания доверенной программно-аппаратной среды для АСУ органов военного и государственного управления, обеспечивающей информационную безопасность и технологическую независимость АСУ ОВГУ. Концепция разработана в соответствии с протокольным решением заседания научно-технического совета Военно-промышленной комиссии при Правительстве Российской Федерации по проблемным научно-техническим вопросам формирования отечественной доверенной аппаратно-программной среды для АСУ органов военного и государственного управления от 4 октября 2011 г. Такого типа репозитория в России пока нет.

В конце декабря 2019 года состоялось заседание секции научного совета при Совете Безопасности Российской Федерации, которая поддержала предложение Минпромторга России и заинтересованных организаций о необходимости создания отечественного репозитория (доверенного государственного фонда алгоритмов и программ).

Советом Безопасности России в Минцифры России были направлены ряд писем с предло-

жением подготовить и внести в установленном порядке в Правительство Российской Федерации проект постановления по конкретному решению ведения доверенного государственного Репозитория на базе государственных предприятий МНИИ «Интеграл» и НИИ «Восход» с учетом опыта Минобороны. Очередным решением Совета Безопасности от 15 ноября 2021 года рекомендовано Минцифры с участием Минпромторга, ФСБ, ФСТЭК, ГК «РОСТЕХ», других заинтересованных федеральных органов исполнительной власти и организаций — «до 1 июня 2022 года, ...представить в Правительство Российской Федерации предложения по внесению изменений в федеральный проект «Цифровые технологии» национального проекта «Цифровая экономика Российской Федерации», необходимости создания находящихся в юрисдикции России отечественных доверенных репозитория».

Как видим, работа на федеральном уровне идет, но пока безрезультатно. Понятия системы отечественных репозитория пока не встречались, отдельные инициативы находятся на этапе разработки. Автору этой статьи, как и уважаемым читателям, хотелось бы увидеть уже выполненное решение Совета Безопасности от 15 ноября 2021 года с учетом новой реальности и новых указов Президента России «О мерах по технологической независимости и безопасности КИИ РФ» — № 166 от 30 марта 2022 года и «О Межведомственной комиссии Совета Безопасности по вопросам обеспечения технологического суверенитета РФ в сфере КИИ» — № 203 от 14 апреля 2022 года.

Из вышесказанного уже давно понятна актуальность и жгучая необходимость иметь на федеральном уровне репозитории не только отдельных крупных и мелких мероприятий

Роман МЫЛИЦЫН

начальник отдела перспективных исследований и специальных проектов ГК «Астра»

КОД ПОД КОНТРОЛЕМ

Аккумуляция разработок программного обеспечения на отечественных площадках с использованием российских репозитория позволяет существенно увеличить технологическую независимость и усилить её в будущем.

В этой связи, развитие инфраструктуры российских репозитория и её активное использование сообществом разработчиков, безусловно, имеет важное значение для развития всей отрасли информационных технологий в нашей стране.

При этом, опыт крупнейших репозитория уже показал, что в современных условиях, когда объем исходного кода и вносимых в него изменений растет лавинообразно, а переиспользование кода без его детального изучения становится повсеместным, резко возрастает необходимость в средствах анализа и контроля состояния исходного кода.

Поэтому в ГК «Астра» при разработке ОС Astra Linux Special Edition создан так называемый «Стенд доверия», на котором проводятся непрерывные исследования средствами статического и динамического анализа хранящегося в репозитории исходного кода этой ОС, в особенности кода ее механизмов защиты. При этом результаты такого анализа помещаются в «Базу данных доверия» для дальнейшей аналитической обработки специалистами и оперативного устранения выявленных ошибок.

Подобный подход позволяет взять под контроль качество исходного кода, видеть полную картину его состояния и в целом внести вклад в безопасную разработку и обеспечение доверия к ОС Astra Linux Special Edition, а также развиваемому для неё российскому репозиторию пакетов.

«Цифровой экономики» со средствами обеспечения жизненного цикла, соответствующей базой знаний, которые системно взаимоувязаны с предоставляемыми государством льготами, субсидиями и тому подобными мерами поддержки отрасли микроэлектроники и программной инженерии как это сделано в ряде стран. Современные среды разработок — репозитории должны быть базовыми технологическими платформами национальной программы Цифровой экономики и других национальных проектов в области образования и науки, обеспечивать современные технологии программирования, реальное тестирование и последующую поддержку жизненного цикла программного обеспечения и аппаратных решений до уровня ПРОДУКТОВ с целью подтверждения качества и защиты прав потребителей, способствовать успешному внедрению существующих лучших отечественных программных продуктов внутри страны и их экспорту.

Репозитории необходимы не только для ГОСТЕХ (D6.10.32, 44,27 млрд в 2021–2024 гг.), но и для десятков других крупных и мелких мероприятий программы Цифровой экономики, например, D6.11.01, 52,76 млрд в 2021–2024 гг., D6.10.93, 30,14 млрд в 2021–2024 гг., D6.10.07, 21,03 млрд в 2021–2024 гг., D4.05.90, 0,28 млрд в 2021–2024 гг., D5.09.28, 0,4 млрд в 2021–2024 гг. (из Паспорта мероприятий программы Цифровой экономики).

Как показала реальная жизнь, согласованную межведомственную концепцию отечественной системы репозитория и отдельное мероприятие по системе отечественных репозитория в федеральном проекте «Цифровые технологии» национального проекта «Цифровая экономика» оказалось невозможно разработать и обосновать, быстро согласовать без соответствующего статуса рабочей группы с последующим долговременным межведомственным научно-техническим сопровождением и их контролем на уровне Координационного центра Правительства или на уровне Совета безопасности.

И в такой рабочей группе особо заинтересованными организациями могли бы стать сам Банк России и системообразующие российские банки, и финансовые организации, для которых «отчетность по импортозамещению» перешла бы в реально работающие проекты.

Для кредитно-финансовой сферы остается и другой путь создания собственной доверенной системы репозитория. Путь по аналогии с решениями Национального Банка Белоруссии и ЕРИП Белоруссии. Надеюсь, читателям этот путь известен и нет необходимости его повторять.

«Дорогу осилит идущий...». Пока в практическом решении проблем отечественной системы репозитория программного обеспечения на федеральном уровне наблюдается «бег на месте» уже которые годы.

Андрей КУРИЛО

советник по вопросам ИБ ФБК и FBK CyberSecurity

ВОПРОС ГОРАЗДО ШИРЕ!

Поставленный вопрос актуален, тесно связан с общей задачей создания некой индустрии, производящей качественное отечественное ПО, и к сожалению, весьма запутан. В результате на практике, на фоне отдельных успехов фирм и организаций, занимающихся разработкой ПО, мы фактически не наблюдаем явного, заметного роста этой индустрии. Это происходит на фоне болезненных санкционных ограничений, сделавших недоступными или токсичными значительное количество зарубежного софта, порой крайне нужного. Ситуация развивается дальше, и уже Президент своим указом практически запрещает использовать, начиная с 2025 года средства защиты информации (надо понимать — как аппаратные, так и программные средства), странами происхождения которых являются иностранные государства, совершающие в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия, либо производителями которых являются организации, находящиеся под юрисдикцией таких иностранных государств, прямо или косвенно подконтрольные им либо аффилированные с ними. Надо полагать, что под эту категорию подпадет некоторое системное или прикладное ПО, например, операционные системы, практически все имеющиеся встроенные средства защиты. Так в чем же дело? Только в отсутствии системы репозитория?

Думаю, что вопрос гораздо шире. В стране не создана система разработки, тестирования, хранения, распространения

и поддержки качественного (надежного и безопасного) отечественного ПО, которая представляла бы собой, как сейчас говорят, «экосистему», работа в которой была бы привлекательна для всех участников процесса:

- ◆ Разработчиков средств разработки,
- ◆ Разработчиков ПО;
- ◆ Тестировщиков (функциональное тестирование и тестирование по требованиям безопасности);
- ◆ Репозитория различного уровня;
- ◆ Национальных реестров ПО;
- ◆ Пользователей.

Определенная база документов технического регулирования для начала решения этой системной задачи есть. Создание самой системы заключается в разработке обязывающих правил работы и регламентов взаимодействия участников этого процесса, приложении организационных усилий, правильного и целевого финансирования. А эта задача абсолютно стандартная и понятная.

Таким образом, вопрос решаем, однако он требует, по нашему мнению, подготовки, в первую очередь, постановления Правительства РФ, регламентирующего отношения и взаимодействие всех участников, так как только на этом уровне возможно объединить усилия ряда различных организаций и ведомств и реально запустить процесс создания качественного отечественного ПО.



Александр ДОЛБНЕВ
руководитель по работе
с финансовым сектором
Yandex Cloud



Андрей ИВАНОВ
руководитель направления
по развитию Cloud Security
Yandex Cloud

ОБЛАКА В ПЕЙЗАЖЕ

КАК БАНКУ ВЫБРАТЬ БЕЗОПАСНОГО ОБЛАЧНОГО ПРОВАЙДЕРА?

Сегодня важными факторами сохранения лидерских позиций банка становятся гибкость и скорость реакции ИТ-инфраструктуры на запросы бизнеса. Облака позволяют банкам использовать технические инновации, быстро запускать новые продукты и масштабировать существующие сервисы. По данным исследования Data Bridge, среднегодовой рост мирового рынка облачных технологий в финансовом секторе с 2021 по 2028 годы составит 25%. И это неудивительно: 9 из 10 финансовых организаций в мире уже используют облака или планируют начать

первые проекты в них в ближайшие полгода, говорит отчёт CSA.

По данным исследования IDC, банковский сектор в России является самым ёмким по потреблению облачных сервисов на горизонте до 2025 года. Однако не все банки готовы к переезду, а некоторые игроки рынка всё ещё настороженно относятся к облачным технологиям. Основные причины — требования информационной безопасности на фоне действующего законодательства и, как следствие, не до конца сформировавшаяся практика и критерии выбора безопасного облака.



ЗАЧЕМ БАНКАМ ОБЛАКА?

Прежде всего облака позволяют банкам улучшать показатель time-to-market. Кстати, самый распространённый сценарий применения облака в банках — перенос тестовых сред и сред разработки. При реализации этого сценария в облако не передаются персональные и другие чувствительные данные, поэтому финансовым организациям достаточно следовать внутренним регламентам по защите информации.

Перенос в облако фронтальных систем и веб-сайтов — ещё один популярный сценарий. Он позволяет динамически масштабировать

Самый распространённый сценарий применения облака в банках — перенос тестовых сред и сред разработки. При реализации этого сценария в облако не передаются персональные и другие чувствительные данные

инфраструктуру с учётом меняющейся пользовательской нагрузки. Банк не переплачивает за простаивающие мощности и при этом обеспечивает необходимую доступность клиентского сервиса.

Облака также помогают банкам при переходе от монолита к микросервисам, что позволяет запускать на облачных мощностях отдельные продукты. Например, банк «Санкт-Петербург» не только создал в облаке среды разработки и тестовые среды, но и разместил сайт и приложение системы офферинга. В итоге показатель time-to-market вырос в 5 раз, экономия на инфраструктуре отдельных проектов составила 30%, а инвестиции в неё распределились на 3 года.

В целом облачные технологии в банковской отрасли позволяют:

- ◆ масштабировать бизнес, сохраняя высокую доступность;
- ◆ быстрее тестировать гипотезы, экспериментировать и проводить пилоты;
- ◆ эффективнее выстраивать разработку и тестирование новых продуктов;
- ◆ прозрачно планировать затраты на ИТ по проектам;
- ◆ привлекать лучших ИТ-специалистов.

РЕГУЛЯТОРНЫЕ ТРЕБОВАНИЯ И СУЩЕСТВУЮЩИЕ БАРЬЕРЫ

При реализации любых облачных сценариев в банках необходимо согласовывать проекты со службой информационной безопасности. Даже если это разработка MVP нового продукта на тестовых данных или вынос тестовых сред в облака, всё равно необходимо учитывать требования ЦБ к обеспечению информационной безопасности.

При переносе в облака систем, обрабатывающих персональные данные, требуется обеспечить соблюдение 152-ФЗ и соответствующих внутренних положений банка. Но наиболее сложный вопрос — передача банковской тайны поставщикам облачных услуг. Думаем, что в дальнейшем могут появиться уточнения в законодательстве и стандартизированные требования к обеспечению безопасности для облачных

провайдеров, что позволит сократить существующие «серые зоны». В настоящее время на площадке Ассоциации Финтех готовятся предложения по этим вопросам.

Помимо регуляторных требований, сдерживать переход в облака могут и некоторые внутренние факторы:

- ♦ отсутствие внутренних политик и регламентов по применению облачных технологий на стыке информационной безопасности, ИТ и управления рисками с учётом «серых зон» существующей нормативной базы;
- ♦ недостаточная техническая экспертиза и опыт работы с облаками;
- ♦ неготовность существующих процессов по подготовке, согласованию архитектурных решений и последующей эксплуатации сервисов банка в облаке;
- ♦ непрозрачность для банков процессов и мер по обеспечению ИБ на стороне облачных провайдеров. Из-за чего могут возникать барьеры даже там, где уже есть решения и выработаны практики.

При этом существует множество сценариев и задач, которые банки могут решать в облаке уже сейчас. Для этого необходимо учитывать требования к информационной безопасности финансовых организаций. К таковым можно отнести СТО Банка России «Обеспечение информационной безопасности организаций банковской системы РФ», СТО Банка России «Управление риском нарушения информационной безопасности при аутсорсинге» и ГОСТ 57580.

Банку остаётся оценить риски использования облаков как один из элементов операционного риска и сформулировать свои требования к безопасному облачному провайдеру.

КАК ВЫБРАТЬ БЕЗОПАСНОЕ ОБЛАКО?

При выборе облачных провайдеров следует обращать внимание на их соответствие существующей и, по возможности, перспективной нормативной базе.

В первую очередь провайдер должен пройти оценку уровня соответствия по ГОСТ 57580. Необходимо учитывать, что Положение Банка

России от 17 апреля 2019 г. № 683-П требует, чтобы кредитные организации обеспечивали уровень соответствия ГОСТ 57580 не ниже третьего, а с 1 января 2023 года — не ниже четвёртого уровня. Поэтому отдавать предпочтение стоит облачным провайдерам с четвёртым уровнем соответствия ГОСТ 57580 и обращать внимание на степень соответствия требованиям пятого уровня.

Безусловно, на критерии безопасности при выборе облака сильно влияют специфика задач и состав обрабатываемых данных. Но в большинстве случаев следует обращать внимание на следующие моменты:

1. Соответствует ли провайдер требованиям действующего законодательства, регулятора и промышленным стандартам, в частности ФЗ-152, ГОСТ 57580, PCI. Важно обращать внимание не только на сам факт наличия аттестата, но и на детали, указанные в заключении. Например, на состав сервисов, которые прошли аттестацию. Соответствие данным нормам и стандартам на стороне провайдера позволит финансовой организации обеспечить соответствие своей системы, размещённой в облаке.

2. Соответствие стандартам, свидетельствующим о зрелости внутренних процессов облачной платформы. Например, наличие сертификатов соответствия ISO 27001, 27017 и 27018 показывает, что у провайдера налажены процессы обеспечения информационной безопасности, и наличие этих сертификатов у провайдера полезно для клиента облака с точки зрения оценки рисков его использования.

3. Наличие у провайдера инструкций и практик по вопросу разделения ответственности за обеспечение безопасности между клиентом и облачной платформой. Без этого достаточно сложно и долго можно будет заниматься аттестацией по ФЗ-152 или ГОСТ 57580 конечных сервисов или систем банка в облаке.

4. Обеспечение безопасности на всех этапах создания и предоставления облачных сервисов и соблюдение процессов безопасной разработки Security Development Lifecycle.

5. Открытость и прозрачность коммуникаций. Зрелые провайдеры не скрывают информацию об инцидентах и делятся данными о каждом случае на своём сайте, разбирают их причины и сообщают о предпринятых действиях.

6. Локализацию и полноту контроля над облачной платформой: наличие собственных ЦОД, организацию физической безопасности, долю облачных сервисов собственной разработки и их включение в Единый реестр российских программ для ЭВМ и БД.

При моделировании угроз для систем и данных, размещённых в облаке, необходимо учитывать важную особенность: более размытый сетевой периметр, чем в инфраструктуре собственного ЦОДа

ПРАКТИЧЕСКИЕ ВОПРОСЫ БЕЗОПАСНОСТИ

Помимо соответствия законодательным требованиям и сертификатам деятельности облачного провайдера, на практике необходимо, чтобы у финансовой организации была разработана политика информационной безопасности. В банках должны существовать чёткие регламенты, в которых прописано, что может храниться в облаке и какие возможности существуют у сотрудников (служба ИБ, администраторы, архитекторы, финансисты, аналитики).

При моделировании угроз для систем и данных, размещённых в облаке, необходимо учитывать важную особенность: более размытый сетевой периметр, чем в инфраструктуре собственного ЦОДа. О размытости корпоративного периметра рассуждают уже не первый год. С приходом мобильности и удалённой работы стена файрволов на границах корпоративной сети уже не столь эффективно помогает защищаться от различных угроз, поэтому и стал набирать популярность подход Defense in Depth. Он организован таким образом, что одной угрозе противостоит набор средств защиты на разных уровнях. В условиях использования облачных сервисов размытость периметра увеличивается. Поэтому очень важно понимать и уметь применять на практике различные инструменты защиты данных, обрабатываемых в том или ином сервисе облака.

Для того чтобы снизить риски при управлении доступом к данным в банках, необходимо соблюдать простые правила.

- ♦ Администратор и любые привилегированные пользователи в облаке должны использовать многофакторную аутентификацию.

- ♦ Принцип минимальных привилегий. Доступы у сотрудников должны быть только к тем сервисам, которые необходимы им для работы.

- ♦ При расширении состава используемых облачных сервисов необходимо помнить, что любой дополнительный компонент в облаке может стать причиной уязвимости остальных. Поэтому нужно регламентировать процесс принятия решений об использовании новых инструментов или запуске новых облачных сервисов.

- ♦ Централизованное управление пользователями. Система управления доступа в облаке должна быть связана с корпоративной системой управления учётными записями и доступом. Такой подход упрощает контроль доступа при увольнении или переходе работника в другой отдел.

Если обобщать, то важно не забыть «растянуть» существующие процессы обеспечения безопасности и соответствующие технические меры на облачные ресурсы и процессы. Кроме

того, существует ряд технических решений и практик, обеспечивающих дополнительную защиту ваших систем.

- ♦ Логическая и сетевая сегментация ресурсов облака. Помогает более гранулярно управлять правами и снижать влияние различных подсистем друг на друга.

- ♦ Хорошо знакомая практика использования бастioned (или jump-серверов) при доступе к виртуальным машинам по SSH или RDP.

- ♦ Правильное использование доступных в облачной платформе ролей и полномочий для реализации принципа минимальных привилегий.

- ♦ Продумать защиту от DDoS с помощью инструментов провайдера или внешних сервисов.

- ♦ Шифрование данных. Зрелые облачные провайдеры предоставляют возможность шифровать данные ключом провайдера. Также можно использовать дополнительное шифрование ключом клиента или шифрование на уровне конечных приложений.

- ♦ Организация мониторинга и анализа аудиторских логов облачных ресурсов. При использовании облаков часть логов можно собирать привычным способом, например с агентов, установленных на виртуальных машинах. Но также стоит помнить, что облачная платформа также предоставляет аудиторские логи по активностям, связанным с ресурсами платформы. Эти логи целесообразно подвергать мониторингу и различным корреляциям для своевременного выявления подозрительных активностей на уровне управления облачными ресурсами.

Польза применения облачных технологий для банков очевидна, поэтому всё больше финансовых организаций будет переезжать в облака по мере развития законодательной и нормативной базы. Выстраивание внутренних процессов банка по безопасному применению облаков требует времени и может приводить к организационным изменениям и созданию облачных центров компетенции. Для крупных и средних банков полный цикл безопасного внедрения системы банка в облаке может занимать от 6 месяцев и более. Важно при этом рассматривать облако не как замещение инфраструктуры в контуре банка, а как органичное продолжение существующего ИТ-ландшафта. Использование облаков позволит банкам быстрее адаптировать бизнес к новым вызовам. Поэтому те банки, которые раньше остальных начнут движение в облака, получат преимущество перед более консервативными игроками финансового сектора.



Юрий КАРДЮКОВ
руководитель группы
финтех-решений
и информационной
безопасности
компания eKassir

ЗАЧЕМ БАНКАМ ПОДКЛЮЧАТЬСЯ К ОТКРЫТЫМ API?

БУДУЩЕЕ ДАВНО ПРИШЛО

Концепция Открытого банкинга предполагает, что игроки финансового сектора — банки, финтехи, страховые компании и МФО, а также технологические компании — получают равный доступ к пользовательским данным. «Общение» в среде Открытого банкинга происходит посредством универсального языка, которым являются открытые API.

Мы в компании eKassir создаём программное обеспечение для банков и других финансовых организаций. Инструментарий Открытого банкинга входит в поле наших компетенций, поэтому мы хотели бы рассказать, как создаётся среда Открытого банкинга в России; зачем банкам и финтехам к ней подключаться?

Взаимодействие через открытые API развивает конкуренцию и даёт равные возможности для всех участников цифрового финансового рынка по созданию новых продуктов и сервисов. Кроме того, Открытый бандинг позволяет клиентам управлять своими данными и получать персонализированные услуги.

ЭТО ПРОЕКТ, НО СТАНДАРТЫ ЕСТЬ

Проект по созданию среды Открытого банкинга реализуется на площадке Ассоциации ФинТех, объединения крупных банков, страховых и технологических компаний. В 2021 году был запущен стенд, на котором участники рынка могут пройти проверку на соответствие стандартам, а также информационный портал, где собрана актуальная информация по проектам Открытого банкинга.

В Российской Федерации в настоящий момент действуют следующие рекомендательные стандарты открытых API:

- ♦ Открытые банковские интерфейсы. Общие положения;
- ♦ Открытые банковские интерфейсы. Получение информации о счёте клиента третьей стороной;
- ♦ Открытые банковские интерфейсы. Иницирование перевода денежных средств

клиента третьей стороной в валюте Российской Федерации;

- ♦ Стандарт Банка России СТО БР ФАПИ. СЕК-1.6–2021 «Безопасность финансовых (банковских) операций. Прикладные программные интерфейсы обеспечения безопасности финансовых сервисов на основе протокола OpenID. Требования Financial-grade API Security. Requirements»;

- ♦ Открытые банковские интерфейсы. Получение публичной информации о банке и его продукте;

- ♦ Стандарт Банка России СТО БР ФАПИ. ПАОК-1.0–2021 «Безопасность финансовых (банковских) операций. Прикладные программные интерфейсы. Обеспечение безопасности финансовых сервисов при инициации OpenID Connect клиентом потока аутентификации по отдельному каналу. Требования».

К настоящему времени разработали API в соответствии со стандартами и вошли в Реестр доверенных участников среды Открытых банковских интерфейсов — банки «Синара» (бывший СКБ-банк), «Точка» и «Промсвязьбанк». Также был реализован первый пилот — передача информации о счетах и транзакциях клиента — юридического лица в процессе онлайн-кредитования. К проектам доверенной среды Открытого банкинга подключаются и другие финансовые организации.

КАКИЕ ПРЕИМУЩЕСТВА?

В среде открытых API клиенты самостоятельно решают, какой информацией, с какими компаниями и на какой срок они хотят поделиться. При этом на любом этапе клиент может отозвать согласие на использование данных.

Для пользователей финансовых услуг Открытого банкинга это сродни освобождению от «мобильного рабства», когда абонентам сотовых сетей разрешили переходить к другому оператору, сохраняя при этом личный номер телефона.

Клиенты финансовых организаций получают возможность поменять приложение, предлагае-

мое одним банком, на любое другое, технически более удобное или предоставляющее интересные условия. Например, пользователь сможет использовать одно приложение для управления всеми своими счетами.

У каждого финтеха и банка есть собственные API, представляющие известную сложность в том случае, когда требуется интегрировать сторонний сервис в банковскую инфраструктуру. Использование открытых API подразумевает, что всё взаимодействие проходит по унифицированным стандартам. Единые правила обмена данными определяют модели данных, формат сообщений, передаваемых участниками, и способы обеспечения информационной безопасности внутри среды Открытого банкинга.

ПРО ФИНТЕХ-КОМПАНИИ

Финтех-компании — очевидные бенефициары внедрения открытых API. Перечислим преимущества, которые они получают, становясь участниками доверенной среды открытых банковских интерфейсов.

- ◆ Доступ к данным клиентов от крупнейших игроков финансового рынка — от банков. Обладая подобным массивом информации, финтехи способны создать более клиентоориентированное программное обеспечение с продолжительным жизненным циклом.

- ◆ Финтехи могут отказаться от необходимости содержать собственный транзакционный бэк-офис, а также снимают часть ограничений и временных лимитов при выводе нового продукта на рынок.

- ◆ Стандартизация программных интерфейсов избавляет финтехи от необходимости настраивать и кастомизировать сервис под каждого нового партнёра.

- ◆ Используя стандартизированные правила обмена данными через открытые API, разработчики финансовых сервисов получают возможность проектировать и реализовывать решения, которые можно будет интегрировать в приложения, в том числе супераппы, различные кредитные организации и прочих участников рынка без необходимости вносить значительные модификации.

ЗАЧЕМ ЭТО БАНКАМ?

Потребители уходят в онлайн, и, чтобы не потерять старых и приумножить число новых клиентов, банки должны следовать за ними. И речь не только о классических каналах дистанционного банковского обслуживания (мобильный и интернет-банки), а о радикальной смене концепции взаимодействия с клиентами.



Не нужно ждать, пока клиент придёт в банк (в отделение / на сайт / откроет мобильное приложение), но следует предлагать свои услуги там и тогда, где это удобно потребителю. Пример — Ozon Банк, который предлагает оформить кредит на покупку прямо на маркетплейсе Ozon.

БУДУЩЕЕ ДАВНО ПРИШЛО

По данным лаборатории Касперского, до пандемии коронавируса около 70% зумеров (молодых людей, родившихся в двухтысячные) почти постоянно пребывало в сети. Отчёт Ernst&Young показывает, что более четверти миллениалов (людей 25–40 лет) в течение полугода используют как минимум два цифровых финтех-сервиса. Согласно данным Forbes, миллениалы и входящие в платёжный возраст зумеры будут главным драйвером спроса на банковские продукты в этом десятилетии. Практически 80% молодых людей пользуются мобильным банкингом, открывают счета и берут кредиты.

Данные о массовой миграции финансовых услуг в виртуальные среды подтверждает исследование Juniper Research, согласно которому

ожидается, что к 2025 году более 4 млрд жителей планеты будут использовать цифровые кошельки, дистанционно предоставляемые платёжные сервисы и, таким образом, минимум раз в сутки станут совершать финансовые операции онлайн.

Системы электронной коммуникации непрерывно развиваются, а вслед за ними к внедрению новых каналов взаимодействия подключаются и банки. Среда открытых API — не о будущем: это актуальная нашему времени цифровая трансформация финансового сектора.

Чтобы ответить на вопрос «Зачем банкам открытые API?», достаточно обратиться к опыту бигтех-компаний, таких как Microsoft, Google, Apple и Amazon. Эти технологические гиганты фактически оплели мир невидимыми сетями и присутствуют повсюду онлайн. Они предоставляют различные сервисы, которые их партнёры реализуют посредством API. В свою очередь, сами партнёры разрабатывают приложения, с помощью которых их клиенты могут пользоваться сервисами бигтехов.

И СНОВА О ПРЕИМУЩЕСТВАХ

Рассмотрим основные преимущества, которые получает банк, присоединяясь к доверенной среде открытых банковских интерфейсов.

♦ **Повышение лояльности клиентов за счёт удобства пользования услугами.** Кейс «Промсвязьбанка» и «Точки» показывает, что одним из существенных плюсов от вхождения в среду Открытого банкинга для кредитных организаций является ощутимое улучшение клиентского опыта. Клиенту банка, использующего открытые API, не нужно заниматься сбором документов, передавать выписки и заявки из одного банка в другой. Вся информация о клиенте передаётся между банками напрямую, быстро и удобно.

♦ **Повышение безопасности и надёжности передачи данных.** Сама технология открытых API подразумевает, что банки передают финансовые сообщения напрямую друг другу по защищённому каналу, то есть снимается угроза того, что личная информация клиентов утечёт «на сторону». Кроме того, исключается участие человека в подготовке документов, то есть снижается вероятность ошибок в предоставленных данных.

♦ **Внедрение ощутимо большего количества современных цифровых сервисов.** Опыт бигтехов подсказывает, что, если банки хотят расширить бизнес-присутствие в онлайн-среде, они должны предоставлять свои цифровые продукты партнёрам за счёт набора API. Банки идут на наращивание клиентских услуг, чтобы

удовлетворить запросы потребителей, однако здесь есть существенная сложность, которая ограничивает возможности подключения финтех-сервисов. Немногие банки могут позволить себе одновременно подключить более двух-трёх сервисов: их обслуживание дорого, внедрение — ещё дороже, а работа с индивидуальными API снижает темпы и количество сторонних интеграций. Подключение к среде открытых API удешевляет работы по подключению новых клиентских сервисов.

♦ **Экономия на самостоятельной разработке.** Далеко не каждый банк обладает достаточными техническими компетенциями, чтобы своими силами реализовать взаимодействие со сторонними поставщиками. Это связано с тем, что высокопрофессиональные ИТ-специалисты, у которых достаточно опыта и навыков выполнить работы по обеспечению безопасности, являются штучным товаром, а их работа чрезвычайно высоко оплачивается. Открытые API во многом закрывают этот вопрос: инструменты среды созданы для максимального удобства финтех- и банков, даже не обладающих штатом высококлассных ИТ-специалистов.

♦ **Новые площадки для продаж продуктов банка.** Отдельный момент, на котором нужно остановиться при рассмотрении преимуществ среды открытых API для банков, — перспективы продвижения клиентских продуктов в новых каналах продаж. В конце 2021 года к пилотным проектам Открытого банкинга подключились финансовые маркетплейсы — Финуслуги Московской биржи и Сравни.ру. То есть финансовые сервисы не только готовы к самостоятельной активности в рамках доверенной среды открытых API, но и рассчитывают на совместную с банками разработку и продвижение новых финансовых продуктов.

Работая в рамках стандартов, зафиксированных регулятором среды открытых банковских интерфейсов, банки могут заметно оптимизировать и расширить собственную инфраструктуру. А значит, они начнут увеличивать прямые продажи через партнёров, которые предложат банковским клиентам самые современные программные решения. Конкурентным преимуществом в финансовом секторе становится клиентский опыт, и тот, кто предоставит потребителю наиболее удобный и релевантный продукт, станет поставщиком трендов в цифровом банковском обслуживании на ближайшие годы.

ЗАМЕЩЕНИЕ ГОРЫ

WINDOWS НЕЗАМЕНИМ, НО ЗАМЕНЯТЬ НАДО. КАК?

Традиционно банки ориентировались на лидеров мирового рынка и самые высокотехнологичные решения. Сейчас сложилась непростая ситуация: уход с рынка вендоров, отказ в техподдержке и обновлениях, с одной стороны; с другой стороны, как следствие этого возникли ограничения со стороны регулятора — объявлено о приостановке ряда сертификатов ФСТЭК России. При этом банковские системы оказались между двух огней. Рассмотрим варианты оперативного выхода из таких непростых и недружественных условий.

ЕЩЁ НЕ ОДИН ГОД...

Многие эксперты дают оценки, что в России более 90% ИС построены на продуктах семейства Windows.

Чаще всего сервис генерации и управления цифровыми сертификатами (сертификаты доступа, PKI-инфраструктура) базируется на Windows Active Directory (далее AD), глубоко интегрированным с AD центром сертификатов Microsoft Certification Authority. Широко используются веб-серверы IIS и базы данных Microsoft SQL или Oracle. Подавляющее количество приложений написано под Windows. Такая ситуация не является благоприятной для экстренной миграции на открытую платформу на базе ядра Linux, на которой базируется большинство отечественных решений.

Ещё не один год в период поэтапного перехода банковские ИС будут содержать два корпоративных домена — один под управлением сервера Windows и второй под управлением сервера Linux. Для увязывания и обеспечения непрерывности работы ИС нужны рабочие инструменты и плавный (так называемый «бесшовный») переход на платформу Linux.

Компания «Аладдин Р. Д.» в сотрудничестве с отечественными разработчиками операционных систем и баз данных уже несколько лет работает над комплексной экосистемой безопасных продуктов. Коллеги сфокусировались на импортозамещении AD и СУБД такими решениями, как Samba DC или FreeIPA (Astra Linux ALD Pro), СУБД Postgres Pro или Jatoba, при этом достаточно успешно решают задачи работоспособности сервисов и доступности информационных активов. Мы, взаимодействуя на

этапах проектирования и разработки российских дистрибутивов на Linux и отечественных СУБД, интегрируем в них наши компоненты ИБ. В настоящее время разработан уже целый пул продуктов и методик внедрения плавной бесшовной миграции всех ресурсов на отечественные «рельсы».

ЧЕМ ЗАМЕНИТЬ MICROSOFT CA?

Одна из основных задач при организации доверенной внутрикорпоративной среды — создание домена доверия, функционально не уступающего импортному, как правило, Microsoft.

В отличие от домена на базе Microsoft AD DS, в отечественных решениях для построения доменов нет встроенного центра сертификатов, такого как Microsoft CS. Разработчики компании «Аладдин Р.Д.» сосредоточились на замещении средств аутентификации, инфраструктуры PKI и организации единого входа (SSO). Эта работа велась на уровне проектирования и разработки решений, т.е. так же, как и у Microsoft, мы ставили задачу тесной интеграции служб организации домена и центра сертификации. В итоге разработали одно из возможных решений для импортозамещения — отечественный корпоративный центр выдачи и обслуживания сертификатов доступа Aladdin Enterprise Certificate Authority (Aladdin eCA), способный заменить импортный Microsoft CS.

Aladdin Enterprise Certificate Authority (Aladdin eCA) — сервер на базе отечественных ОС, обеспечивающий управление цифровыми сертификатами (ЦС) пользователей и техническими средствами информационной системы (выпуск, распространение, аннулирование, приостановка, возобновление).

Aladdin eCA, основанный на технологии открытых ключей (PKI), — это решение «из коробки», с которым легко разворачивать домены



Сергей ШАЛИМОВ
руководитель направления по работе с технологическими партнерами «Аладдин Р.Д.»

Одна из основных задач при организации доверенной внутрикорпоративной среды — создание домена доверия, функционально не уступающего импортному

безопасности и обслуживать цифровые сертификаты контроллеров доменов, серверов, сетевого оборудования и АРМ пользователей. Aladdin eCA глубоко интегрирован со службами глобальных каталогов, что позволяет обеспечить непрерывность и связанность сервисов при миграции.

Aladdin eCA может обеспечить замену Microsoft CA в корпоративных и государственных информационных системах. Он может применяться в ГИС до 1-го класса защищённости включительно, ИСПДн до 1-й категории включительно, на объектах КИИ до 1-й категории включительно, а также в АСУ ТП на критически важных объектах, потенциально опасных объектах до 1-го класса защищённости включительно.

ПРО ОТЕЧЕСТВЕННУЮ РКИ

В банковской сфере обслуживание клиентов тесно связано с удалённым доступом к информационным ресурсам, в котором применяется не менее чем двухфакторная усиленная аутентификация, а в расширенном пакете услуг — квалифицированная электронная подпись, строгая аутентификация с применением различных факторов аутентификации, в том числе и биометрических.

На рынке аутентификации наблюдается приостановка деятельности, а также не исключён и потенциальный уход с российского рынка ряда крупнейших западных вендоров (Vasco, Yubico, Thales, EMC и др.). Что можно использовать взамен?

Представим одно из возможных решений. Это отечественный продукт, разработанный «Аладдин Р. Д.», — высокопроизводительный сервер аутентификации JAS (JaCarta Authentication Server) с поддержкой как аппаратных OTP- и U2F-токенов, так и программных OTP/PUSH/SMS-аутентификаторов. JAS поддерживает генерацию программных OTP с помощью приложения на смартфоне, передачи через СМС или Push, а также поддерживает все известные «железные» токены-брелоки

с кнопкой или экраном для генерации OTP по стандартам RFC4226 (HOTP) и RFC6238 (TOTP), USB-токены, например JaCarta WebPass, любые U2F-токены, например JaCarta U2F из достаточно широкого семейства JaCarta.

JAS обеспечивает безопасный механизм передачи секрета для инициализации генератора OTP в приложении Aladdin 2FA, при этом позволяет работать и с любыми другими приложениями типа Google Authenticator, «Яндекс. Ключ» в стандартном режиме.

Основные преимущества JAS — это простота внедрения, поддержка самых распространённых прикладных сервисов, удобный и понятный личный кабинет для пользователя, универсальное мобильное приложение Aladdin 2FA.

Также JAS сертифицирован ФСТЭК России на соответствие уже новым требованиям на УД-4, что позволяет использовать его для защиты информации в ИСПДн до 1 уровня включительно и при создании автоматизированных ИС до класса защищённости 1Г включительно.

БЕЗОПАСНАЯ РАБОТА С БД

Безопасная работа с базой данных (БД) — это краеугольный камень безопасности любой ИС. В банковской сфере невозможно оставаться в современном состоянии, когда самые распространённые продукты MS SQL и Oracle оказались под прицелом недружественных отношений с вендорами, а утечка данных может стать невосполнимой потерей. Основная отечественная платформа замещения СУБД представлена продуктами PostgreSQL и PostgresPro.

Для защиты баз данных от возможных утечек при миграции с MS SQL и Oracle на отечественные СУБД используется система «Крипто БД». Даже если переезд, например, с Oracle невозможен, как в случае с большими базами данных, «Крипто БД» позволяет остаться на этой платформе, заменяя встроенные в Oracle средства защиты сертифицированными российскими. Система также изолирует обрабатываемые данные от самой СУБД, предотвращая их утечку.

«Крипто БД» поддерживает сразу несколько платформ баз данных, что позволяет защитить информацию в исходной СУБД (например, Oracle или MS SQL) и одновременно в новой, строящейся (например, Postgres Pro или PostgreSQL).

Защитные механизмы «Крипто БД» основаны на стойких отечественных криптоалгоритмах, в БД защищаются таблицы или отдельные столбцы, реализованы методы «прозрачного» шифрования. Продукт соответствует всем требованиям ФСБ России к СКЗИ, что подтверждено

На рынке аутентификации наблюдается приостановка деятельности, а также не исключён и потенциальный уход с российского рынка ряда крупнейших западных вендоров (Vasco, Yubico, Thales, EMC и др.). Что можно использовать взамен?

соответствующими заключениями ФСБ России по классам КС1, КС2 и КС3. Это позволяет системе защиты обеспечивать противодействие наиболее критичным угрозам — нарушению целостности и конфиденциальности информации. Чаще всего в банках это персональные данные сотрудников и клиентов.

Основные сценарии применения «Крипто БД» могут реализовать такие задачи, как защита конфиденциальной информации в СУБД при взломах информационных систем, предотвращение доступа со стороны привилегированных пользователей, разграничение прав доступа пользователей к защищаемой информации, маскирование и деперсонализация информации в СУБД, предотвращение возможности восстановления удалённой информации, аудит фактов доступа пользователей к защищаемой информации и другие.

ПРО БЕЗОПАСНОСТЬ РАБОЧИХ МЕСТ

Перевод автоматизированных рабочих мест (АРМ) сотрудников на отечественное ПО с использованием платформы Linux также сопряжён с вопросами информационной безопасности. Одно из возможных решений для данной задачи — клиентское ПО SecurLogon, которое позволяет добавить недостающие компоненты на клиентские ОС и автоматически сконфигурировать клиентские АРМ для задач единого входа в различных вариантах построения доменов — Samba DC, FreeIPA, Microsoft AD, что максимально соответствует политике сохранения разных доменов в период миграции.

Aladdin SecurLogon также позволяет реализовать двухфакторную аутентификацию в разных инфраструктурах, добавить аутентификацию по цифровым сертификатам в такие распространённые протоколы и сервисы, как SSH, RDP, почтовые клиенты, браузеры, подпись и доступ в СЭД. Для больших инсталляций остро стоит задача автоматической централизованной конфигурации клиентских АРМ, так как привычных групповых политик в Linux пока ещё нет. С помощью Aladdin SecurLogon можно автоматизировать настройку АРМ и организовать до 1000 АРМ за 20 минут.

ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ И ПЕРСОНАЛЬНЫХ ДАННЫХ

Для защиты данных на дисках в Windows многие используют встроенную функцию шифрования BitLocker, рискуя полностью потерять к ним доступ. Оперативно обезопасить информацию на дисках рабочих станций и серверов

Aladdin SecurLogon также позволяет реализовать двухфакторную аутентификацию в разных инфраструктурах, добавить аутентификацию по цифровым сертификатам в такие распространённые протоколы и сервисы, как SSH, RDP, почтовые клиенты, браузеры, подпись и доступ в СЭД

способны продукты линейки Secret Disk — система прозрачного шифрования данных для Windows и Linux. Эти отечественные разработки развиваются в течение всего периода действия программы импортозамещения. Основа ПО — крипто-ядро SD CE, сертифицированное ФСБ России (КС1, КС2), код механизмов защиты не содержит чужеродные включения.

Оперативная замена импортных средств шифрования отечественным Secret Disk для ОС Windows (Secret Disk 5) снимет остроту проблемы защиты данных, поскольку его внедрение занимает считанные минуты. Это позволит сохранить данные от утечки по техническим каналам встроенными механизмами Microsoft. В случае перехода на ОС на базе ядра Linux защиту обеспечит продукт Secret Disk Linux.

Новый продукт Secret Disk Linux поддерживает лидирующие отечественные ОС — Astra Linux SE 1.7, РЕД ОС 7.3 и 7.3.1. Он обеспечивает шифрование виртуальных дисков, прозрачное шифрование информации, двухфакторную аутентификацию пользователей на базе алгоритма ЭП ГОСТ Р 34.10–2018, разграничение прав доступа.

При таком способе перехода применяют единые технологии защиты в ОС Windows/Linux, что поддерживает бесшовную интеграцию разнородных систем и возможность использования единой системы управления в гетерогенной среде.

ЗАКЛЮЧЕНИЕ

Представленные в статье решения помогут оперативно организовать безопасную среду для корпоративной информационной системы, обеспечить переход на доверенные средства аутентификации, безопасную работу СУБД как отечественных, так и иностранных поставщиков, а также поэтапно осуществить бесшовный перевод пользователей на отечественные продукты, обеспечив надёжную защиту информации.

УЧИТЫВАТЬ ПРИ ВЫБОРЕ

ПОМОЩЬ ТЕОРИИ ПРИ ИМПОРТОЗАМЕЩЕНИИ СРЕДСТВ АУТЕНТИФИКАЦИИ



Алексей САБАНОВ

доктор технических наук, профессор кафедры защиты информации МГТУ им. Н.Э. Баумана, заместитель генерального директора АО «Аладдин Р.Д.»

В связи с приостановлением работы и ухода ряда крупных западных поставщиков средств аутентификации с российского рынка перед банками встала срочная задача быстрого выбора адекватного отечественного решения. В данной статье обсуждаются некоторые существенные проблемы, сопутствующие такому выбору, а также аспекты, которые надо учитывать в первую очередь, чтобы не потерять имеющийся уровень защищённости доступа к информационным ресурсам. Значительная часть изложенного ниже материала опирается на обзоры международных стандартов и зарубежной нормативной базы [1–3], основной международный стандарт по аутентификации [4], принятые национальные стандарты по идентификации и аутентификации [5–9] и находящиеся на разных стадиях принятия проекты стандартов, в которых аутентификация рассматривается с точки зрения уверенности в получаемых результатах. Также в статье используются основные положения научных статей, в которых рассмотрены наиболее используемые процессы [10] и методы формирования уровней доверия к результатам аутентификации [11], подробно исследованы методы двухфакторной аутентификации [12], выявлены риски идентификации [13,14] и аутентификации [15], рассмотрены национальные рекомендации по идентификации и аутентификации США [16] и Канады [17], а также сформированы качественные [18, 19] и количественные показатели уровня рисков ошибочной аутентификации [20].

НЕКОТОРЫЕ ПРОБЛЕМЫ ИМПОРТОЗАМЕЩЕНИЯ

О необходимости применения идентификации и аутентификации (ИА) указывается во многих федеральных законах и подзаконных актах, однако практически нигде не указано, КАК должна строиться система ИА. В работах [1–3] сделан вывод о том, что нормативная база в части регулирования ИА недостаточно развита, о чём можно судить по весьма скромному по полноте и качеству содержанию отечественной базы технических спецификаций (стандартов, методик, руководств), методов, протоколов и технологий ИА. В условиях нуждающейся в совершенствовании нормативно-правовой базы и

недостатка утверждённых методических рекомендаций уполномоченных органов выбор методов и средств ИА отдан на откуп владельцам или операторам ИС. В таких условиях для построения эффективных систем ИА одним из путей решения является опора на научную базу.

Интернет полон статей «специалистов» по ИА с подчас сомнительными советами по использованию средств ИА. Средний уровень (аналог «средней температуры по больнице») таких «советов» часто можно оценить как низкий.

Одной из традиционных задач безопасности является поиск компромисса между безопасностью и удобством пользователей. Зачастую в погоне за удобством теряется защищённость и обоснованность выбора методов и средств ИА.

Чтобы корректно решать указанные проблемы, углубимся в интенсивно развивающуюся теорию доверия к результатам аутентификации. Кратко рассмотрим общую теорию, виды и средства аутентификации, а также типовые ошибки при выборе вида и средств аутентификации.

ВИДЫ И СРЕДСТВА АУТЕНТИФИКАЦИИ

В соответствии с [5] при организации доступа должен использоваться один из видов аутентификации: простая, усиленная или строгая. При простой аутентификации применяется однофакторная односторонняя аутентификация с организацией передачи аутентификатора от субъекта доступа к объекту доступа. При усиленной аутентификации применяется многофакторная односторонняя аутентификация или многофакторная взаимная аутентификация с организацией обмена аутентификационной информацией между субъектом доступа и объектом доступа. При строгой аутентификации должна применяться многофакторная взаимная аутентификация с организацией двухстороннего, между субъектом доступа и объектом доступа, или многостороннего (при использовании третьей доверенной стороны) обмена аутентификационной информацией. В процессе перечисленных видов аутентификации должны использоваться криптографические протоколы аутентификации, соответствующие виду организации обмена сообщениями между участниками процесса аутентификации. При аутентификации могут использоваться следующие средства аутентификации:

♦ Запоминаемый секрет (например, пароль). При аутентификации с помощью данного средства аутентификации используется фактор знания — подтверждается знание секрета.

♦ Поисковый секрет (например, одноразовый пароль). Представляет собой физическую или электронную запись, в которой хранится совокупность секретов, формируемых для субъекта доступа регистрирующей стороной. При аутентификации с помощью данного средства аутентификации используется фактор владения (подтверждается обладание и контроль над аутентификатором).

♦ Внеполосный аутентификатор («второй канал», например смартфон). Представляет собой зарегистрированное устройство, которое является уникально адресуемым и может взаимодействовать с доверяющей стороной по отдельному каналу связи, называемому вторым каналом. При аутентификации с помощью данного средства аутентификации используется фактор владения (обладание и контроль над аутентификатором). Внеполосный аутентификатор, как правило, применяется совместно с другими аутентификаторами.

♦ Однофакторный генератор одноразовых паролей (ОТР — One Time Password). При аутентификации используется фактор владения (обладание и контроль над аутентификатором).

♦ Многофакторный генератор одноразовых паролей. Используется фактор владения (обладание и контроль над аутентификатором) совместно с фактором знания и/или с биометрическим фактором.

♦ Однофакторное криптографическое программное средство аутентификации. Представляет собой криптографические ключи и программу, осуществляющую криптографические операции, которые хранятся на носителе, входящем в состав средства вычислительной техники (СВТ) или аналогичного устройства. При аутентификации используется фактор владения (обладание и контроль над криптографическими ключами).

♦ Однофакторное криптографическое техническое средство аутентификации. Осуществляет хранение выработанных и/или импортированных в него криптографических ключей, а также выполняет криптографические операции с их использованием и представляет результаты через непосредственное соединение с СВТ. При аутентификации используется фактор владения (подтверждается обладание и контроль над криптографическими ключами).

♦ Многофакторное криптографическое программное средство аутентификации. Доступ к криптографическим ключам осуществляется с использованием второго фактора аутентификации, представляющего собой информацию,

полученную с клавиатуры СВТ (пароль, PIN-код и т.п.) или биометрического считывающего устройства. Используется фактор владения (обладание и контроль над криптографическими ключами) совместно с фактором знания и/или с биометрическим фактором.

♦ Многофакторное криптографическое техническое средство аутентификации. Устройство аутентификации осуществляет хранение самостоятельно выработанных и/или импортированных в него криптографических ключей, а также выполняет криптографические операции с их использованием. Доступ к криптографическим ключам и/или результатам криптографических операций осуществляется с использованием второго фактора аутентификации. Используется фактор владения (обладание и контроль над криптографическими ключами) совместно с фактором знания и/или с биометрическим фактором.

♦ Многофакторное криптографическое техническое средство аутентификации с неизвлекаемым ключом. Устройство аутентификации вырабатывает закрытые неизвлекаемые криптографические ключи, а также выполняет криптографические операции с их использованием и представляет результаты через непосредственное соединение с СВТ. Использование криптографических ключей и/или результатов криптографических операций осуществляется после активации второго фактора аутентификации. Используется фактор владения (обладание и контроль над криптографическими ключами) совместно с фактором знания и/или с биометрическим фактором.

УРОВНИ ДОВЕРИЯ

Уровень доверия аутентификации определяет достигнутую уверенность в том, что субъект доступа действительно является тем **зарегистрированным** субъектом доступа, за кого себя выдаёт предъявленным идентификатором. Уровень доверия аутентификации определяет необходимые к применению вид аутентификации и средства аутентификации. Устанавливаются три уровня доверия аутентификации: низкий уровень доверия (некоторая уверенность в том, что субъект доступа действительно является тем зарегистрированным субъектом, за кого себя выдаёт предъявленным идентификатором доступа), обеспечиваемый простой аутентификацией; средний уровень доверия (умеренная уверенность), обеспечиваемый усиленной аутентификацией; высокий уровень доверия (значительная уверенность в том, что субъект доступа действительно является зарегистрированным субъектом, за кого себя выдаёт предъявленным идентификатором), обеспечиваемый применением строгой

Уровень доверия аутентификации	Уверенность в результатах аутентификации	Необходимые		Допустимые	
		виды аутентификации	средства аутентификации	виды аутентификации	средства аутентификации
1	2	3	4	5	6
Низкий	Некоторая уверенность в том, что субъект доступа действительно является тем зарегистрированным субъектом доступа, за кого себя выдаёт предъявленным идентификатором доступа	Простая	Запоминаемый секрет, поисковый секрет, однофакторный генератор одноразовых паролей	Простая, усиленная, строгая	Многофакторный генератор ОТР, однофакторное криптографическое программное средство, однофакторное криптографическое техническое средство, многофакторное криптографическое программное средство, многофакторное криптографическое техническое средство, многофакторное криптографическое средство аутентификации с неизвлекаемым ключом
Средний	Умеренная уверенность в том, что субъект доступа действительно является тем зарегистрированным субъектом доступа, за кого себя выдаёт предъявленным идентификатором доступа	Усиленная	Многофакторный генератор ОТР или совместно с запоминаемым секретом должны использоваться поисковый секрет, или внеполосное устройство, или однофакторный генератор ОТР, или однофакторное криптографическое ПО аутентификации, или однофакторное криптографическое техническое средство аутентификации	Усиленная, строгая	Многофакторное криптографическое программное средство, многофакторное криптографическое техническое средство, многофакторное криптографическое средство аутентификации с неизвлекаемым ключом
Высокий	Высокая уверенность в том, что субъект доступа действительно является тем зарегистрированным субъектом доступа, за кого себя выдаёт предъявленным идентификатором доступа при условии, что субъект доступа знает, обладает и контролирует используемые средства аутентификации	Строгая	Многофакторное криптографическое техническое средство, или однофакторное криптографическое техническое средство совместно с запоминаемым секретом, или многофакторный генератор ОТР совместно с однофакторным криптографическим техническим средством, или однофакторный технический генератор ОТР совместно с многофакторным криптографическим программным средством, или однофакторный технический генератор ОТР совместно однофакторным криптографическим программным средством аутентификации и запоминаемым секретом	Строгая	Многофакторное криптографическое техническое средство аутентификации с неизвлекаемым ключом
Очень высокий	Максимальная уверенность в том, что субъект доступа действительно является тем зарегистрированным субъектом доступа, за кого себя выдаёт предъявленным идентификатором доступа	Строгая	Многофакторное криптографическое техническое средство аутентификации с неизвлекаемым ключом	–	–

Таблица 1. Уровни доверия аутентификации

аутентификации. Допускается использование строгой или усиленной аутентификации для обеспечения требуемого в конкретной среде функционирования низкого уровня доверия, а также использование строгой аутентификации для обеспечения требуемого среднего уровня доверия. Результаты такого рассмотрения сведены в таблицу 1.

Из анализа таблицы видно, что с низкого по высокий уровни доверия могут достигаться разными комбинациями видов и средств аутентификации, а очень высокий уровень доверия — с

применением только одного средства аутентификации с неизвлекаемым ключом. Согласно результатам работ [4, 13,15] выбор метода аутентификации должен определяться результатами анализа рисков доступа к конкретной транзакции или проникновения к информационному ресурсу злоумышленника под видом легального пользователя.

НЕКОТОРЫЕ ТИПОВЫЕ ОШИБКИ

К сожалению, в большинстве случаев двухфакторной аутентификацией (2ФА) часто называ-

ют совсем не те виды и средства аутентификации, которые были рассмотрены в предыдущем разделе. Так, последовательное (не одновременное) применение одного или различных однофакторных методов аутентификации не является 2ФА. Такая аутентификация согласно [5] называется многошаговой. Более того, надёжность такой аутентификации определяется надёжностью самого слабого звена. Типичным примером такой аутентификации является последовательная аутентификация сначала к СБТ, затем к компьютерной сети, затем к информационному ресурсу или прикладной программе. Защищённость такой последовательной аутентификации определяется защищённостью самого слабого шага. Например, если при этом на каждом шаге применяются пароли, то аутентификация является однофакторной, а оценка защищённости всей цепочки шагов определяется самым слабым паролем.

Второй наиболее распространённой в последнее время ошибкой является отнесение аутентификации к 2ФА при использовании двух или более биометрических характеристик (например, лицо и голос). Строго говоря, такой процесс должен называться не аутентификацией, а идентификацией. Статья 7.7 стандарта [5] говорит о том, что «применение фактора биометрического в качестве единственного фактора при однофакторной аутентификации не допускается», а в рассматриваемом случае дважды используется именно биометрический фактор.

Ещё одной ошибкой является отнесение аутентификации к 2ФА при использовании только вероятностных (не детерминированных) характеристик, примером которых является определение местоположения, имеющего погрешности обсервации, обусловленные точностью позиционирования. В качестве второго примера можно привести применение биометрии, характеристики которой всегда содержат ошибки первого и второго рода.

ЗАКЛЮЧЕНИЕ

Показано, что «результатирующая» уверенность в результатах аутентификации зависит не только от применяемого вида, но и от используемых при этом средств аутентификации. Существенную роль при этом играют методы и результаты первичной идентификации субъекта доступа, а также способ хранения секрета, используемого в качестве аутентификационной информации. Чем выше уровень доверия первичной идентификации, способ хранения секрета и применяемые вид и средства аутентификации, соответствующий данному уровню доверия, тем к более высокорисковым транзакциям можно допускать субъекта после успешной аутентификации. При этом уровне доверия всех трёх составляющих (первичная идентификация, вид и средства аутентификации, способ хранения секрета) должны соответствовать друг другу. Предлагается учитывать вышеизложенное при выборе импортозамещающих вида и средств аутентификации.

ЛИТЕРАТУРА

1. Кузьмин А. С., Сабанов А. Г. Анализ зарубежной нормативной базы по идентификации и аутентификации. Инженерный журнал: наука и инновации. 2013. Вып. 11 (23). С. 1–13.
2. Сабанов А. Г. Общий анализ международных стандартов по идентификации и аутентификации при доступе к информации. Часть 1 // Инсайд. Защита информации. 2016. № 2 (68). С. 84–87.
3. Сабанов А. Г. Общий анализ международных стандартов по идентификации и аутентификации при доступе к информации. Часть 2 // Инсайд. Защита информации. 2016. № 3. С. 70–74.
4. ISO/IEC 29115:2013 «Information technology — Security techniques — Entity authentication assurance framework» <https://www.iso.org/standard/45138.html>
5. ГОСТ Р 58833–2020 Защита информации. Идентификация и аутентификация. Общие положения. <https://docs.cntd.ru/document/1200172576>
6. ГОСТ Р 59383–2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом. <https://docs.cntd.ru/document/1200179662>
7. ГОСТ Р 59515–2021 Информационные технологии. Методы и средства обеспечения безопасности. Подтверждение идентичности. <https://docs.cntd.ru/document/1200179667>
8. ГОСТ Р 59381–2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 1. Терминология и концепции. <https://docs.cntd.ru/document/1200179660>
9. ГОСТ ISO/IEC 24760–2–2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 2. Базовая архитектура и требования. <https://docs.cntd.ru/document/1200180228>
10. Сабанов А. Г. Классификация процессов аутентификации // Вопросы защиты информации. 2013. № 3 С. 46–52.
11. Сабанов А. Г. Уровни доверия к результатам идентификации и аутентификации субъекта доступа в период цифровой трансформации // Вопросы кибербезопасности. 2019. № 5 (33). С. 19–25.
12. Сабанов А. Г. Методы двухфакторной аутентификации // Инсайд. Защита информации. 2021. № 6. С. 52–56.
13. Сабанов А. Г. Концепция предварительного анализа рисков первичной идентификации субъектов доступа // Инсайд. Защита информации. 2020. № 2. С. 74–79.
14. Сабанов А. Г., Шубинский И. Б. Метод анализа технологических рисков первичной идентификации субъектов доступа // Инсайд. Защита информации. 2020. № 3. С. 57–61.
15. Сабанов А. Г. О применимости методов управления рисками к процессам аутентификации при удалённом электронном взаимодействии // Электросвязь 2014. № 6. С. 39–42.
16. Paul A. Grassi, James L. Fenton, Elaine M. Newton and others. NIST Special Publication 800–63 — B. Authentication and Lifecycle Management. June 2017. <https://pages.nist.gov/800-63-3/sp800-63b.html>, <https://doi.org/10.6028/NIST.SP.800-63b>
17. Canada User Authentication Guidance for Information Technology Systems https://www.csecc.gc.ca/en/system/files/pdf_documents/itsp.30.031v3-eng_0.pdf
18. Сабанов А. Г. Уровни доверия к аутентификаторам // Вопросы защиты информации. 2019. № 2. С. 10–17.
19. Сабанов А. Г. Аутентификация и системы разграничения доступа: концепция оценки доверия к результатам // Инсайд. Защита информации. 2021. № 2. С. 10–17.
20. Жильев А. Е., Сабанов А. Г., Брагин Д. С., Шелупанова П. А., Мицель А. А., Катаев М. Ю. Подход к формированию уровней доверия для оценки рисков ошибок аутентификации // Вопросы защиты информации. 2022. № 1. С. 17–22.

«НАС НЕ ДОГОНЯТ!»?

АНТИФРОД-СИСТЕМЫ В БОРЬБЕ С КРЕДИТНЫМ МОШЕННИЧЕСТВОМ



Сергей ПАРФЁНОВ
технический директор
«Фаззи Лоджик Лабс»

По данным из открытых источников, в 2021 году удалось предотвратить кражу 24,2 млрд рублей кредитных средств клиентов. Рассказываем о новых разработках компании «Фаззи Лоджик Лабс» в области защиты от кредитного мошенничества с помощью антифрод-системы Smart Fraud Detection.

С ростом онлайн-технологий кредитования, когда пользователи могут получить заём удалённо в короткие сроки

через мобильный или интернет-банк, банки столкнулись не только с конкуренцией с другими финансовыми организациями, но и с большим разнообразием новых методов соинженерии и мошенничества в ДБО с кредитным функционалом. Если это не корпоративное мошенничество, в котором участвуют сотрудники организации, и банк готов выдать кредит по удалённому каналу, то банк обязан безошибочно идентифицировать клиента (рис. 1).

Сейчас банки часто используют антифрод-системы для идентификации клиента и больше времени уделяют проверке операций после получения кредита, фиксируют, если кредитные средства переводятся кому-то сразу после получения, и запускают дополнительные механизмы проверки в случае сомнительных операций. При этом кросс-канальные системы антифрода, несомненно, обладают большими преимуществами, так как мошенничество и вывод денежных средств происходят часто в разных каналах.

Преимущества применения антифрод-систем для защиты от мошенничества с кредитами:

- ♦ сбор пользовательской информации по всем каналам, включая мобильные приложения и интернет-банк;
- ♦ идентификация и сведения, состояние устройств, включая с мобильных приложений SDK;
- ♦ проверка по справочникам, «чёрным» и «белым» спискам;
- ♦ нормализованная оценка риска проведения финансовых операций методом правил и алгоритмами машинного обучения, расчёт параметров in-тему по внутрисистемным объектам.

В компании «Фаззи Лоджик Лабс», развивая кросс-канальную систему обнаружения и выявления мошеннических транзакций в режиме реального времени Smart Fraud Detection, мы разработали технологии, которые показали себя эффективными в выявлении мошенничества в кредитной сфере (рис. 2).

1. Технология для оценки поведенческих профилей. Функционал позволяет индивидуально настраивать собственные объекты хранения для расчёта данных о поведении. Например, по составному объекту

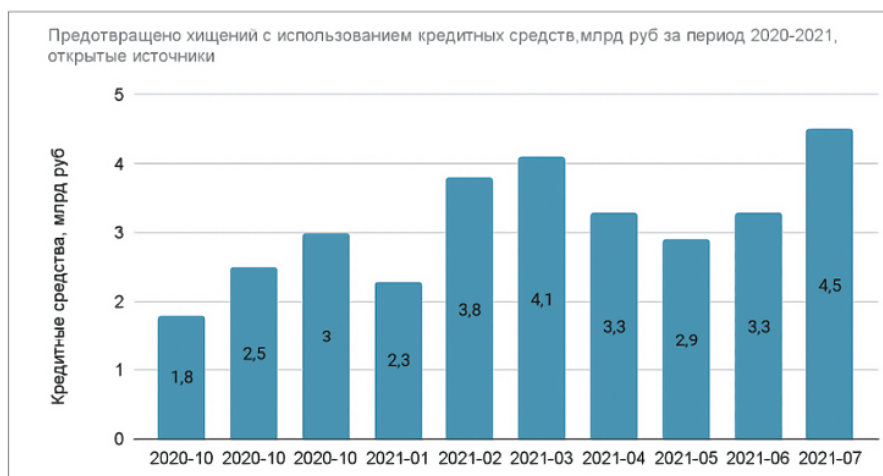


Рисунок 1. Данные по кредитному мошенничеству

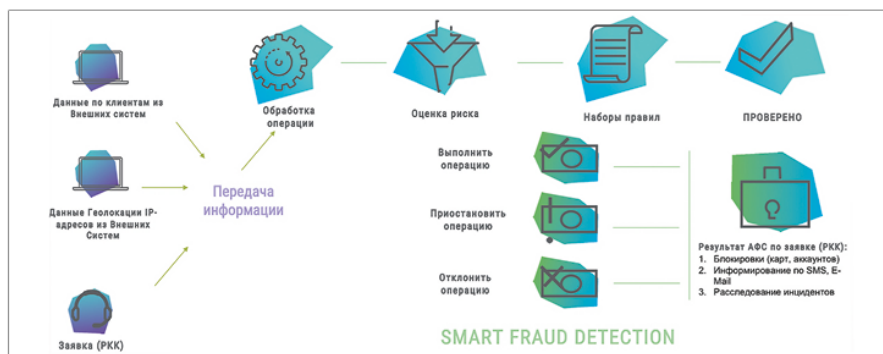


Рисунок 2. Схема работы Smart Fraud Detection при выявлении мошенничества с кредитами

типовые устройства, скорость перемещения по IP; проверяются платежи по реквизитам и устройствам известных мошеннических операций, проведённых в других банковских каналах.

* * *

Одной из основных задач любого банка является обнаружение мошенника как можно быстрее. Но если кредит уже выдан, то мошенников можно обнаружить и на ранних стадиях мониторинга антифрод-системами и службами безопасности банка.

Рисунок 4Б. Отслеживание повторяемости похожих номеров



Максим ПЯТАКОВ
заместитель
генерального
директора, CtrlHack



Владимир СОЛОВЬЁВ
руководитель направления
внедрения средств защиты
АО «ДиалогНаука»

РУССКИЙ ХАКЕР. БЕЛЫЙ ХАКЕР. РОБОТ-ХАКЕР

АВТОМАТИЧЕСКАЯ СИМУЛЯЦИЯ КИБЕРАТАК КАК ЧАСТЬ ЭФФЕКТИВНОЙ СИСТЕМЫ ЗАЩИТЫ

Сейчас большинство компаний, государственных предприятий и органов власти обеспокоены проблемой защиты от кибератак. В зависимости от текущего уровня защиты и понимания возможных последствий кибератак принимаются различные меры, направленные на повышение уровня защищённости до приемлемого уровня. При этом средства защиты компаний включают в себя большое количество различных продуктов, причём очень часто от разных вендоров. Для реагирования на более сложные атаки компании выстраивают свой SOC или подключают соответствующую услугу от сервис-провайдера. Расширяется штат сотрудников, отвечающих за настройку средств защиты, мониторинг и реагирование на инциденты. Но насколько эффективно работает вся эта система в целом и каждый из её компонентов? Действительно ли вероятность проведения успешной кибератаки снизилась или злоумышленник всё так же легко может проникнуть в сеть компании? Это общие вопросы, с которыми сталкиваются каждый день специалисты по информационной безопасности. Вопросов много, а возможностей получить ответ, подтверждённый фактами, не так много.

СПОСОБЫ ПРОВЕРКИ КИБЕРЗАЩИТЫ

Ответить на вопросы об эффективности системы киберзащиты можно, реализовав у себя в инфраструктуре симуляцию действий злоумышленников. Фактически это единственный способ определить, насколько вы реально защищены от кибератак. Много лет такие активности проводились в рамках выполнения тестов на проникновение (pentest). В последние годы в дополнение к тестированию на проникновение ряд компаний стал пользоваться услугами red team. В основе этих услуг лежит работа «белых» хакеров, которые используют различные техники и средства, полностью повторяющие действия реальных злоумышленников. Однако обе эти услуги имеют ряд недостатков. За время выполнения работ у команд нет возможности покрыть всю инфраструктуру, особенно если мы говорим об инфраструктурах из десятков тысяч узлов в сети. Команды могут отработать только часть векторов атак и хакерских техник. При этом такие работы практически никогда не выполняются на постоянной основе без перерывов. И результат сильно зависит от квалификации команды, которую не всегда возможно точно определить — человеческий фактор. Ко всему прочему, результаты проведённых тестирований на проникновение попадают в «чужие» руки, за пределы компании.

Таким образом, тестирование на проникновение и работа команд red team позволяют в некотором объёме оценить уровень реальной защищённости компании. Но этот результат не является полной оценкой, и в большинстве случаев компании могут позволить себе тестирование на проникновение раз в полгода или год. А в ситуации постоянного развития технологий и изменений в инфраструктуре нужно иметь возможность получать такую оценку на постоянной основе с максимальным покрытием различных атакующих техник и для всей инфраструктуры.

АВТОМАТИЧЕСКАЯ СИМУЛЯЦИЯ КИБЕРАТАК

Для решения таких задач на мировом рынке появились продукты, позволяющие в автоматическом режиме проводить симуляции кибератак во всей инфраструктуре. Позднее Gartner выделил такие решения в отдельный класс Breach and attack Simulation (BAS). Сейчас продукты данного класса представлены и на российском рынке. Решения класса BAS позволяют проводить проверки работы средств защиты, эффективности работы SOC, качества работы выстроенных процессов, а также работу персонала. То есть автоматически можно проверить все составляющие комплексной системы киберзащиты и при этом делать это на постоянной основе и не зависеть от внешних команд и уровня их компетенций.

Основным вектором проверки в рамках симуляций кибератак традиционно для продуктов класса BAS были периметровые средства защиты, средства защиты электронной почты и средства защиты конечных точек. Все из представленных на рынке решений позволяют проводить такие проверки. Однако каждый продукт выполняет такие проверки по-своему.

В последнее время продукты класса BAS стали также предлагать возможности по проверке работы правил обнаружения в решениях класса SIEM и SOC в целом. В рамках проведения таких проверок разработчики продуктов активно используют методологию и соответствующую базу знаний о тактиках, техниках и их реализациях, например матрицу MITRE ATT&CK.

Также проведение симуляций действий злоумышленника позволяет проверить и работу персонала в части мониторинга и реагирования на эти инциденты.

Таким образом, применение BAS позволяет:

- ♦ CISO получать в любой момент времени реальную оценку защищённости инфраструктуры и в зависимости от этого более эффективно и обоснованно планировать развитие системы киберзащиты;

- ♦ подразделениям, отвечающим за эксплуатацию и развитие средств защиты, определять, как средства защиты в реальности реагируют на различные хакерские действия, корректны ли настройки этих средств защиты и нет ли отличий в настройках средств защиты в разных сегментах сети;

- ♦ сотрудникам SOC проверять работу правил обнаружения подозрительных действий злоумышленников, реализацию процессов реагирования на инциденты и корректность playbook'ов в системах класса SOAR.

Для получения полной информации о реальном уровне защищённости вашей компании применение решений класса BAS нужно выстроить в отдельный процесс, который позволял бы проводить симуляции по всей инфраструктуре по заранее заданному и согласованному расписанию с использованием различных сценариев.

ПОВЫСИТЬ ЭФФЕКТИВНОСТЬ SOC

Проблема повышения эффективности работы SOC намного сложнее, чем проблема выбора эффективных настроек средств защиты. Основа SOC — корреляционные правила обнаружения различных техник злоумышленников (в большинстве случаев реализованных на базе решений класса SIEM) как на этапе первичного проникновения, так и на последующих этапах кибератаки. При этом, по оценкам независимых экспертов, корреляционные правила обнаружений, которые поставляются вендорами решений класса SIEM, позволяют детектировать не более 20% техник из матрицы MITRE ATT&CK. До 15% из этих правил работают некорректно в реальной инфраструктуре. То есть нельзя поставить SIEM-систему с набором правил детектирования от вендора и работать с этим набором. Для того чтобы эффективно обнаруживать техники злоумышленников, необходимо постоянно развивать набор правил корреляции. Для этого, во-первых, нужно постоянно анализировать новые и постоянно развивающиеся техники злоумышленников. Во-вторых, разрабатывать средства для проверки того, как эти техники работают в конкретной инфраструктуре и достаточно ли событий поступает в SIEM-систему для обнаружения злоумышленника. И уже на основе анализа этих данных разрабатывать правила корреляции. На последнем этапе нужно проверить, как это правило работает во всей инфраструктуре. Руками выполнять все эти действия, даже используя необходимые техники, что используют настоящие злоумышленники, дорого и требует огромного количества ресурсов.

Продукты класса BAS позволяют решить эти проблемы. Во-первых, они несут с собой необходимую экспертизу и знания по новым атакующим техникам злоумышленников. Во-вторых, позволяют провести автоматическую симуляцию этих техник. На основе полученных результатов аналитики SOC смогут разработать необходимые правила корреляции и далее автоматически перезапустить симуляции для проверки корректности их работы.

Фактически BAS на данный момент — это единственное средство, которое

позволяет проводить автоматический аудит всех изменений в инфраструктуре и помогает более эффективно разрабатывать новые правила корреляции для эффективного обнаружения злоумышленников.

СИМУЛЯЦИЯ АТАК И РОССИЙСКИЙ CTRLHACK

Единственным на данный момент российским продуктом класса BAS является платформа CtrlHack. CtrlHack позволяет проводить симуляции различных техник злоумышленников непосредственно в инфраструктуре организации. Симуляции выполняются на узлах, где установлены агенты CtrlHack. При этом вся система может быть полностью развернута внутри инфраструктуры организации.

CtrlHack позволяет проводить симуляции, направленные на проверку работы периметровых средств защиты (IPS, NGFW), средств защиты электронной почты («песочница», почтовые антивирусы), средств защиты конечных точек (антивирусы, EDR). Но основным вектором для CtrlHack является симуляция различных техник злоумышленников, направленных на проверку работы правил корреляции в решениях класса SIEM, а также на повышение эффективности разработок данных правил.

В базе знаний CtrlHack есть симуляции техник для всех стадий выполнения атаки, и этот набор постоянно обновляется и расширяется. Решение также позволяет добавлять собственные объекты во внутреннюю базу знаний для последующего использования при запуске симуляций. Это могут быть вредоносные ссылки, файлы, скрипты.

По результатам симуляции станет понятно, насколько полно собираются все необходимые события, как работают правила корреляции в решениях класса SIEM и насколько полно обнаруживаются разные стадии выполнения атак. А детальная техническая информация о выполненных в рамках симуляций действиях позволит аналитикам SOC легко разрабатывать новые правила корреляции (или модифицировать имеющиеся) и в дальнейшем тестировать работу этих правил.



Павел СМЕРНОВ
директор по развитию
компании «КриптоПро»



Сергей КОВТУНОВ
руководитель проектов
компании «КриптоПро»

АРХИВНОЕ ХРАНЕНИЕ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ С ЭП

ЗАКОНОДАТЕЛЬСТВО И ПРАКТИКА

Многие организации сейчас используют электронный документооборот — как внешний, так и внутренний. При этом определить авторство документа и убедиться в том, что он не был изменён в процессе своего жизненного цикла, позволяет использование электронной подписи. Хранение, в том числе и долговременное, является частью жизненного цикла практически всех видов электронных документов, подписанных электронной подписью.

ПРОБЛЕМАТИКА

При организации архивного хранения электронных документов возникают такие сложности, как:

- ♦ проблема долговечности носителей;
- ♦ устаревание программного и аппаратного обеспечения;
- ♦ проблемы, возникающие при необходимости миграции электронных документов;
- ♦ проблема обеспечения аутентичности и юридической значимости документа в течение всего срока хранения.

Если первые три проблемы обсуждаются давно и уже имеют технические и организационные решения, то предложений по решению последней проблемы немного.

ДВА ПОДХОДА

Сам термин «аутентичный электронный документ» (authentic electronic document-based information) описан в стандарте ГОСТ Р 54989–2012/ISO/TR 18492:2005 как «электронный документ, точность, надёжность и целостность которого сохраняются с течением времени». То есть любой электронный документ, подписанный электронной подписью, является аутентичным. Если при подписании использовалась квалифицированная ЭП, электронный документ является безусловно равнозначным документу на бумажном носителе, подписанному собственноручной подписью. Основная проблема здесь — проверка того, что сертификат подписанта был действителен на момент подписания электронного документа. И для решения задачи обеспечения аутентичности необходимо реализовать возможность проверки электронной подписи документа в течение всего срока хранения. В настоящий момент в законодательстве описаны два подхода, которые призваны решить эту проблему.

По нормам 63-ФЗ «Об электронной подписи» действительность сертификата на момент подписания электронного документа подтверждается при наличии «достоверной информации о моменте подписания электронного

документа». Такую информацию можно взять из так называемой метки доверенного времени (ответа доверенной службы штампов времени, TSP-службы). Однако само по себе наличие метки времени в электронной подписи ничего не говорит о действительности сертификата подписанта. Значит, для обеспечения положительного результата проверки подписи в рамках архивного хранения одной лишь метки времени недостаточно.

Второй подход описывает законопроект № 1173189–7, находящийся в стадии рассмотрения Государственной думой РФ. Для архивного хранения предлагается доверять подписи архивариуса — лица, осуществляющего хранение электронного документа на основании лицензии, или иного лица, осуществляющего хранение электронного документа, — и в момент окончания срока действия сертификата исходного подписанта или архивариуса осуществлять переподписание документов. Но при постоянно растущем объёме электронных документов со временем переподписание архивного массива может стать затруднительным.

Очевидно, что эти подходы не дают возможности получения положительного результата проверки в течение всего срока хранения документа. И всё же решение существует.

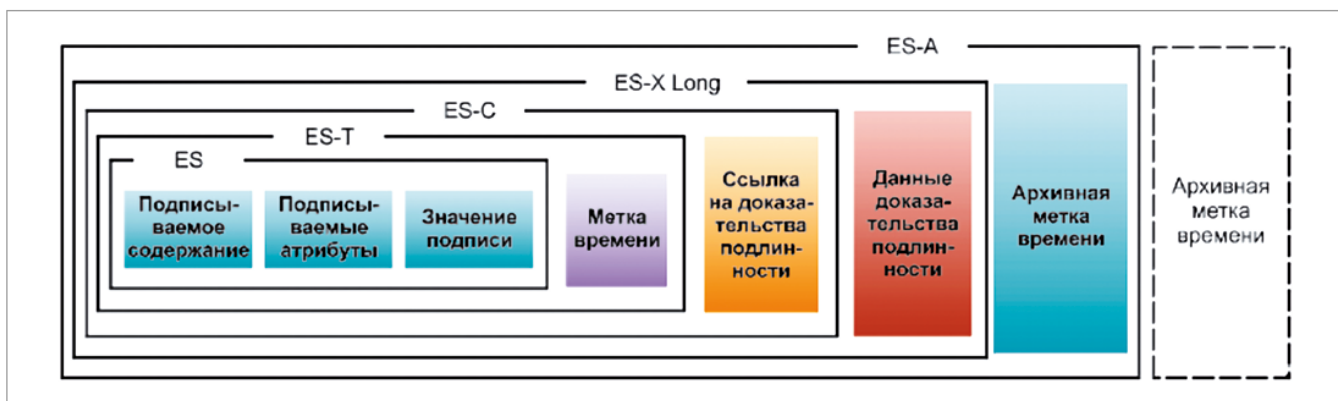


Рисунок 1. Форматы подписи AdES

ТРИ ФОРМАТА

В России довольно широко используются форматы усовершенствованной электронной подписи CAdES (CMS Advanced Electronic Signature) и XAdES (XML Advanced Electronic Signature), закреплённые в стандартах организации ETSI. Для краткости будем называть их вместе AdES. В зависимости от назначения электронной подписи в этих спецификациях определены разные виды формата усовершенствованной подписи (рис. 1), но сейчас наиболее распространены эти:

- ♦ AdES-BES: формат, в котором рассмотрены значение электронной подписи и некоторая дополнительная информация;

- ♦ AdES-T: расширение формата ES, в котором добавлена метка времени подписи, полученная от доверенной службы времени и используемая для доказательства момента формирования подписи;

- ♦ AdES-X Long: расширенный формат, в котором добавлена информация обо всех сертификатах (цепочках сертификатов), необходимых для проверки подписи, доказательства их действительности на момент подписания, и дополнительная метка времени, полученная от доверенной службы времени и используемая для заверения доказательств подлинности.

РАЗВИТИЕ ФОРМАТА

Формат AdES-X Long позволяет обеспечить временное (оперативное) хранение и положительный результат проверки электронной подписи документов сроком до 10–15 лет с момента подписания. Практически все продукты

компании «КриптоПро», связанные с созданием или проверкой электронной подписи, от «КриптоПро ЭЦП Browser plug-in» и до «КриптоПро DSS» или «КриптоПро SVS», умеют работать с данным форматом. Однако для документов долговременного (больше 15 лет) или постоянного хранения данный формат подписи не подходит из-за ограниченного срока жизни сертификата службы штампов времени (обычно не более 15 лет), который используется для заверения доказательств подлинности.

Развитием формата AdES-X Long является формат AdES-A, который даёт возможность в процессе хранения подписи документа добавлять дополнительные архивные метки времени, предназначенные для защиты подписи, предыдущих меток времени и доказательств подлинности. В отличие от типа AdES-X Long, при хранении подписи такого формата необходимо добавлять новые архивные метки времени в течение всего жизненного цикла документа. Но данную процедуру потребует выполнять значительно реже (раз в 10–15 лет) в сравнении с ежегодным переподписанием документа подписью архивариуса, и сам процесс добавления штампа времени проходит существенно быстрее создания подписи.

«КРИПТОПРО АРХИВ»

Компания «КриптоПро» разработала ряд продуктов, поддерживающих формат AdES-A. Одним из них является «КриптоПро Архив», созданный для:

- ♦ подготовки электронной подписи документов к временному (до 10 лет),

долговременному (свыше 10 лет) и постоянному централизованному хранению;

- ♦ усовершенствования электронных подписей документов форматов CAdES-BES, CAdES-T, CAdES-C, CAdES-XLT1 до формата CAdES-A, обеспечения юридической значимости электронных документов при их хранении за счёт использования хранящихся в подписи доказательств подлинности и заверяющих их архивных меток (штампов) времени;

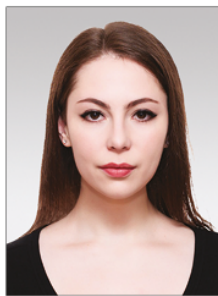
- ♦ контроля сроков действия доказательств юридической значимости документов при их длительном хранении и их автоматического обновления;

- ♦ приёма и передачи информации об электронных подписях и мета-данных электронных документов временного, долговременного и постоянного хранения между «КриптоПро Архив» и информационными системами организации.

Опыт первых внедрений «КриптоПро Архив» доказал его эффективность в решении задачи по получению положительного результата проверки в течение всего срока хранения документа. Мы активно развиваем функциональность «КриптоПро Архив», следя за законодательской деятельностью в области архивного хранения, а также опираясь на обратную связь от тех, кто уже интегрировал наш продукт в свои информационные системы и системы документооборота.



Евгения КОЛОДИНА
директор по развитию
ГК «ЦИБИТ»



Ксения МИНАКОВА
руководитель Департамента
образовательных проектов
ГК «ЦИБИТ»

КАДРЫ РЕШАЮТ ВСЁ

УКАЗ ПРЕЗИДЕНТА РФ № 250

1 мая 2022 года Президент России Владимир Путин подписал Указ № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». Документ вызвал широкую дискуссию в отрасли. Через месяц после его подписания Правительством РФ был представлен полный перечень ключевых организаций, которым предстоит осуществить оценку уровня защищённости

информационных систем с привлечением организаций-лицензиатов ФСБ России и ФСТЭК России. И уже в начале июля появилась информация о проекте Постановления Правительства России об утверждении типового положения о заместителе руководителя организации по вопросам информационной безопасности и типового положения о подразделении информационной безопасности.

КАДРОВЫЙ ВОПРОС

Одно из важнейших изменений, продиктованных документом, касается кадрового вопроса. Согласно Указу, в обозначенных ведомствах и организациях должны быть созданы подразделения по информационной безопасности. Речь идёт об обнаружении, предупреждении и ликвидации компьютерных атак и реагировании на инциденты.

По первым оценкам аналитиков отрасли, новые меры в той или иной мере затрагивают порядка 500 тысяч российских организаций, соответственно можно прогнозировать потребность в более чем 1 млн специалистов по информационной безопасности.

Из Указа № 250 (рис. 1) следует, что к компаниям из перечня Правительства РФ относятся органы государственной власти, предприятия с госучастием, субъекты критической информационной инфраструктуры (КИИ), стратегические и системообразующие организации. Руководить новыми ИБ-подразделениями в соответствии с Указом должны лица в ранге заместителя руководителя компании/ведомства.

Документ возлагает ответственность за кибербезопасность на топ-менеджмент компаний, чтобы исключить игнорирование вопросов защиты информации на предприятиях.

Согласно появившейся недавно информации о проекте Постановления Правительства об утверждении типового положения о заместителе руководителя организации по вопросам ИБ, такой сотрудник в компании должен иметь либо высшее профильное образование не ниже уровня

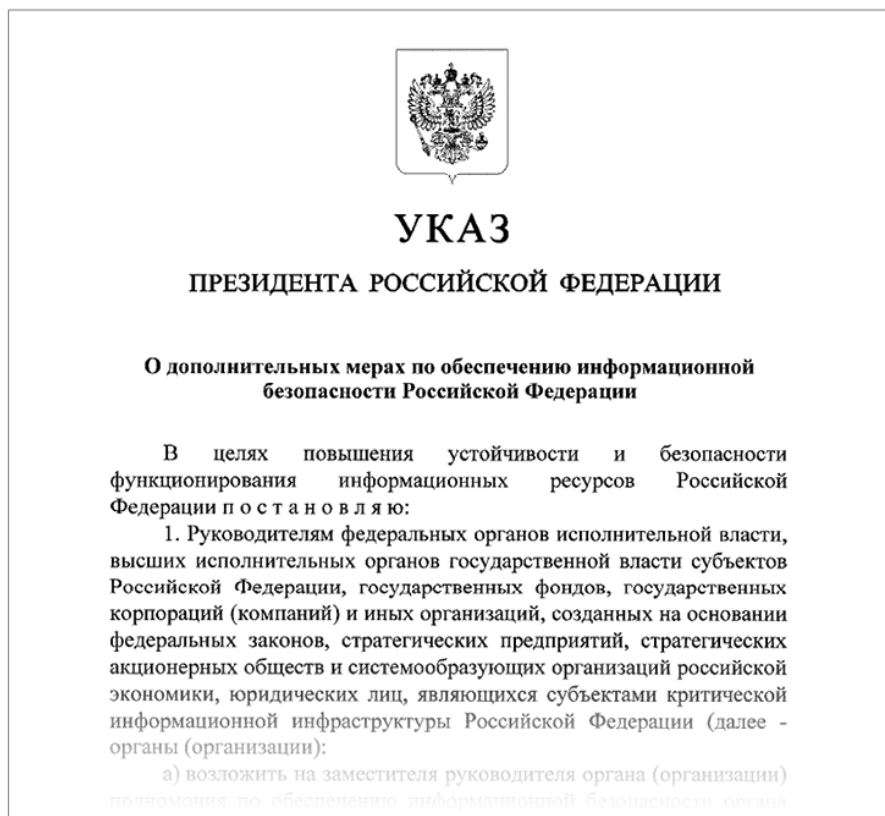


Рисунок 1. Из Указа Президента РФ № 250

специалитета или магистратуры, либо просто иметь высшее образование, но при этом пройти профессиональную переподготовку по информационной безопасности.

КАК СООТВЕТСТВОВАТЬ НОВЫМ ТРЕБОВАНИЯМ?

Указанным организациям нужно будет создать структурное подразделение внутри компании, отвечающее за обеспечение информационной безопасности, либо же передать эти функции уже существующему отделу/департаменту.

Таким образом, мы видим два пути решения задач в части соответствия требованиям Указа № 250. Первый — это обучение действующих сотрудников компании по программам профессиональной переподготовки, удовлетворяющим требованиям документа. Второй вариант — подбор специалистов, уже имеющих необходимую квалификацию и соответствующих нужным критериям.

Обучение сотрудников по программам профессиональной переподготовки. В случае, если обязанности по обеспечению информационной безопасности компании будут возложены на уже существующее ИТ-подразделение, то специалистам может понадобиться профессиональная переподготовка по направлению «Информационная безопасность».

В состав группы компаний «ЦИБИТ» входит собственный отраслевой Учебный центр, который специализируется на оказании услуг по дополнительному профессиональному образованию в области информационной безопасности по программам профессиональной переподготовки и повышения квалификации.

В перечне Учебного центра «ЦИБИТ» целый ряд образовательных программ, согласованных с ФСБ России и ФСТЭК России. Программы профессиональной переподготовки по информационной безопасности, согласованные с регулирующими органами, в том числе удовлетворяют критериям для соответствия требованиям Указа № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»:

1. «Технологии и средства обеспечения компьютерной безопасности» (540 часов);

2. «Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну» (504 часа).

Большой спектр предлагаемых обучающих курсов позволяет подготавливать специалистов самого высокого уровня, соответствующих требованиям регулирующих органов и актуальным нормам законодательства.

Подбор специалистов, соответствующих требованиям. Оптимальным решением для предприятий, которым необходимо будет пополнить кадровый состав квалифицированными специалистами, станет обращение к профессиональным рекрутерам.

В состав группы компаний «ЦИБИТ» входит кадровое агентство, которое специализируется на подборе персонала в сфере информационной безопасности уже более семи лет. За это время не только накоплен опыт и знание рынка, но и сформирована собственная уникальная база кандидатов: вакансии компаний-клиентов закрываются максимально оперативно, при этом подобранные работники соответствуют всем предъявляемым требованиям.

Стоит отметить: специалисты ЦИБИТ работают с действительно ценными кадрами, например, с бывшими сотрудниками силовых структур, в

том числе с соискателями, которые занимались обеспечением информационной безопасности на государственном уровне.

АУДИТ СРЕДСТВ И СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

В начале лета Министерством цифрового развития, связи и массовых коммуникаций РФ был представлен Перечень ключевых организаций, которым предстоит осуществить оценку уровня защищенности информационных систем с привлечением организаций-лицензиатов ФСБ России. Всего в список вошли 74 организации, включая государственные ведомства, СМИ, авиакомпании, крупнейшие банки и проч.

Департамент аттестационных работ ГК «ЦИБИТ» для решения этой задачи оказывает комплексную услугу по проведению аудита применяемых средств и систем защиты информации.

Такая проверка позволяет обследовать организацию с целью оценки применяемых средств и систем защиты информации на наличие СЗИ с действующими сертификатами, а также СЗИ, выпущенными в недружественных странах. Далее наши специалисты вносят предложения по замене средств защиты информации, если несоответствующие СЗИ будут обнаружены.

Результатом работ является проведенная система защиты информации или предложения по её модернизации.

ЦИБИТ («Центр исследования безопасности информационных технологий») — консалтинговая компания, накопившая опыт экспертизы и помогающая организациям соответствовать требованиям по информационной безопасности с 2009 года.

Профессиональная цель ГК «ЦИБИТ» — лидерство в своей области. Сегодня компания способствует совершенствованию профессиональной среды и стремится задавать вектор развития для структур, работающих в сфере информационной безопасности.

Глобальная цель ЦИБИТ — через формирование понимания необходимости защиты информации в современном мире делать жизнь сообщества 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.

Контакты:

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



ВРЕМЯ ПЕРЕМЕН

КАК ВЫПОЛНИТЬ НОВЫЕ ТРЕБОВАНИЯ РЕГУЛЯТОРОВ В ИБ И НЕ ПОСЕДЕТЬ



Алексей ПАРФЕНТЬЕВ
руководитель отдела
аналитики «СёрчИнформ»

2022 год для сферы информационной безопасности стал знаковым: начали движение «тектонические плиты», которые ИБ-активисты пытались сдвинуть несколько лет. С начала года защита данных «на устах» у высших чинов, президент предписал создать ИБ-подразделения в организациях и назначить заместителей руководителя, ответственных за безопасность. А к концу полугодия Госдума проголосовала за долгожданные поправки в 152-ФЗ «О персональных данных».

Вопросы информационной безопасности вышли в стране на революционно новый уровень. В теории это значит, что оборот и хранение наших данных станут безопаснее. На практике — что почти 80% компаний столкнутся с серьезными проблемами. Давайте разберемся, что и для кого меняется с точки зрения обеспечения информационной безопасности.

1. Обязательное импортозамещение защитных технологий. В марте 2022 года президент подписал Указ № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры РФ». Документ запретил значимым объектам КИИ закупать иностранное ПО, а с 2025 года нельзя использовать уже закупленные иностранные лицензии. Указ, вместе с «горящими» проблемами вроде уходящих один за одним западных вендоров, когда заказчики остались без защиты, оплаченных лицензий и техподдержки, подстегнул интерес к российскому ПО. И хотя выбор отечественного ИБ-софта широкий, темпы замещения буксуют. По опросам коллег, доля российских средств защиты в некоторых сегментах составляет только 15%.

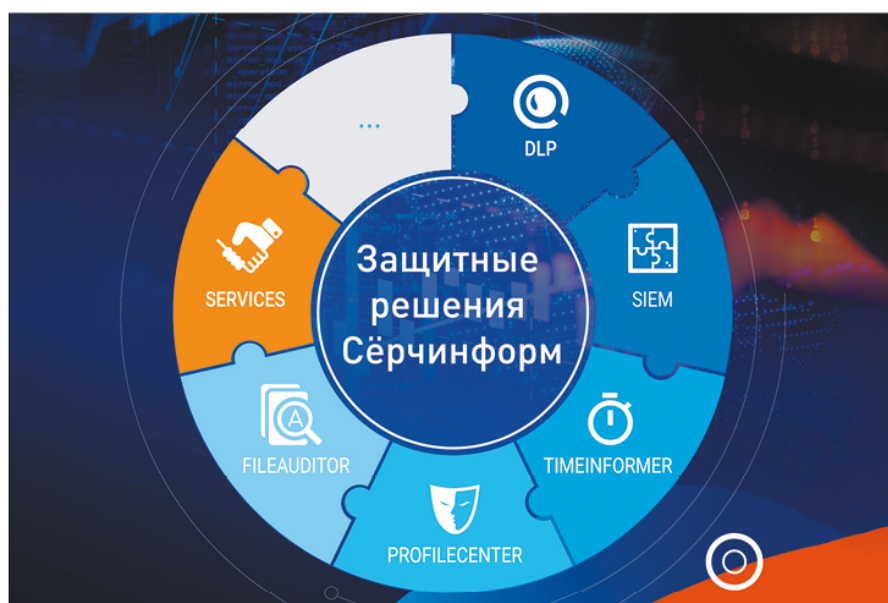
Причин этому две: во-первых, многие решения написаны под иностран-

ные ОС и оборудование, поддержке российского системного софта разработчики уделяли меньше времени, это сказывалось на функционале. Вторая большая проблема для заказчика — в «железе». Иностранная поставка практически встала, а в стране пока не хватает мощностей, чтобы произвести отечественные процессоры в необходимых объемах.

Однако рынок уже адаптируется к новым реалиям и предлагает решения. Проблему с оборудованием «закрывает» перенос защитных систем в облака и работа с вендорами по MSSP-модели.

В этом случае вопрос, где найти мощности для развертывания систем, да так, чтобы они соответствовали всем стандартам — «головная боль» провайдера. Например, мы «подружили» всю нашу линейку ПО с отечественными облачными провайдерами, поддерживаем и расширяем возможности защиты ПК на российских ОС, контроля отечественного ПО (мессенджеров, офисных программ и пр.), перевозим софт на российские СУБД PostgreSQL. Эта практика распространяется во всех сегментах рынка, вендоры идут навстречу заказчикам и способны быстро создать условия для комфортного импортозамещения.

2. Отделы ИБ и замы по безопасности. В мае вышел Указ № 250 «О дополнительных мерах по обеспечению информационной безопасности РФ». Он предписывает всему госсектору, а также системообразующим предприятиям и КИИ создать подразделения по ИБ. На руководителей структур ложится персональная ответственность за ИБ, причем они должны иметь доступ к высшему руководству для оперативного информирования об угрозах.



Указ призван решить проблему: по данным нашего исследования, в 2020 году в 60% российских компаний не было подразделения по защите информации. Но опаснее то, что такие подразделения может оказаться не из кого собрать. В 2021-м треть компаний говорили об острой нехватке ИБ-специалистов.

В этих условиях выполнить требования указа будет проблематично. Решением могут стать сервисы по информационной безопасности. Контроль внешних угроз можно возложить на SOC, мониторинг утечек и контроль персонала — на аутсорсеров DLP и других систем внутренней защиты.

Выгода подхода в том, что специалисты заказчика смогут работать в системах параллельно с внештатными аналитиками, перенимать их опыт и практики.

Например, мы в формате аутсорсинга оставляем за сотрудниками заказчика высшие привилегии в наших системах и готовы обучать работе в системе. Плюс к тому в учебном центре постоянно действуют больше десятка программ для повышения квалификации ИБ-специалистов.

3. Отчетность об утечках и оборотные штрафы. Летом Госдума проголосовала за поправки к ФЗ-152 «О персональных данных». Ожидается, что осенью закон будет подписан и вступит в силу. И компании, которые хранят и обрабатывают ПДн, будут обязаны в течение суток отчитываться регуляторам в случае киберинцидента и в течение 72 часов представлять им результаты внутренних расследований. А еще одна инициатива, выдвинутая Минцифры, вводит оборотные штрафы в 1% за утечки и 3%, если компания попытается скрыть инцидент (эти цифры еще могут измениться). Эти поправки, по сути, самые массовые и требования коснутся всех, кто обрабатывает и хранит личные данные граждан.

Проблема в том, что выполнить требования будет невозможно, если нечем выявить инцидент и расследовать его причины. Учитывая объемы обработки ПДн, собрать эти сведения вручную невозможно. Поэтому потребуется внедрять специальные средства контроля (см. врезку).

С таким набором систем жизненный цикл ПДн в компании будет под

DCAP-системы, чтобы найти все персданные в компании и отслеживать действия с ними. Это необходимый минимум, чтобы «закрыть» новые требования. Автоматический аудит и логирование файловых операций помогут понять, у кого есть доступы к ПДн и отрегулировать их, зафиксировать инцидент по аномальной активности с файлами, по логам восстановить картину нарушения.

«СёрчИнформ FileAuditor» надёжно определяет уязвимый контент, фиксирует нарушения прав доступа и изменения в критичных данных, защищает документы от опасных действий сотрудников благодаря блокировкам на уровне файловых потоков.



DLP-системы — самый «профильный» инструмент, который автоматически обнаружит и сможет заблокировать утечку. DLP контролируют каналы передачи данных, активность сотрудников в ПО, локальной сети и на внешних сервисах, так что зафиксируют передачу ПДн за пределы корпоративного периметра в любом виде. DLP с развитой аналитикой помогут определить границы инцидента и собрать необходимые доказательства.

Выбор DLP на российском рынке большой, так что решающими могут стать «бонусные» фишки. Например, в «СёрчИнформ КИБ» есть таск-менеджер для удобного управления расследованием, карточки пользователей с досье нарушений и больше 30 отчетов с возможностью быстрого экспорта — как раз хватит, чтобы «закрыть» новые нормативы. К тому же КИБ бесшовно интегрируется с файловым аудитором и может, например, одновременно контролировать движение сразу всех файлов, которые DCAP определил как «ПДн».



SIEM-системы выявят внешние атаки и другие угрозы системам обработки ПДн. Это нарушения доступов, уязвимости, взлом периметра, неочевидные причины «самопроизвольных» утечек — скажем, если из-за изменений настроек сервера база с ПДн стала доступна в интернете. Данные о происходящем SIEM собирают из источников во всей IT-инфраструктуре, так что все проблемы с ИБ решаются по принципу одного окна. Например, система увидит связь между алертом о подозрительных операциях из DCAP и об утечке от DLP, и сообщит об этом в реальном времени.

В «СёрчИнформ SIEM» встроен сканер уязвимостей, он поможет заранее увидеть, откуда ждать кибератаку. А если взлом или утечка произошли, интеграция SIEM с ГосСОПКА позволит быстро отчитаться по всей форме.



контролем. Комплекс ПО позволит не допустить утечек в будущем: распределить доступы к персданным, заблокировать передачу этих данных в любых каналах, создать правила корреляции, которые укажут на проблемы.

ГДЕ НАЙТИ ФИНАНСИРОВАНИЕ?

Итого — решения есть, компании не остаются один на один с новой реальностью и могут рассчитывать на поддержку вендоров. Но остается проблема, что одномоментно предстоит провести огромную работу по перестройке ИБ-инфраструктуры, это большие затраты времени и денег. Защиту на переходный период можно перевести в аутсорсинг. А чтобы найти средства на закупку собственных решений, можно рассмотреть субсидирование закупок государством: грантовые проекты,

например, реализуют Сколково и РФРИТ. Можно поучаствовать в программах вместе с вендорами, чтобы получить средства сразу на проработанный проект внедрения. А чтобы к нему подготовиться, заранее протестируйте возможности защиты в «боевых» условиях.

Все продукты «СёрчИнформ» доступны для бесплатного пилотирования в течение месяца. Оставьте заявку на триал на сайте searchinform.ru:



«НАДО ГЛУБЖЕ ПЛАНИРОВАТЬ, ГЛУБЖЕ БЮДЖЕТИРОВАТЬ, И ВСЁ ПОЛУЧИТСЯ»

ИМПОРТОЗАМЕЩЕНИЕ В ПОВЕСТКЕ ДНЯ ИТ-КОНФЕРЕНЦИЙ

Этой весной много мероприятий прямо или косвенно были посвящены импортозамещению в сфере ИКТ. Открыла этот марафон 31 марта конференция CNews, которая так и называлась: «Импортозамещение-2022». Состоявшаяся 6 апреля встреча информационно-аналитического агентства TAdviser «Banks IT Day» тоже не стала распылять внимание гостей: там либо напрямую говорили об импортозамещении, либо представляли соответствующие продукты и услуги. Вполне органично эта тема прозвучала и 12 апреля на CISO Форуме — 2022.

13 апреля на форуме «РазвИТие» разговор продолжили. Тут наряду с «де-юре» нишевым (но о-очень дорогостоящим) вопросом импортозамещения в сфере так называемого инженерного ПО были поставлены вопросы налаживания взаимоотношений между вендорами и заказчиками ПО. Причём речь шла о взаимоотношениях более сложных, чем просто «купи-продай». Например, впервые прозвучал конкретный ответ заказчика на центральный вопрос о выборе приоритета между функциональностью и

импортонезависимостью. Была дана твёрдая установка на параллельное решение обеих задач. Запомнился, кстати, комментарий на этот ответ представителя двигателестроителей, заявившего, что постановка вопроса в коннотации альтернативы свидетельствует о недостатках в планировании ресурсов, которые, если их недостаточно, следует найти, так как «ДВУХ ЛЕТ У НАС МОЖЕТ И НЕ БЫТЬ».

18 мая агентство TAdviser провело конференцию «Импортозамещение в новых условиях». Мероприятие длилось больше восьми часов, но сохранило аудиторию до последней минуты последнего доклада. Почти три десятка докладчиков представили возможности отечественных компаний в сфере замещения корпоративных ИТ-приложений. Наряду с сугубо информационными сообщениями, представлявшими продукты, звучали и рекомендации по методологии перехода на отечественное ПО.

31 мая на форуме SummIT-2022 были представлены отечественные достижения в цифровизации промышленности, госуправления, финансовой сферы, ретейла, в технологиях бизнес-аналитики

и анализа больших данных, в облачных технологиях и т.д.

К июню, когда «импортозаместительный» поток вопросов, фактов и аргументов пошёл по второму, если не третьему кругу, стало возможным подвести итоги этих весенних обсуждений. Произошло это 1 июня на Форуме DLP+, посвящённом технологии и решениям, по которым Россия, по оценкам экспертов, «впереди планеты всей».

РЕПЛИКА В СТОРОНУ

«Заместить» в ИТ, оказывается, надо всё — базовые аппаратные платформы/БАП (серверные, настольные, мобильные, коммуникационные, для хранения данных); ПО для встроенных в оборудование вычислительно-управляющих систем, включая ОС; ПО для офисных приложений и корпоративного управления; для систем информационной и кибербезопасности; инженерное ПО/пакет САПР) и т.д. и т.п.

Рассуждая о БАП, сразу вспоминают о процессорах, забывая (или «забывая»?) о прецизионных резисторах и конденсаторах, о проектировании многослойных плат, корпусах микросхем и серверов...

Обсуждая ПО, нет-нет, да и забудут об инструментарию разработчика, о «мелочёвке» вроде драйверов, написание которых тесно связано с решением вопроса о периферийном оборудовании для полноценной экипировки БАП.

САМОЕ СЛАБОЕ ЗВЕНО

О перспективах отечественного «железа» на мероприятиях почти ничего

Впервые прозвучал конкретный ответ заказчика на центральный вопрос о выборе приоритета между функциональностью и импортонезависимостью. Была дана твёрдая установка на параллельное решение обеих задач

не говорили — по принципу «или хорошо, или ничего». Исключение, пожалуй, составили конференция «Импортозамещение-2022» и форум DLP+.

В заголовок обзора вынесены слова гендиректора Delta Computers, представившего на конференции «Импортозамещение-2022» план действий по импортозамещению «железа» корпоративно-серверного уровня. Его финальное заявление: «Работать будет на чём, хотя и выйдет дороже», — прозвучало оптимистично.

На форуме DLP+ спектр обещаний был шире и распространялся уже на перспективы появления отечественных настольных и мобильных устройств. Обещания эти попали под мощный шквал сомнений и критики, но доводы докладчика всё же позволяют верить в успех. Особенно если государство наряду с регуляторно-указующими функциями начнёт выполнять и функции регуляторно-избирательно-по-умному-поощряющие.

ЧЕГО В ЭТОМ СУПЕ НЕ ХВАТАЕТ?

В части ПО есть основания для большего оптимизма. По данным АРПП «Отечественный софт», «информационная безопасность — сектор, традиционно сильный в нашей стране, здесь мы имеем решения мирового уровня», а «проникновение отечественных ИТ-продуктов такого рода в госсектор и госкомпании составляет до 90%».

В то же время у крупных частных компаний взгляд на ситуацию менее радужный. По мнению экспертов CISO форума, «практически в каждой продуктовой нише в сегменте ИБ есть российские решения, однако их качество, управляемость, производительность, масштабируемость оставляют желать лучшего. И если предприятия малого и среднего бизнеса могут в той или иной степени использовать отечественные продукты, то для крупного бизнеса это невозможно в силу масштаба их деятельности».

В сегменте офисного делопроизводства и корпоративного управления ситуация с импортозамещением тоже неудовлетворительная. «Согласно последнему исследованию АРПП,

По данным АРПП «Отечественный софт», «информационная безопасность — сектор, традиционно сильный в нашей стране, здесь мы имеем решения мирового уровня», а «проникновение отечественных ИТ-продуктов такого рода в госсектор и госкомпании составляет до 90%»

проникновение отечественных ИТ-продуктов в госсектор и госкомпании составляет 30–35%. При этом основа основ — платформенные решения — составляет менее 5%» (со слов председателя правления АРПП «Отечественный софт»).

При этом, по мнению экспертов конференции TAdviser «Banks IT Day», перевод офисных рабочих мест на отечественный софт мог бы давно состояться, если бы знакомство с соответствующими программами началось со школьной скамьи (вместо тотального ориентирования детей на решения Microsoft). О наличии несложных в развёртывании отечественных офисных решений говорилось и на форуме DLP+.

Уместно тем не менее упомянуть, что, по мнению директора ДИБ Банка «Тинькофф» Дмитрия Гадаря (высказанному на CISO Форуме), на российском рынке не хватает решений для организации виртуальных рабочих мест.

На форуме DLP+ был поднят вопрос об отечественном работоспособном доверенном браузере, однако участники обсуждения так и не смогли подтвердить наличие заказчика такой разработки и, как следствие, вспомнить о каких-либо успехах в этой области.

Зато в нише так называемого системного ПО в нашей стране, похоже, наблюдается избыток разработок операционных систем на базе ядра Linux. При этом упоминания о 4–5 из таких ОС чаще прочих встречаются в докладах о функциональном тестировании продуктов и решений из Единого реестра ПО на совместимость между собой.

А если говорить об инструментарии разработчиков программ, то в России «не покрыты такие классы решений, как динамические и статические

анализаторы кода» (Дмитрий Гадарь на CISO Форуме).

ВЫВОДЫ

Понятно, что удалось посетить не все мероприятия, где говорилось об импортозамещении. Но и по приведённой выборке можно сделать некоторые выводы.

Первый. Даже у поколений, сформированных в эпоху тотальной атаки на национальную самоидентификацию, возникает понимание, что «надо искать свой путь, чтобы в дальнейшем мы были конкурентоспособны как в области ПО, так и в элементной базе — создании совместных предприятий полного цикла, специальных инвестиционных зон и прочего» (Николай Белобров, «РТК-Солар»).

Второй. Несмотря на деиндустриализацию страны, в сфере разработок ПО имеются решения если и не «мирового уровня», то такие, что могут быть доведены до современных требований «крупного бизнеса». Тут есть примеры и разработок «с нуля», и проектов-реинкарнаций из 90-х. Та же «ТУРБО-Бухгалтер», созданная около трёх десятилетий назад, сегодня переписана и вполне успешно работает как «платформа ТУРБО для импортозамещения систем управления предприятием».

Третий. Проявилась и когорта «сколковского замеса» в хорошем смысле этого выражения. На конференции CNews, например, компании Comindware, GreenData, PRAVO TECH представили разработки, претендующие как на закрытие управленческих потребностей руководителей топ-уровня, так и на пользу для служб ИТ и офисного персонала (автоматизация рутины, комфортная работа в наборе приложений, удобство освоения).

CISO ФОРУМ — 2022

РЕАЛЬНЫЕ CISO О СВОИХ ВИРТУАЛЬНЫХ АНАЛОГАХ И РЕАКЦИИ НА ТЕКУЩУЮ СИТУАЦИЮ

С ISO Форум — 2022 прошёл в стандартном формате «пленарка + мастер-классы и технологические панели + выставка + неформальное общение». Темы кулуарных бесед и официальных мероприятий во многом отражали реакцию на истеричные движения «коллективного запада». Но и они не заслонили текущих проблем отечественной ИБ.

В формате мастер-класса Алексей Лукацкий рассказал о месте и роли системы управления правами доступа к информационным ресурсам и о технологиях идентификации и аутентификации («На код вперёд. Современная идентификация и аутентификация»), Рустэм Хайретдинов поделился взглядами на принципы и технологии сглаживания коллизий во взаимоотношениях бизнеса, ИТ и ИБ в масштабах организации («Пожарная команда: взаимодействие ИТ и ИБ во время «идеального шторма»), Евгений Питолин из «ТерраЛинк» научил, «как сделать ИБ конкурентным преимуществом» и т.д. и т.п.

Особенности дня нынешнего обусловили появление в темах форума таких формулировок, как «война и мир в киберпространстве», «антикризисные кейсы в действии», «какие ноу-хау выбрать сегодня», и задали тему пленарной дискуссии «Если завтра война, если завтра в поход... Один день из новой жизни CISO».

К ЖЕЛЕЗНОМУ ЗАНАВЕСУ ГОТОВЫ

«И страшной сказкой стал для них провал и Лиссабона, и Мессины». Стал, но не для всех. По крайней мере, не для тех, кто был приглашён в президиум пленарки.

В президиуме собралось довольно разноразличное отраслевое представительство — «ибэшные» топы из «Яндекс Банка», «Райффайзенбанка», «Тинькофф», Газпромбанка, а также из

компании «S7 Информационные технологии», Федерального фонда обязательного медицинского страхования, рекрутингового агентства hh.ru, Ассоциации ФинТех. В онлайн-формате «присутствовал» представитель Росатома.

На заботливый вопрос модератора Алексея Лукацкого о возможных изменениях в режиме дня в пользу бессонницы члены президиума и на словах, и своим внешним видом заверили присутствующих в том, что со сном всё ок, хотя работы и прибавилось. На дату 12 апреля 2022 года число кибератак существенно возросло, но годы киберулучшений позволили их по большей части успешно отразить.

На вопрос, готова ли к восстановлению «железного занавеса» стратегия ИБ в организациях, спикеры бодро ответили, что они всегда знали, с кем имеют дело. Однако отметили, что особенностью возникающих сложностей стала одномоментность исхода из России иностранных вендоров.

Ответом на это обстоятельство было разное. Кто прикупил впрок, кто инхаусно оупенсорсит, а кто уже лучше вендора разбирается в нюансах работы своего оборудования и сам обеспечивает поддержку и управляет обновлениями.

Уместно заметить, что эксперты «пленарки» и стоящие за ними организации — это элита не только бизнеса, но и «кибербеза».

А вот среди основной массы гостей форума лишь единицы, как оказалось, заложили в свои модели угроз предательство вендоров.

Тем не менее участники дискуссии высказали мнение, что предприятия малого и среднего бизнеса могут достаточно успешно использовать отечественные продукты, ведь сегодня практически в каждой продуктовой нише ИБ-оборудования есть одно или несколько российских решений. Но если российские SIEM и антивирусы отвечают современным требованиям, то в других категориях «многие российские

продукты есть, но их функциональность и производительность меньше, чем это необходимо для крупных организаций. Почему? Потому что раньше их производили совсем для других задач и больше вкладывались в западное программное обеспечение» (Артём Калашников, Газпромбанк).

Поэтому, например, «Райффайзенбанк» делает ставку на собственные разработки на базе Open Source.

В качестве иной альтернативы некоторые эксперты рассматривают замену иностранных решений набором из нескольких отечественных. Представитель Газпромбанка так образно описал эту ситуацию: «У нас есть колёса, рамы, кабина, ходовые части, салон. Теперь из этого отечественного „лего“ нужно что-то собрать. Причём важно собрать целостную конструкцию — „железо“, платформы, виртуализации, бизнес-приложения. Такие кейсы будут актуальны».

«ВОЗЬМЁМСЯ ЗА РУКИ, ДРУЗЬЯ!»

Санкционная ситуация и ужесточающаяся «нормативка» стимулируют многое. Например, наведение мостов между отечественными вендорами и заказчиками, чтобы на основе «сигналов обратной связи» вендоры отшлифовали ИБ-«комплектующие» до состояния, при котором из них можно будет «системно интегрировать» решения и бюджетные, и достаточно высокой производительности.

Тема взаимоотношений вендоров и заказчиков была затронута и на пленарке, но детально её разбирали на треке «Безопасность vs бизнес: маркетинг в ИБ: доверяй, но проверяй». На эту же тему работала выставочная зона, эпицентром действия на которой стал стенд Positive Technologies.

Как известно, сегодня в центре внимания этого отечественного вендора — разработка платформы для создания корпоративных ИБ-решений,



Фото: infor-media.ru



Фото: infor-media.ru

позволяющих в автоматическом режиме обнаруживать и останавливать атаку силами одного человека. В рамках продвижения своей идеологии компания провела на стенде ряд впечатляющих демонстраций.

КРАХ ИТ-БОЛОНСКОЙ СИСТЕМЫ?

Вполне традиционно организаторы форума предложили экспертам пленарки обсудить и вопросы кадрового обеспечения. Но в несколько изменившемся, по мнению организаторов, контексте:

Почему SANS перестал учить российских ИБшников? Как и где готовить специалистов?

Смена локаций и «утечка мозгов»: где брать кадры при массовом оттоке специалистов из России?

Но как выяснилось, этот пресловутый SANS перестал учить российских «ибэшников» ещё раньше, чем были объявлены СВО-санкции. Об этом поведал онлайн-спикер из Росатома.

И в связи с этим возникает вопрос, чему такому может обучить зарубежный SANS, чего не знают эксперты, работающие на российском рынке? Примером этих знаний могут являться лекции Алексея Лукацкого на CISO форумах последних лет, комментарии Дмитрия Гадаря на ряде мероприятий, выступления экспертов на PHDays... Примеры можно перечислять долго.

Сам собой возникает вопрос: не пора ли процессу импортозамещения охватить и образовательную сферу? Да,

упомянутых и неупомянутых экспертов трудно усадить за создание учебников. Но надо искать стимулы и инструменты. Почему олимпийских чемпионов страна «награждает» машинами и квартирами, а достойно отметить труд по созданию отечественного курса по ИБ руки не доходят?

Что же касается «смены локаций и утечки мозгов», то, возможно, слухи о массовом оттоке специалистов из России сильно преувеличены? И CISO Форум 2022 заложил первую мину под подобные спекуляции. Многие СМИ после 12 апреля облетели сказанные на форуме слова о том, что «согласно статистическим данным, нет никакой волны якобы уехавших. Те, кто уехал, сделали бы это независимо ни от каких событий, потому что давно были готовы к этому. А у большинства нет никакого желания уезжать. Сейчас наблюдаются потери среди элитных кадров ИБ, но война за специалистов высочайшего класса шла всегда».

Автор приведённой цитаты и модератор «пленарки» вряд ли сговаривались, но так совпало, что тема «войны за специалистов высочайшего класса» нашла своё отражение в дискуссии 12 апреля. Причём решение было предложено весьма мирное, с использованием терминологии нашей эпохи и в духе времени.

«НА РАБОТУ СЕГОДНЯ НЕ ПОЙДУ»

Речь идёт о возможном создании института виртуальных CISO (vCISO) —

приглашаемых по временным контрактам кризисных ИБ-менеджеров для решения внезапно возникших задач или купирования угроз.

«Пленарка» в целом оживилась перспективой такой подработки, на которую, как было предположено, можно будет тратить два-три часа в неделю на одну компанию. Один из CISO даже вспомнил реальный пример виртуализации своей практики, но весьма описательно, без уточнения временных затрат, объёмов и характера подготовленных рекомендаций и исправлений.

В связи с этим остался открытым вопрос и о возможных предельных объёмах работ, выполняемых vCISO без ущерба для своей деятельности в рамках обязанностей realtimeCISO, и о степени реальной ответственности виртуального CISO за действенность предложенных мер.

Не менее важным аспектом появления виртуальных CISO является угроза переоценки зарплат на фоне возможных успехов vCISO при односторонней рабочей неделе с неполным присутствием в этот один день.

Уместно заметить, что в начале июня в отечественных радиоСМИ прошла информация о сокращении Илоном Маском персонала на своих предприятиях и о настоятельном его требовании явиться оставшимся с «удалёнки» на рабочие места.

POSITIVE HACK DAYS 11

ОТ ХАКЕРСКОГО «ХАРДКОРА» ДО ВОПРОСОВ ИНВЕСТИРОВАНИЯ В ИБ

Устроители называют Positive Hack Days «форумом по практической безопасности», а его остепенившиеся старожилы — «хардкорным хакерским мероприятием». Однако уже несколько лет форум выделяет часть своих площадей для обмена мнениями между «безопасниками в пиджаках», а в этом году прошла ещё и серия встреч, посвящённых инвестициям в ИТ-компании ИБ-рынка. Их участники обсудили изменения на фондовом рынке и новые подходы к работе с инвесторами, состояние и перспективы рынка ИБ, опыт выхода на биржу... Обсуждалась, в частности, проблема слабой открытости внутренней жизни ИБ-компаний для рынка инвестиций. Эксперты отметили, что уровни осведомлённости глобальных инвесторов и инвесторов целевых существенно отличаются между собой.

Если как пример рассмотреть компанию Positive Technologies, то у неё уже больше 44 тыс. акционеров, 99% из них — физические лица. Топы компании рассказали, как планируют за год удвоить бизнес и привлечь не менее 100 тыс. акционеров. Заметную роль в повышении инвестиционной привлекательности компании сыграли и будут играть ежегодные PHDays. Одиннадцатый год подряд форум раскрывает разные грани жизни рынка ИБ в целом и Positive Technologies в частности.

«ПИДЖАКИ» НА PHDAYS

В рамках встреч «кибербеза в пиджаках» в нынешнем году наряду с оперативным обсуждением уже проявившихся и выявленных проблем «практической безопасности» (тех, что возникли из-за весеннего обострения в среде некогда партнёров России), устроители Форума сочли необходимым обсудить и долгосрочную стра-

тегию обеспечения так называемой цифровой трансформации. Это словосочетание следует рассматривать как «зонтичное» обозначение целого набора технических, организационных, экономических и даже политических процессов.

Для обсуждения в этом контексте проблем ИБ была проведена специальная панельная дискуссия, спикерами которой выступили представители «Росатома», Ростелекома, Центра компетенций по импортозамещению в сфере ИКТ, АНО «Цифровая экономика». Там были подняты на щит ряд фундаментальных проблем, причём акцент сделали на необходимости «переосмысления» самих технологий ИБ в парадигме «цифровой трансформации».

На секции «Без третьих лишних: защита supply chain» дополнили и развили содержание уже ставшей расхожей темы, что «дофевральские» модели угроз для ИБ не включали в качестве врага иностранного вендора или иностранное государство. Обсуждались также разные аспекты такого явления, как сознательная порча так называемого открытого кода (этот ресурс шаблоном рассматривается в качестве «быстрой» альтернативы коммерческому иностранному ПО).

На этой же секции речь зашла и о встраивании лживого «контента» на сайты СМИ и госучреждений. В связи с этим уместно отметить, что впервые в числе гостей PHDays была замечена директор департамента информации и печати МИД России Мария Захарова.

В эфирной студии форума М. Захарова отметила, что глобализация рынка информации и ускорение темпов «производства» и распространения информации на основе цифровых ИКТ вызвали своего рода «обратный эффект» в контексте как бы обретения вождельной «свободы слова». Сегодня человек, с одной стороны, с трудом воспринимает поток информации, а с другой — перестаёт доверять

информации. Этот «обратный эффект» стал особо заметен на фоне усиливающейся цензуры со стороны даже не государств, а просто крупнейших «западных» корпораций.

«Они начали своего рода „обратную политику“. От свободы слова к её ограничению в виде модерирования и прямого цензурирования», — заявила М. Захарова.

В связи с этим директор департамента информации и печати МИД России подчеркнула необходимость создания в стране своих цифровых продуктов и решений, которые бы обеспечили распространение информации, свободной от модерирования и цензурирования со стороны отдельных государств и даже людей.

«Нужно прекратить протекционизм и лоббирование в отношении западных цифровых продуктов, долгое время доминировавших на российском рынке. Для этого есть политическая воля, желание и возможности», — отметила М. Захарова.

«УЖАСНОЕ, НО СИМПАТИЧНОЕ». ПРО ХАРДКОР

Среди базовых ценностей Positive Hack Days — тесное общение «белых» хакеров, пентестеров, багбаунтеров. Эта могучая туса — десятки выступлений и активное общение в «кулуарах» — роится вокруг изюминки мероприятия — соревнований на киберполигоне The Standoff.

Нынешний The Standoff работал при организационном участии казанской ГК Innostage. Его эксперты взяли на себя задачу по развёртыванию инфраструктуры полигона и его поддержке, специалисты центра предотвращения киберугроз Innostage CyberART вели мониторинг «киберпротивостояния» и обеспечили демонстрацию цепочек реализованных атак гостям форума, а также выступили менторами одной из команд «защитников».



Фото: phdays.com

Одной из особенностей The Standoff 2022 стала демонстрация ужасов межотраслевого влияния, когда киберугрозы реализуются в КИИ разных сфер виртуального Города.

В этом году пять команд «синих» защищали Город, отслеживая перемещения атакующих «красных» внутри инфраструктуры, расследуя инциденты, изучая их техники и тактики. За четыре дня кибербитвы «синие» предоставили 287 отчётов об инцидентах и 10 отчётов о расследованиях. Среднее время расследования составило 9 часов 15 минут, а минимальное — 1 час 13 минут.

Победителями со стороны атакующих стала команда Codeby (она заработала 27 715 баллов), на втором месте — True0xA3 (23 381 балл) и на третьем — Invuls (12 352 балла). За четыре дня атакующие сдали 295 отчётов об уязвимостях.

На PHDays 11 была представлена платформа The Standoff 365 Bug Bounty. Она создана для объединения ресурсов корпоративных и индивидуальных игроков рынка ИБ в совместной работе по поиску уязвимостей и оценки защищённости организаций. Платформа позволяет компаниям со зрелыми процессами ИБ достоверно и объективно оценить защищённость бизнеса. В этом

году были предусмотрены награды не только за найденные уязвимости, но и за обнаруженные способы реализации недопустимых для бизнеса событий.

Также в рамках PHDays 11 прошли конкурсы по взлому банкомата, кассовой системы и POS-терминала (с денежными призами!), состязание по похищению NFT, а также финал первого Всероссийского конкурса проектов Open Source для школьников и студентов.

«ТЫ ЛУЧШЕ БУДЬ ОДИН, ЧЕМ ВМЕСТЕ С КЕМ ПОПАЛО»

Обстановка у входа в ЦМТ 18 мая 2022 года напоминала беспечные майские дни года этак 18-го. Однако сквозная тема PHDays 11 — вход в эру Independence — возвращала в нынешнюю реальность. Реальность, в которой сомнительно выглядело позиционирование форума как международного, а англоязычное наименование «новой эры российского кибербеза» и вовсе казалось неуместным на фоне окрысившегося «коллективного Запада» (ИМХО).

Хотя что-то в этом есть — ведь мир, судя по оценкам авторитетных экономистов и политологов, стоит на пороге регионализации экономик и геополитических интересов. А стало быть,

обеспечение безопасности в региональных «квартирах» уже не может строиться на основе глобальных цифровых технологий, рычаги управления которыми (как и кнопки на полное отключение) находятся в неконтролируемом Центре. И это открывает для нашей страны горизонты сотрудничества в сфере ИБ на самых разных иностранных языках.

Хотя ведь было и время, когда наши заказчики усердно учили русский.

ИТОГИ

По итогам PHD11 напрашивается вывод, что нынешняя ситуация в сфере ИБ хуже, чем хотелось бы, но лучше, чем можно было ожидать. А для повышения градуса оптимизма есть два основания.

Первое — это приходящее понимание о наличии вендора в модели угроз, что заставляет отечественный кибербез «искать свой путь, чтобы в дальнейшем мы были конкурентоспособны как в области ПО, так и в элементной базе — создании совместных предприятий полного цикла, специальных инвестиционных зон и прочего» (Николай Белобров, «Solar Интеграция»).

А второй — стратегия национальной безопасности России, рассматривающая кибервойну в качестве основания для несимметричного ответа.



КОНФЕРЕНЦИЯ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАНКОВ»

«ЕСТЬ БАНКИ, КОТОРЫЕ ЗНАЮТ, КАК ДЕЛАТЬ.
ОСТАЛОСЬ ТОЛЬКО СДЕЛАТЬ»

Отмена февральского уральского «ибэшного Давоса» имела и положительную сторону. Банковское сообщество сэкономило интеллектуальные ресурсы для анализа того безобразия, суть которого даже не удалось конвенционально сформулировать как тему ключевой дискуссии на конференции «Информационная безопасность банков».

Винить в этом безобразии можно только жадность российского государствообразующего бизнеса и обслуживающих его интересы россиян. Отказ в кормлении собственной промышленности сначала привёл к повинности кормления зарубежной ИТ-индустрии. А сегодня геополитические амбиции коноводов этой ИТ-индустрии доросли до уровня амбиций старухи из пушкинской сказки.

«Ответка» от золотой рыбки в пути, но ремонтировать разбитое корыто придётся в любом случае. И конференция выявила несколько подходов к организации этих самых «ремонтных работ». Первый подход — действия регуляторов.

КОМАНДА, ВО ФРОНТИ

После 24 февраля оперативные меры по корректировке «нормативки» стали

одним из ключевых факторов в повышении защищённости объектов КИИ и иных объектов, напрямую зависящих от устойчивости КИИ.

В своих комментариях к сложившейся ситуации Виталий Лютиков, заместитель директора ФСТЭК России, упоминал и скорую актуализацию 149-ФЗ, и упрощение процедур сертификации российских разработчиков, и наполнение новыми смыслами понятийного аппарата ИБ.

Последнее относится, в частности, к термину «сложные целенаправленные атаки» (advanced persistent threat, АРТ) и представлениям о злоумышленнике, организующем такие атаки. Как отметил В. Лютиков, сегодня злоумышленниками стали в первую очередь государства и компании-вендоры. А новыми технологиями для АРТ-атак становится отзыв сертификатов и недружественные обновления для «окирпичивания» оборудования. Эту тему развивал в своих комментариях и Сергей Корелов (НКЦКИ).

Как отметил замдиректора ФСТЭК России, в боевых условиях регуляторы оперативно вырабатывают, наряду с техническими, ещё и организационные меры по повышению защищённости объектов, направляя свои рекомендации в органы регионального и федерального уровня власти.

В общем, «...режь последний огурец!»

ГВОЗДИ БЫ ДЕЛАТЬ ИЗ ЭТИХ ЛЮДЕЙ!

Второй подход — действия работающего в сфере ИБ частного бизнеса и департаментов ИБ в финансово-кредитных организациях.

Работа этих структур, чьи логотипы мы привыкли видеть на баннерах и стендах в числе организаторов, партнёров и спонсоров ведущих мероприятий в сфере ИБ, определяется сегодня, как и всегда, правилом «делай, что должно, и будь что будет». С подчёркиванием, что если «как должно», то и будет как надо. Все эти отнесённые ко второй категории (по порядку упоминания, а не качеству) игроки рынка ИБ регулярно проводили киберучения, обобщённо оценивали угрозы со стороны заклятых партнёров-вендоров и знают матчасть не понаслышке.



Комплексная оценка действий частного бизнеса и департаментов ИБ прозвучала в комментариях замдиректора Департамента ИБ Банка России Андрея Выборнова и директора Департамента обеспечения кибербезопасности Минцифры Владимира Бенгина.

По мнению финансового мегарегулятора, на текущем этапе войны банковская отрасль отразила все атаки. Но, как тут же отметил А. Выборнов, нет оснований почитать на лаврах, «предстоит серьёзная работа, связанная с совершенствованием способов защиты и наращиванием темпов и масштабов импортозамещения».

Оценка ситуации в отрасли со стороны Банка России практически совпала с оценкой представителя Минцифры. По

его мнению, «мы» адекватно среагировали на проявившиеся риски, «так что даже было незаметно, что есть какая-то деградация».

И здесь уместно добавить, что начавшаяся 24 февраля спецоперация помимо заявленных целей ослабила напряжённость на некоторых участках внутреннего фронта — фронта борьбы с мошенничеством в финансовой сфере. По данным Минцифры, 24 февраля количество мошеннических звонков упало практически до нуля, а в марте их число составило лишь треть от мартовской величины прошлого года. Представитель Лаборатории Касперского, подтвердив информацию о сокращении мошеннических звонков, упомянул также



и о мартовском падении активности вирусов-шифровальщиков.

Комментарий Сергея Голованова, главного эксперта по безопасности из Лаборатории Касперского, прозвучал на сессии, посвящённой «противодействию кибератакам в финансовой сфере, развитию центров мониторинга ИБ и процессов реагирования на инциденты». Модератором сессии был Дмитрий Гадарь, вице-президент, директор департамента ИБ «Тинькофф Банка», и его «подопечными» на сессии были затронуты не только оперативные вопросы противодействия кибератакам и описания нынешнего «ландшафта» киберугроз (включая вопрос об открытой вербовке в «даркнете» пятой колонны продажных сотрудников). Эксперты также «послали свою кукурузу вперёд» и заглянули в будущее — поделились мнениями о перспективах и технологиях борьбы с инсайдерами «когда всё закончится», высказали личные мнения о сути проблемы кадрового обеспечения СОСов и о возможностях разворачивания СОС «по кнопке» за счёт стандартизации правил.

В общем, «...а караван идёт».

«А МЫ ПОЙДЁМ НА СЕВЕР!»

Третий подход к поведению «после 24 февраля» продемонстрировал бизнес. Правильнее даже говорить о целом «букете» подходов. И один из «цветков» — это аллюзия на известную студенческую тему, когда экзаменатор выбирает из альтернативы выгнать сразу или

разрешить пересдачу, а студент просит четвёрку. Тут хороший пример — просьбы о приостановлении санкций в отношении финансовых учреждений, не реализовавших до 24 февраля комплекс мер по импортозамещению. О такой инициативе рассказал в ходе ключевой дискуссии Алексей Войлуков, вице-президент АБР. Авторы инициативы ссылаются на то, что «даже если есть полноценные отечественные аналоги СЗИ, то быстро их внедрить в крупных и средних банках не так просто».

Но зачем «быстро»? Кто мешал «перекреститься» до того, как «грянул гром»?

Одним из ответов на такую «аргументацию» стала инициатива ФСТЭК по разработке документа по упрощению ряда процедур сертификации российских разработчиков. Как пояснил Виталий Лютиков, документ касается и процедурных вопросов, и вопросов, связанных с отработкой отдельных положений требований доверия.

Ещё один стиль поведения бизнеса заставляет вспомнить «воспоминания» короля из шварцевского «Обыкновенного чуда»: «Во мне проснулся дед с материнской стороны. Он при малейшем несчастье ничего не предпринимал, надеялся на лучшее. Когда при нём душили его любимую жену, он стоял возле и уговаривал: потерпи, может, обойдётся».

Этот литературный фрагмент в очередной раз пришёл на ум во время круглого стола «Санкции. Новая старая реальность». Один из обсуждавшихся на нём вопросов — «Отечественный

HSM в платёжных системах — это реальность или несбывшийся проект ЦБ?». В качестве рефери выступил Артём Сычёв, а в виртуальных «красном» и «синем» углах круглого стола расположились Вендор (Дмитрий Гусев, АО «ИнфоТеКС»; Владимир Простов, «КриптоПро») и Заказчик в лице представителей комитета по ИБ АБР и Ассоциации ФинТех.

Признание Заказчиком возможности использовать отечественный HSM в платёжных системах и его готовность начать финансирование проекта по внедрению отечественного оборудования оказалось бы не только важным шагом по вытеснению зарубежных вендоров с нашего рынка, но и заложило бы фундамент для выхода в перспективе отечественных компаний на зарубежные рынки тех стран, для которых конкуренция коллективного Запада с Россией является инструментом для обеспечения технологической независимости от монополии политической конъюнктуры.

При этом уместно заметить, что в ходе дискуссии представитель «ИнфоТеКС» напомнил присутствующим о не раз возникавшей необходимости «допиливаний по месту» при внедрении даже как бы «коробочных» зарубежных HSM-продуктов.

К сожалению, Заказчик уклонился от прямого ответа на вполне конкретные предложения «ИнфоТеКС» и «КриптоПро» о возможных сроках реализации пилотного проекта, а также от обсуждения тех компромиссов, на которые ему предлагали пойти.

В своих интересах бизнес пытается даже разыграть карту несостоявшегося «отъезда айтишников». На конференции упоминалось об обращении АБР в Центробанк и правительство с просьбой расширить налоговые и иные послабления для своих подопечных «под соусом» стимулирования работы ИТ-специалистов в финансовых учреждениях.

Но разве интересная, нужная работа и хорошая зарплата — это недостаточные стимулы? Или чего из этого набора нет в жизни банковских «айтишников»?

Уместно заметить, что не так давно прошла информация и о «шаге конём» — о заявке руководству страны на прямое признание банков ИТ-компаниями.

В общем, «...а кому мать родна».

ФОРУМ DLP+ 2022

DLP КАК ПОВОД

Успех в решении формальной задачи Форума DLP+ 2022 был предопределён ходом ряда предыдущих событий. Пресса на протяжении последних лет держит в «подогретом» состоянии тему утечек, виновниками которых являются сотрудники пострадавших организаций. На «пленарке» апрельского CISO Форума была затронута тема «саботажников» (не путать с «уехавшими айтишниками»), а от саботажа до инсайда путь недлинный. На апрельской же конференции «Информационная безопасность банков» обсуждался вопрос об открытой вербовке в «даркнете» сотрудников, готовых содействовать размещению зловредных программ в корпоративной инфраструктуре. На майском PHDays 11 провели полномасштабную секцию «Скандалы, интриги, расследования: как защититься от утечки данных».

Словом, устроителям Форума DLP+ 2022 оставалось только дожидаться 1 июня, чтобы сорвать свой джекпот. Причём для этого даже не потребовалась центральная сцена Дома предпринимателя на Покровке. Немалую аудиторию тех, кто уже «созрел» или близок к этому, собрал кулуарно расположенный «зал 2», в котором и прошёл трек «Применение DLP на практике. Реальные кейсы».

РАСШИРЕНИЕ ВОЗМОЖНОСТЕЙ

«Зубры» рынка представили здесь широкий спектр рекомендаций по эксплуатации систем класса DLP: от тех, что позволяют быстро «сконфигурировать» систему и экономно её эксплуатировать, до тех, что позволяют расширить список «добавленных стоимостей» от использования систем класса, скажем так, DLP+. Как оказывается, современный программный комплекс, продаваемый под маркой «система DLP», по своим возможностям выходит далеко за пределы функциональности для выявления

фактов утечек данных за периметр и расследований по этим инцидентам.

Система класса DLP+ позволяет мониторить даже состояние такого нематериального параметра, как рабочая атмосфера в коллективе, не говоря уже о таких вполне экономических материях, как учёт рабочего времени и уровень загрузки оборудования.

Наиболее образно такие «дополнительные» возможности представил в своём докладе директор по ИБ

ГК «Сегежа». Он сравнил систему DLP со швейцарским ножом, причём КАЖДЫЙ инструмент из немалого их числа в швейцарской игрушке был сопоставлен с реализованной на предприятии функциональностью.

Именно эта «многогранность» современного DLP-комплекса и позволила привести в соответствие с реальностью устаревшее название подразделения — отдел ИБ — в одной из организаций. Отдел преобразовали





в Департамент обеспечения бизнеса группы компаний. О предпосылках такой трансформации рассказал Иван Дмитриев (TalentTech) на треке «DLP и всё вокруг. Место DLP в системе безопасности».

DLP + ИИ

Понятно, что, став «службой» больше чем «двух господ», система класса DLP + стала гораздо сложнее в настройке, но и здесь вендоры стараются идти в ногу со временем. В частности, компания InfoWatch в докладе «Другие времена — другая DLP» представила возможности так называемого искусственного интеллекта в части помощи в настройке политик, которые теперь в зависимости от обстоятельств могут быть перенастроены если не в считанные часы, то практически за день.

Уместно заметить, что не все участники дискуссии на треке «Применение DLP на практике...» разделяли оптимизм InfoWatch по части внедрения ИИ в DLP. И для тех, кто считает внедрение ИИ в DLP преждевременным, кому не нужен «швейцарский нож», компания «Атом Безопасность» предложила свой комплекс Staffcop — «для контроля над информационными потоками и действиями сотрудников». Компания не маркирует своё DLP-предложение постфиксом «+», но указывает, что Staffcop имеет и функциональность SIEM.

КАК ОБОСНОВАТЬ

О том, как обосновать приобретение системы DLP, состоялась целая дискуссия, в которой принял участие Андрей Масалович, президент консорциума «Инфорус», известный на просторах

YouTube под ником Кибердед — по результатам своей просветительской деятельности в сфере ИБ. Не будучи лицом «лично прямо или косвенно заинтересованным», он набросал несколько бюджетных схем апробации DLP-системы в организации с одновременным причинением немедленной пользы, а также продемонстрировал убедительные технологии убеждения руководства в приобретении системы.

А как лицо лично заинтересованное в повышении уровня ИБ в стране, А. Масалович привёл ряд соображений в пользу объективной полезности DLP и обратил внимание аудитории на те угрозы, которые в ближайшем будущем (сразу по возвращении к родным пенатам) слушателям Форума придётся решать. Включая проактивное выявление неадекватного «админа»,



который по приходе на службу в какой-то момент может «обрушить» всю ИТ-инфраструктуру компании по политическим мотивам.

НЕ ПРИШЛО ЕЩЕ ВРЕМЯ?

Не осталось без внимания Форума и то обстоятельство, что большинство своих «+ возможностей» современная система DLP реализует благодаря детальному сбору данных о практически каждом сотруднике организации. То есть персонал, эксплуатирующий DLP-систему, в силу служебной необходимости получает доступ к зачастую достаточно личной информации сотрудника. Если тот совершает действия, не вполне безопасные с точки зрения общих представлений о мерах сохранения в неприкосновенности личного информационного пространства.



Проблематика возникающих при этом коллизий обсуждалась на треке «Применение DLP на практике. Реальные кейсы» и в ходе дискуссии «Экономическая безопасность и правовое обеспечение DLP», в которой приняли участие три профильных юриста. И хотя и здесь, и ранее, на PHDays 11, поднимались вопросы правоприменительной практики в этой сфере, похоже, время простых правовых решений применительно к DLP-криминалистике ещё не наступило.

ВРЕМЯ СОБИРАТЬ КАМНИ

Целевые задачи Форума DLP+ 2022 «упали» на «почву», уже подготовленную усилиями коллег «по цеху» к адекватной оценке угроз инсайдерства.

А Форум, в свою очередь, внёс свой вклад в подготовку общества к осознанию ситуации, в которой придётся работать в ближайшей перспективе.

На дискуссии «Кому принадлежит будущее» Егор Кончаловский посетовал на потерю «западной мечты», которой некие «Мы» грезили «всё детство и юность».

В отличие от юного Кончаловского, российский «айтишник» и/или «ибэшник», даже если он и не хотел жить «как на Западе», последние два десятилетия был вынужден так жить. Нынешние CISO были поставлены в условия, когда предложенные им правила ИТ-«игры» не предусматривали использование советского опыта построения критических инфраструктур на принципах автаркии от «западных»

поставок и принципах технологической независимости.

Вместо этого новоиспечённое руководство страной и экономикой выставило рейтинг «бесконечного доверия» зарубежным поставкам, закачивая деньги в зарубежную отрасль ИТ.

Отечественный же ИТ-отрасли было предложено самостоятельно нарисовать себе «образ будущего» на основании внедрённой в умы её лидеров мечты «жить как на Западе» и, добавим, принципов работы «как на Западе».

И Форум подсветил результаты этого процесса на ключевой дискуссии «Текущие технологии, новейшие угрозы. Как правильно бороться с инсайдерами».

В качестве примеров достигнутого состояния отрасли уместно привести прямые цитаты:

«... бизнес не сможет создать СУБД в рамках рыночной конкуренции, потому что нет таких инвестиций, возможностей».

«... чтобы обеспечить устойчивость к нагрузкам, нам нужно нагрузочное тестирование на оборудовании, которое не может закупить бизнес».

Но особенно запомнилась следующее высказывание: «Те, кто хочет большую гарантию от вендора, просят продать им сертифицированную версию. В этом случае ПО прошло более тщательный и специализированный контроль и установлено соответствие с документацией, [что] отсутствуют недokumentированные возможности».

В этот момент вспомнился незабвенный Воланд и его аксиома о свежести.



Дмитрий МАХАЕВ
эксперт

ВОПРОС XXI ВЕКА

НУЖЕН ЛИ ВАМ СВОЙ SOC И ЦЕНТР ГОССОПКА?

В 2021–2022 годах в России и мире значительно возросли риски, связанные с угрозами кибербезопасности. Тема ИБ стала особенно актуальной в начале 2022 года, когда хактивизм стал более распространённым явлением. На волне этих событий многие организации задумались о создании собственных центров мониторинга и реагирования на инциденты информационной безопасности (SOC, Security Operations Center), в том числе и для соблюдения требований законодательства. Напомню, что 1 мая 2022 года вышел указ президента, прямо возлагающий персональную ответственность за киберинцидент, произошедший в субъекте критической информационной инфраструктуры (КИИ), на руководителя организации или его заместителя.

При этом в России давно функционирует Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА), которая в сознании многих ассоциируется с SOC на уровне предприятия, что не совсем верно.

А ЧТО НЕ ТАК-ТО?

ГосСОПКА действительно предназначена для выявления и обмена информацией о компьютерных атаках. Это иерархическая организационно-техническая структура, находящаяся в эксплуатации НКЦКИ (Национального координационного центра по компьютерным инцидентам). ГосСОПКА выполняет функции, схожие с функциями SOC, однако утверждать, что

получение статуса центра ГосСОПКА автоматически означает, что у вас появился SOC, закрывающий все ваши потребности, неверно. И вот почему:

1. Основное назначение ГосСОПКА — выявлять атаки на объекты КИИ и проводить мероприятия по ликвидации последствий таких атак и снижению вероятности их повторного возникновения. SOC же должен реагировать на кибератаки, направленные на все ИТ-системы предприятия, а не только на КИИ.

2. ГосСОПКА — это крупная организационная система, которая состоит из совокупности SOC. Они обмениваются информацией с вышестоящим или головным центром ГосСОПКА и покрывают разнообразные предприятия. При этом система не привязана к процессам конкретной организации и направлена на решение задач защиты только объектов КИИ. SOC предприятия — это организационная единица, тесно привязанная (в идеале) к процессам конкретной организации, задачи которого не ограничиваются только защитой объектов КИИ.

Получение статуса корпоративного центра ГосСОПКА даёт вам право взаимодействовать напрямую с НКЦКИ по ряду вопросов в рамках заключённого соглашения о взаимодействии. При этом в документе обычно явно прописываются конкретные зоны ответственности и права корпоративного центра ГосСОПКА. Но помимо прав, соглашение о взаимодействии накладывает и определённые обязанности. Поэтому, прежде чем делать дальнейшие шаги по созданию корпоративного

центра ГосСОПКА, давайте ответим на вопрос...

ДЛЯ ЧЕГО ВАМ НУЖЕН КОРПОРАТИВНЫЙ ЦЕНТР ГОССОПКА?

Первый ответ обычно — для выполнения требований, определённых в № 187-ФЗ. Закон обязывает уведомлять об инциденте НКЦКИ (а для организаций кредитно-финансовой сферы — и ФинЦЕРТ Банка России).

Но обратите внимание, что нигде не приводится требование, что уведомлять НКЦКИ может только корпоративный центр ГосСОПКА!

Более того, создание корпоративного центра ГосСОПКА влечёт за собой большое количество организационно-методической работы и согласований как внутри организации, так и с НКЦКИ. Не исключено, что ваш SOC, который закрывает в текущей реализации все потребности организации, банально не будет удовлетворять всем требованиям, предъявляемым НКЦКИ к корпоративному центру ГосСОПКА. В итоге вам придётся выделять дополнительные бюджеты на увеличение ставок в подразделении, закупку новых технических средств и т.д. Не каждый бизнес готов на это пойти, ведь в конечном счёте это может быть неоправданно: получаемая выгода, такая как возможность работать по ряду вопросов с НКЦКИ напрямую, иногда может быть меньше затрат.

Кроме того, не следует забывать, что присвоение статуса корпоративного центра — это право, а не обязанность НКЦКИ. Они могут и отказать.

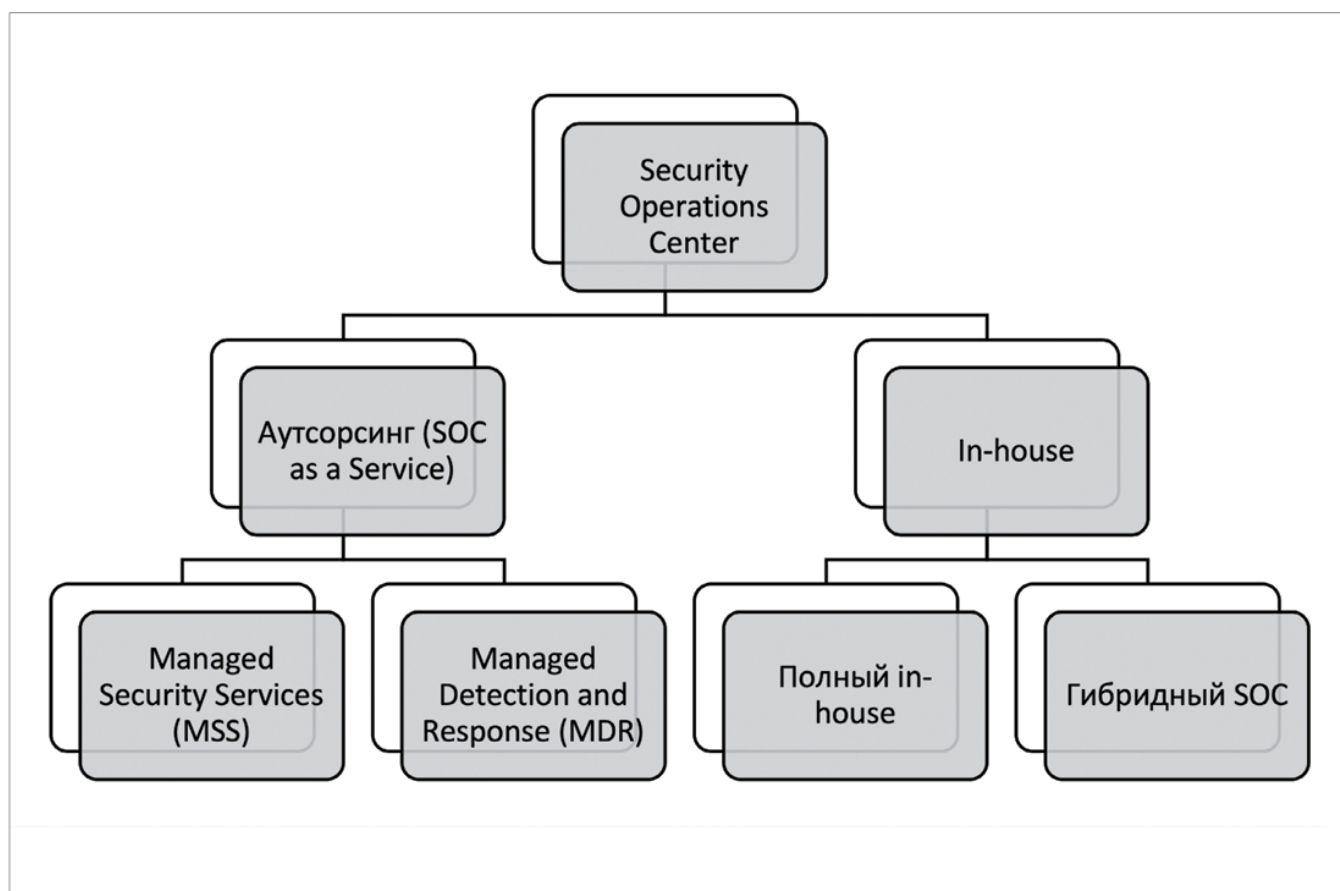


Рисунок 1. Условно типы SOC можно представить так

И КАК ПОНЯТЬ, НУЖЕН ЛИ КОРПОРАТИВНЫЙ ЦЕНТР ГОССОПКА ИЛИ ПРОЩЕ ОСТАТЬСЯ В СТАТУСЕ SOC?

Итак, когда есть смысл создавать корпоративный центр ГосСОПКА? Смысл есть, если вы подходите хотя бы под два формализованных условия из перечисленных:

1. Вы — субъект КИИ (или станете в скором времени).
2. У вас крупная, территориально распределённая организация (филиальная сеть либо сеть с дочерними зависимыми обществами).
3. Вы находитесь в списке стратегических предприятий (см. ежегодно обновляемый Указ Президента РФ от 04.08.2004 № 1009).

В этом случае выгода от создания корпоративного центра ГосСОПКА для всех участников процесса перевешивает все трудности (перестройка внутренних процессов, дополнительные траты на приведение своего структурного подразделения в соответствие

требованиям НКЦКИ, разработка, утверждение и согласование соответствующей методологии).

Во всех прочих вариантах — корпоративный центр вам не нужен. Выполнять требования законодательства вы можете либо путём заключения соответствующего соглашения с НКЦКИ (без получения статуса корпоративного центра), либо передавая данные через коммерческий SOC или ведомственный центр ГосСОПКА (который, в свою очередь, доведёт их до НКЦКИ).

ВЫ ВСЁ ЖЕ РЕШИЛИ СТРОИТЬ КОРПОРАТИВНЫЙ ЦЕНТР. ЧТО ДАЛЬШЕ?

В любом случае, будете вы становиться корпоративным центром или нет, начать следует с создания собственно SOC.

А прежде чем строить, нужно решить ряд организационных вопросов.

♦ Тип SOC: будет он полностью на аутсорсинге или частично (гибридная модель)? Или целиком внутри организации (in-house)?

♦ Готова ли организация в принципе к появлению SOC? Существуют ли соответствующие организационно-распорядительные документы? Готовы ли смежные подразделения к взаимодействию? Успех реагирования на инцидент во многом зависит от того, насколько чётко налажен процесс взаимодействия!

♦ Если отдаётся на аутсорсинг (целиком или частично), то что именно отдаётся? Какая целевая модель аутсорсинга?

Условно типы SOC можно представить так, как показано на рис. 1.

Основная разница между типами SOC приведена в таблице 1.

С точки зрения организации, все подходы одинаково хорошо выглядят в глазах регулятора. Несмотря на это, многие начинают с ходу строить in-house, собирая следующие подводные камни.

Забыв о том, что «SOC = процессы + технологии + люди», начинают сразу с людей или покупки техники. В итоге получается перекосяк: люди и техника

АУТСОРСИНГ

Тип и особенности	Основные плюсы	Основные минусы
MSS В первую очередь направлен на соблюдение комплаенса, отработку и выявление типовых атак; Может выполнять повышение осведомлённости сотрудников; Защита от DDoS-атак и атак на веб-приложения.	Обычно более квалифицированный персонал, чем в in-house; Наличие готовых Playbook и Runbook; Накопленный экспертный опыт по выявлению и реагированию на инциденты; У MDR, как правило, развитая форензика, умение выявлять и реагировать на APT-атаки и нетиповые (неизвестные) атаки, развитый Threat Hunting; CAPEX низкий или отсутствует (затраты предсказуемые); Быстрое развёртывание, результаты возможно получать уже в первые месяцы работы; Работа 24x7; Наличие необходимых лицензий ФСТЭК, ФСБ на оказание услуг (важно, так как для in-house может потребоваться получение лицензии в случае оказания услуг ДЗО); Обычно уже центр ГосСОПКА.	Меньшее погружение в инфраструктуру по сравнению с in-house; Зависимость от каналов связи выше, чем у in-house.
MDR Делает всё то же самое, что и MSS, но в дополнение: Развитый процесс Threat Hunting; Компетенции по выявлению сложных атак реагированию на них и их расследованию (в т.ч. проправительственных APT-группировок); Имеет (либо может оперативно разработать) нетиповые сценарии выявления и отработки инцидентов ИБ); Может выполнять функции частичного или полного администрирования СЗИ заказчика.		

IN-HOUSE

Тип и особенности	Основные плюсы	Основные минусы
Гибрид	Разумный баланс между «дорогими» и «дешёвыми» специалистами; Часть основного инструментария (SIEM и проч.) может быть у вас; Экспертиза аутсорсера (Playbook, Runbook, их доработка); Обычно хорошее понимание своей инфраструктуры.	CAPEX-затраты всё равно присутствуют; Средние возможности масштабирования; Дольше (по сравнению с MSS/MDR) развёртывается.
Полный in-house «Всё у себя». Полностью контролируемый SOC, слабо зависящий от контрактных отношений	Хорошее понимание собственной инфраструктуры; Быстрый (в теории) процесс реагирования за счёт сокращения цепочки отдающих команды. Но на практике это часто нивелируется «просадками» во время выполнения реагирования из-за нехватки опыта у специалистов, особенно для сложных инцидентов.	Большой CAPEX, OPEX; Непредсказуемость затрат; Обычно более низкая квалификация специалистов (если только не крупная организация); Долго запускать (от 2 лет); Зачастую не самым оптимальным образом организованные процессы (за счёт отсутствия экспертного опыта); Проблемы найма и удержания квалифицированных специалистов.

Таблица 1. Основная разница между типами SOC

есть, а работа не идёт. Считайте, потеряли год сразу.

В процессе постройки SOC выясняется, что нужно провести кучу параллельных работ (инвентаризация, аудит, оценка текущего состояния защищённости, улучшение/дозакупка/донастройка СЗИ и т.д.). Но из-за отсутствия опыта построения SOC и очерёдности процессов глобальная задача разделяется на множество мелких процедур, и всё зависает в бесконечных согласованиях. Итог: руководство теряет интерес к этим начинаниям.

Упираясь в тот факт, что невозможно организовать какой-то поддерживающий процесс или сделать оптимальный Playbook и, как следствие, Runbook, операционная деятельность проседает.

Проблемы удержания квалифицированного персонала. Всё упирается не только в зарплату, но и в отсутствие интересных задач для второй или третьей линии. К примеру, если вы возьмёте высококвалифицированного специалиста по форензике, то долго его не удержите: при отлаженных процессах по мониторингу и реагированию на инциденты ИБ-задач, требующих работы форензера, будет от силы 2–3 в год. Остальное время специалист будет либо ничего не делать, либо выполнять неинтересную ему работу. И тогда начнёт искать другое место, где его навыки будут более востребованными.

Реальная отдача при полностью самостоятельной постройке SOC — не ранее, чем через 2–3 года. Вы уверены, что бизнес согласится столько ждать?

Вы уверены, что на пути постройки не совершите никаких иных ошибок, которые могут стать фатальными и свести на нет усилия по построению SOC? Например, неверная оценка числа событий, приходящих на SIEM, ошибки при проектировании архитектуры и иные.

ПРО ПОЛУЧЕНИЕ СТАТУСА

С точки зрения получения статуса корпоративного центра ГосСОПКА всё просто. Вы пишете официальное письмо от имени руководителя организации либо его заместителя по контактам, указанным на сайте НКЦКИ (cert.gov.ru). В нём сообщаете о своём желании создать корпоративный

центр ГосСОПКА и объясняете его необходимость. В случае если в НКЦКИ решат, что вы всё-таки можете в теории получить статус, вам пришлют необходимые методические рекомендации, по которым вы должны будете собрать необходимые данные и передать их в НКЦКИ, а также обеспечить проведение иных мероприятий. В процессе вы заключаете безвозмездное соглашение о взаимодействии с НКЦКИ и после успешного подписания получаете статус и обязанности корпоративного центра. Обязанности определяются соглашением о взаимодействии, а также иными документами НКЦКИ.

Повторно отмечу, что возможность заключения соглашения с НКЦКИ не коррелирует напрямую с получением статуса корпоративного центра ГосСОПКА: вы можете заключить соглашение о взаимодействии без этого статуса.

В то же время получение статуса корпоративного центра ГосСОПКА накладывает обязанности по уровню технического оснащения и компетенции персонала, которые может быть трудно выполнить. Поэтому задача построения работоспособного SOC (который включает, в частности, проверку навыков сотрудников на киберполигонах — иначе как быть уверенным, что в нужный момент все будут знать, как действовать) встаёт особенно остро.

И КАК ПОСТУПАТЬ?

Существует более-менее универсальный рецепт построения SOC, который позволяет соблюсти разумный баланс между временем создания, качеством функционирования и затратами, а также соответствием необходимым требованиям НКЦКИ.

Рецепт 1: отдать всё на аутсорсинг. Просто и быстро. Вопреки распространённому мнению, 99% инцидентов — типовые и не являются уникальными для какой-либо организации. Для выявления и защиты от таких атак разработаны соответствующие сценарии, а с учётом опыта аутсорсера сценарии многократно отработаны и выверены и подойдут для подавляющего большинства заказчиков. Работоспособный SOC у вас возникнет в считанные недели, а

персонала в вашей организации потребует минимум.

Рецепт 2: пойти по пути создания гибридного SOC. В этом сценарии мы значительно сокращаем время и средства до появления нормального работающего SOC. Это считается в настоящее время оптимальным путём. Он заключается в следующих шагах (таблица 2).

ЗАКЛЮЧЕНИЕ

Итак, большинству организаций корпоративный центр ГосСОПКА не нужен, особенно если их основная цель — это формальное закрытие требований законодательства. Тут проще и дешевле отдать всё на аутсорсинг. Но если вы:

- ♦ в перечне стратегических организаций,

- ♦ имеете большую филиальную сеть либо ДЗО,

- ♦ и вы — субъект КИИ,

то смысл в собственном центре ГосСОПКА есть. При этом готовьтесь понести определённые затраты (как ресурсные, так и материальные), чтобы создаваемый центр соответствовал всем требованиям НКЦКИ. Если вы создаёте свой SOC, без получения статуса корпоративного центра ГосСОПКА, то вы можете применять разные практики. Но как только речь заходит о получении советующего статуса, готовьтесь строго учитывать все рекомендации и требования НКЦКИ.

Но в любом случае нужно, чтобы центр ГосСОПКА функционировал не на бумаге, а в реальности. А это процессы, техника, люди.

«Просто» SOC, напротив, нужен сейчас практически всем. Но современные реалии таковы, что построить его полностью in-house способны лишь крупные предприятия, которые смогут не только нанять, но и удержать дорогостоящих специалистов в компании.

Кроме того, как показала практика, для расследования серьёзных инцидентов всё равно привлекается сторонний подрядчик, у которого есть — внезапно — свой MSS/MDR SOC.

Нужно отметить, что концепция полного in-house SOC постепенно изживает себя именно из-за того, что трудно удержать ценные кадры.

Поэтому оптимальный вариант — гибридный SOC с передачей ряда

Шаг	Что делаем	Для чего
1	Выбираем и заключаем договор с организацией, предоставляющей услуги MSS/MDR SOC. Важный момент: организация должна иметь соответствующие лицензии на оказание услуг, а также оказывать услуги по построению SOC на стороне заказчика. Желательно также, чтобы подрядчик мог организовать проверку знаний сотрудников на киберполигоне и при необходимости организовать повышение их квалификации.	Получаем экспертный опыт по построению SOC: какие процессы нужно внедрить/оптимизировать, готовые Playbook и Runbook. Не нужно пугаться «шаблонных» Playbook: обычно у аутсорсера накоплен большой экспертный опыт, а 99% инцидентов — типовые; сценарий реагирования на них слабо зависит от конкретной организации. В силу большого объема заказчиков, как правило, наработаны сценарии под организации практически любой отрасли; сразу встаём под защиту (фактически SOC начал работать); если вы намерены строить корпоративный центр ГосСОПКА, то подрядчик поможет вам оценить необходимость его создания и окажет необходимые консультации, повышающие шансы получения положительного решения у НКЦКИ; имеем возможность найти и адаптировать сотрудников «под себя»; ряд технических мероприятий, необходимых для запуска SOC, способен провести подрядчик; итогом станет фактическое начало работы SOC и минимизация рисков совершения типовых ошибок при его построении.
2	Выстраиваем процессы по взаимодействию на своей стороне.	При выявлении инцидента потребуются привлечение смежных подразделений (ИТ-служба, иные подразделения); подрядчик может оказать помощь по выстраиванию процессов взаимодействия и фиксации соответствующих регламентов и SLA по взаимодействию; итогом станет готовность смежных подразделений отрабатывать инциденты и давать обратную связь по результатам их устранения.
3	Определяем перечень сервисов, которые готовы забрать на себя.	На основе отчётов подрядчика о типовых инцидентах ИБ вы определите, что сможете держать у себя, бюджеты на ФОТ и на технику, отдать подрядчику дорогостоящие сервисы (например, компьютерную криминалистику); итогом должна стать согласованная «дорожная карта», показывающая, какие функции остаются у подрядчика, какие переходят заказчику и сроки перехода.
4	Набираем людей, проводим необходимые процедуры по закупке и внедрению нужных средств (при поддержке аутсорсера).	Не прерываем основную деятельность SOC (инциденты выявляются, реагирование производится силами подрядчика, пока проходят все процедуры); разрабатывается дорожная карта перехода сервиса от подрядчика к заказчику; итогом должна стать набранная команда и внедрённые технические средства для конкретного этапа «дорожной карты».
5	При поддержке аутсорсера подготавливаем персонал и забираем сервисы.	С помощью подрядчика проводится проверка навыков персонала для дальнейшей передачи сервиса без деградации качества; при необходимости организовывается обучение и повторная проверка навыков персонала; итогом должна стать передача сервиса в зону ответственности заказчика в соответствии с разработанной «дорожной картой».
6	Повторяем шаги 4–5 до достижения необходимого результата.	В соответствии с «дорожной картой».
7	ИТОГ: работающий гибридный SOC.	Для передачи инцидентов в НКЦКИ можно использовать либо сервисы подрядчика, либо путём заключения соответствующего соглашения с НКЦКИ (обязательное наличие статуса корпоративного центра не требуется); в случае если вы строите корпоративный центр ГосСОПКА, на этом этапе вы готовы выполнять соответствующие мероприятия, если не начали их исполнять ранее.

Таблица 2. Рецепт 2: пойти по пути создания гибридного SOC

дорогостоящих функций, требующих высококвалифицированных специалистов, — на аутсорсинг в коммерческий SOC, обладающий всеми необходимыми лицензиями и опытом. Кроме

того, использование гибридной модели значительно упростит процесс повышения компетенций ваших специалистов за счёт проведения тренировок на киберполигонах (эту услугу обычно

предлагают современные коммерческие SOC), а также вы всегда можете быть уверены, что вас поддержат при реагировании на сложные инциденты и при их расследовании.

ИБ-РЕШЕНИЯ ПО МОДЕЛИ OPEN SOURCE

КАК СРЕДСТВО ИМПОРТОЗАМЕЩЕНИЯ



**Александр
ГЕРАСИМОВ**
эксперт BIS Journal

Кибератаки на IT-инфраструктуру госорганов и бизнеса активно продолжаются. Спрос на средства защиты растет, а зарубежные вендоры, поставляющие ИБ-решения, уходят из России. Есть мнение, что дефицит продуктов в этой сфере можно быстро сократить, импортозаместив их IT-продуктами с открытым исходным кодом. Расскажу, как обстоят дела с этим на сегодняшний день.

Почему нельзя полностью заменить ушедших вендоров? На рынке есть множество хороших и бесплатных решений, которые могут использоваться как маленькие, так и крупные фирмы. В основном это средства для тестирования кода и выявления уязвимостей в приложениях. Но также много и тех, что не в состоянии обеспечить достойную замену из-за нехватки функциональности и плохой поддержки. Стартапы или средний бизнес могут почти полностью закрыть потребности в защите Open Source, за исключением антивирусов, WAF и DLP-технологий.

Энтерпрайз сегмент не может позволить себе полностью перейти на Open Source из-за требований к необходимому уровню стабильности и поддержки. Например, там огромное количество конечных устройств пользователей — ПК, ноутбуков, телефонов, которые нужно защищать. В каждый момент времени отслеживать аномальное поведение, вирусы, обновления ПО и риски. Open Source-решений для таких задач нет, либо они работают неточно. Выходом из этой ситуации может стать только выбор подходящего отечественного решения, либо индивидуальная

кастомная доработка существующих Open Source-решений.

Один из важных средств защиты — класс решений SIEM. Они агрегируют события операционной системы, логи и выдают аналитику об угрозах. Это позволяет центру реагирования следить за аномальной активностью и трафиком.

SIEM-решений на базе Open Source есть несколько. Но они применимы только в небольших компаниях, где немного источников событий. Энтерпрайз не может всерьез рассматривать их, как замену из-за отсутствия привычных функций и стабильной поддержки. После ухода текущих вендоров они будут искать тех, кто работает с рынком РФ, либо отечественного производителя.

Игнорировать обновления и оставить средства защиты на текущем уровне тоже не выход — постоянно появляются уязвимости нулевого дня, которые могут проэксплуатировать. При этом вполне реально обеспечить, например, безопасность приложений с помощью Open Source. Многие решения позволяют реализовать процессы безопасной разработки на Open Source.

Станет ли больше отечественных ИБ-решений с Open Source-компонентами? Существует около пяти популярных продуктов на российском рынке, основанных на Open Source. Чаще всего это различные сканеры уязвимостей, а также решения Anti-DDoS и WAF.

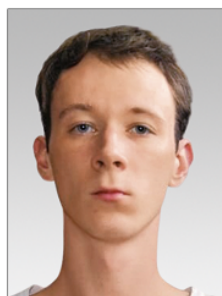
С учетом ухода с рынка зарубежных вендоров, поставляющих ИБ-решения, скоро российских ИБ-решений на базе Open Source станет больше. Даже мы в Awillix используем Open Source-сканеры

внутри своего продукта — регулярно мониторинга уязвимостей, который непрерывно оценивает уровень защищенности цифровых активов компании 24/7. Разные инструменты могут давать разный результат. Чтобы покрыть периметр заказчика как можно большим количеством проверок, можно использовать, в том числе OpenSource-решения. Это позволяет агрегировать все найденные недостатки и контролировать их исправления из централизованной платформы.

Риски и преимущества Open Source сегодня. Open Source — не всегда синоним «бесплатно». Конечно, ты демонстрируешь свой код, при этом можешь его продавать. Как правило производители продуктов на базе Open Source зарабатывают на добавочной стоимости продукта: это может быть крутой веб-интерфейс с дашбордами и аналитикой, или платная подписка с дополнительными возможностями, или подключение дополнительных пользователей.

Риски использования Open Source только в том, что исходный код открыт и в нем легче искать уязвимости, нежели искать их, не имея никакого представления о его внутреннем устройстве.

Преимущества Open Source в том, что решения не попадут под санкции. Если они классные, то комьюнити самостоятельно их развивает. Люди могут свободно дорабатывать код, влиять на проект и добавлять функциональности, просто отправив их автору. Таких примеров очень много, например, программная поисковая система Elasticsearch или набор программ Nextcloud, которыми пользуются все ИТ-сообщество.



Павел ИВАНОВ
аспирант Финансового университета
при Правительстве РФ



Михаил ЛЕВАШОВ
профессор Финансового университета
при Правительстве РФ

НОВЫЕ СМЫСЛЫ

ПРОБЛЕМАТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ГИБРИДНОЙ ОБЛАЧНОЙ ИНФРАСТРУКТУРЕ В УСЛОВИЯХ НУЛЕВОГО ДОВЕРИЯ

Облачные технологии в последние годы занимают лидирующие позиции в среде информационных технологий. Доля компаний, владеющих облачными ресурсами, с каждым годом возрастает. Развитие и перевод инфраструктуры в облачные среды происходят практически в двух третях предприятий финансовой, промышленной, образовательной, медицинской отраслей, включая коммерческие и некоммерческие предприятия.

Рынок облачных технологий и сервисов развивается уже достаточно давно. Пандемия коронавируса дала этому развитию мощный толчок, связанный с необходимостью создания условий полноценной удалённой работы для большинства компаний всех уровней. Эта задача наложилась на общие тенденции цифровизации и цифровой трансформации бизнес-процессов и процессов управления, которые в последнее время являются определяющими в отрасли информационных технологий. В этих условиях облачные технологии наполнились новыми смыслами, позволяющими реализовать цифровую трансформацию в условиях удалённой работы, обеспечивая при этом сокращение расходов на реализацию бизнес-процессов за счёт перевода капитальных затрат в операционные, а также за счёт отказа от доработок собственных ИТ-инфраструктур, требующих материальных вложений на этапах внедрения, поддержки и модернизации сервисов.

При этом указанные задачи необходимо решить в условиях обеспечения концепции **нулевого доверия** как к объектам внутренней ИТ-инфраструктуры, включающим пользователей, устройств (узлы) и ПО, так и к облачным приложениям и хранилищам данных.

БЕЗОПАСНОСТЬ ОБЛАЧНОЙ ИНФРАСТРУКТУРЫ

Говоря об инфраструктуре организации, необходимо сделать акцент на сегменте IaaS, который предоставляет потребителям возможность получать вычислительные ресурсы как на публичной основе (публичное облако), так и на частной основе (частное облако).

Поставщик публичного облака является владельцем центров обработки данных (ЦОД) и управляет ими. Вся ответственность за обслуживание оборудования и инфраструктуры, а также обеспечение быстрого доступа к приложениям и данным лежит на нём. За счёт правильного перераспределения вычислительных ресурсов между потребителями обеспечивается масштабируемость, гибкость и высокая доступность сервисов, а также удовлетворение различных требований рабочей нагрузки¹.

Частным облаком является облачная инфраструктура, которая используется одним клиентом. Провайдер может как предоставлять вычислительные ресурсы

в собственных центрах обработки данных, обеспечивая необходимые меры для единоличного использования инфраструктуры, так и разворачивать её в центрах обработки данных клиента с учётом заключённого договора на предоставление услуг. Такой подход позволяет пользоваться всеми преимуществами «облака» и при этом обеспечивать достаточно высокий уровень безопасности, контроль над всеми ресурсами и выполнение нормативных требований, поскольку для таких инфраструктур отсутствуют проблемы с разграничением доступа между множеством клиентов, что характеризует публичные облака, и могут быть приняты комплексные меры по приведению в соответствие требованиям стандартов, реализацию которых не нужно разделять с облачным провайдером.

В части информационной безопасности публичные облака имеют некоторые преимущества, например, выполнение части мероприятий по защите информации в рамках облачной инфраструктуры, что снимает с клиентов задачи по реализации этих функций². Однако использование публичного облака влечёт за собой также и значительные риски в случае, когда клиенту требуется хранить и обрабатывать конфиденциальную информацию, например персональные данные различных категорий.

¹ IBM Cloud Learn Hub // [Электронный ресурс]: IBM Cloud Education. URL: <https://www.ibm.com/cloud/learn/public-cloud> (дата доступа: 20.02.2022).

² What is a public cloud? Public vs. private cloud // [Электронный ресурс]: Cloudflare. URL: <https://www.cloudflare.com/learning/cloud/what-is-a-public-cloud/> (дата доступа: 23.02.2022).

ГИБРИДНАЯ ОБЛАЧНАЯ ИНФРАСТРУКТУРА

Текущий уровень развития информационных технологий и потребности общества обуславливает невозможность использования крупными организациями только одной выбранной модели облачной инфраструктуры, поскольку такой подход повлечёт бы за собой появление стоп-факторов при расширении, модернизации и внедрении новых сервисов.

В таких случаях предлагается применять «гибридное облако». Это архитектурная модель, которая одновременно включает в себя частную и публичную облачную инфраструктуру, объединённую в единую унифицированную платформу. Такое решение обеспечивает максимальную гибкость при развитии компаний и их бизнеса. При грамотной организации и управлении указанной инфраструктурой компании могут успешно совмещать использование частного облака, а также множества сервисов публичного облака. Частная инфраструктура будет обеспечивать функционирование основных информационных систем, а в публичной — могут размещаться вычислительные ресурсы для тестирования новых решений или средств, аналитики больших данных или выполнения иных задач, требующих динамического выделения ресурсов и более высоких затрат при реализации в частной инфраструктуре. Также возможно перераспределение мощностей или перенос данных между облачными ресурсами в зависимости от объёмов вычислений, нагрузки на сеть или же колебаний стоимости ресурсов.

Основной проблемой в использовании гибридной модели облачной инфраструктуры является сложность в унификации компонентов, обеспечивающей эффективность её использования, управление распределёнными информационными системами и сервисами и контроль этих сервисов. Эти задачи должны решаться за счёт совместимости компонент гибридного облака, сопоставимости их функциональных возможностей, возможностей мониторинга и контроля.

Вопросы обеспечения информационной безопасности гибридной облачной инфраструктуры в основном определяются степенью защищённости

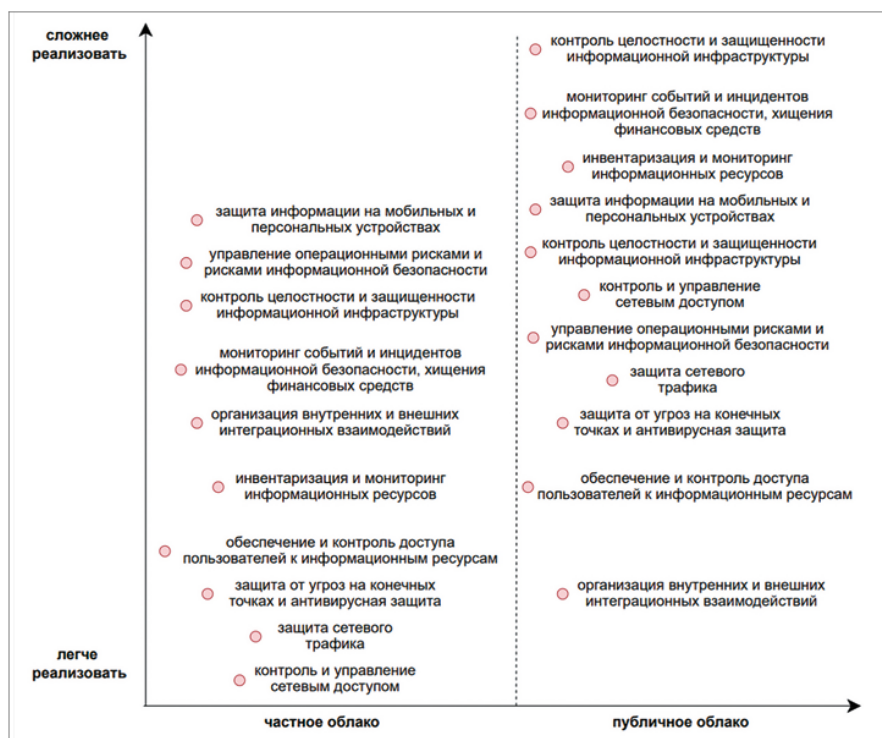


Рисунок 1. Распределение опций безопасности по сложности их реализации

публичного облака с учётом защиты процессов обмена информацией между ним и частным облаком. Степень защищённости частного облака значительно превышает степень защищённости публичного облака. Например, реализация мониторинга информационной безопасности может быть реализована системами частного облака, но не может быть реализована ресурсами, предоставляемыми по моделям PaaS и SaaS, поскольку сервисы информационной безопасности таких ресурсов обеспечиваются облачным провайдером.

Значительные различия существуют в уровнях аутентификации и авторизации пользователей в частном и публичном облаках. Они должны быть сопоставимы и не позволять эксплуатировать уязвимости, связанные с повышением привилегий или несанкционированным доступом. Наиболее сложным аспектом безопасности являются процессы управления уязвимостями, которые в публичных сервисах могут в принципе отсутствовать и тем самым существенно повышать риски использования подобных сервисов, предоставляя потенциальному злоумышленнику пути для нанесения ущерба всей инфраструктуре.

Таким образом, аспектами информационной безопасности, которые требуют тщательной проработки в гибридной облачной инфраструктуре, являются:

- ♦ обеспечение и контроль доступа пользователей к информационным ресурсам;
- ♦ автоматизированное управление и контроль доступа к ресурсам;
- ♦ контроль целостности и защищённости информационной инфраструктуры;
- ♦ инвентаризация и мониторинг информационных ресурсов;
- ♦ построение защищённых каналов связи и защита сетевого трафика;
- ♦ организация внутренних и внешних интеграционных взаимодействий;
- ♦ антивирусная защита и защита от угроз на конечных точках;
- ♦ защита информации на мобильных и персональных устройствах;
- ♦ мониторинг событий и инцидентов информационной безопасности, а также хищения финансовых средств;
- ♦ управление операционными рисками и рисками информационной безопасности.

На рисунке 1 представлено распределение опций безопасности с точки зрения сложности их реализации в

частном и публичном облаках, представленном всеми моделями предоставления (IaaS, PaaS, SaaS).

ПОДХОДЫ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ГИБРИДНОЙ ИНФРАСТРУКТУРЫ

В случае использования публичных облачных ресурсов традиционный подход, подразумевающий построение защищённого периметра, за которым размещается вся информационная инфраструктура, является неэффективным, так как строгий периметр фактически перестаёт существовать. Одним из основных концептов, который используется организациями при использовании публичных платформ и сервисов, является концепция нулевого доверия. Она базируется на постулатах расширенного управления идентификацией и аутентификацией, логической и сетевой сегментации и предлагает сосредоточиться на обеспечении безопасности пользователей, активов и информационных ресурсов, а не на построении строго ограниченного сетевого периметра.

Для гибридной облачной инфраструктуры характерно применение смешанного подхода, который предусматривает как построение традиционного периметра безопасности, так и использование принципов концепции нулевого доверия при организации удалённого доступа, в том числе доступа с портативных и мобильных устройств. Подавляющее большинство систем и средств защиты не позволяет элиминировать угрозы, связанные с применением облачных сервисов, предоставляемых провайдерами. Некоторые из этих сервисов не несут значимых рисков и успешно внедряются в информационные и технологические процессы финансовых организаций, а некоторые требуют принятия рисков информационной безопасности и тщательной проработки компенсирующих мер, в том числе с использованием организационных мер контроля.

Степень доверия к уровню безопасности сервисов PaaS и SaaS до сих пор находится на довольно низком уровне, поскольку вопросы безопасности и их решение остаются на стороне провайдера. Среди проблем с безопасностью публичных сервисов выделяются следующие:

- ♦ процессы управления аутентификацией провайдера не соответствуют принятым политикам либо не поддерживаются существующими в компаниях процессами;

- ♦ инфраструктура облачного провайдера не имеет сертификации на соответствие национальным (отраслевым) стандартам;

- ♦ облачный провайдер не предоставляет сведения о применяемых методах и средствах защиты информации, а также не может гарантировать безопасность обработки и хранения чувствительных данных;

- ♦ подключение к сервисам облачного провайдера не может подвергаться контролю в достаточной степени;

- ♦ инфраструктура и системы хранения данных провайдера физически расположены на территориях иностранных государств либо на вычислительных ресурсах иных облачных провайдеров.

ИНОЙ ПОДХОД К ЗАЩИТЕ ГИБРИДНОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Информационные инфраструктуры, изначально построенные по модели локальной инфраструктуры или частного облака, не предполагают возможности использования публичных облачных сервисов без нарушения установленных требований и стандартов в области информационной безопасности. При этом постоянно развивающиеся облачные сервисы, применение которых несёт организациям и в первую очередь бизнесу преимущества, будут продолжать создавать сложности и проблемы в области ИБ. Это, в свою очередь, требует проведения исследований в части безопасного применения облачных сервисов не в рамках рассмотрения существующих средств защиты, а на уровне инфраструктуры информационной системы.

Предлагается рассмотреть подход, который предполагает использование концептуально иной модели построения гибридной информационной инфраструктуры и, в частности, системы защиты информации. За её основу может быть взята модель безопасности нулевого доверия, на основании которой строятся механизмы защиты, и

брокер безопасности, который выступает посредником всех взаимодействий с облачными сервисами. Он играет роль интеграционного решения, обеспечивающего управление и идентификацию доступа, реализацию и контроль политик безопасности, управление событиями безопасности и ряд процессов реагирования на инциденты³.

В основе гибридной системы защиты лежат принципы нулевого доверия, а именно:

- ♦ обеспечение безопасного и подтверждённого каждого пользователя (устройства) к информационным ресурсам;

- ♦ использование модели минимально необходимых привилегий и контроля доступа;

- ♦ мониторинг действий и активности пользователей за счёт аналитики данных.

Управление и контроль доступа пользователей к информационным ресурсам является одними из наиболее важных процессов в данной модели. Все конечные устройства являются потенциально недоверенными субъектами доступа, права доступа которых не превышают минимально необходимых. Для субъектов, требующих более широких полномочий или административного доступа, подразумевается приведение в соответствие определённым требованиям информационной безопасности. Помимо пользователей, недоверенным считается и доступ со стороны тех частей инфраструктуры, которые расположены вне защищённого периметра.

Внедрение промежуточного слоя, включающего брокера безопасности, между потребителями, публичной облачной инфраструктурой и инфраструктурой организации позволит обеспечить значительно более высокий уровень защищённости, поскольку все взаимодействия с недоверенными и публичными сервисами должны быть реализованы через проксирующий слой, который призван реализовать большую часть тех функций информационной безопасности, которые

³ Information Technology. Gartner Glossary // [Электронный ресурс]: URL: <https://www.gartner.com/en/information-technology/glossary/cloud-access-security-brokers-casbs>.

не могут быть обеспечены на стороне облачного провайдера.

Концептуальный план разрабатываемой в рамках данного исследования архитектуры, представленный на рисунке 2, должен решить задачи управления, контроля и защиты гибридной информационной инфраструктуры.

Данный подход к построению системы защиты подразумевает организацию трёх основных уровней (периметров) защиты:

- 1) уровень сетевого периметра частной инфраструктуры (частное облако или локальная инфраструктура);
- 2) уровень системы защиты гибридной инфраструктуры;
- 3) уровень конечных устройств (клиентов доступа).

Первый уровень защиты подразумевает защищённую по традиционной модели инфраструктуру организации, которая требует доработок в части подключения ко второму уровню защиты, основному элементу архитектурной концепции — уровню системы защиты гибридной инфраструктуры.

Второй уровень представляет собой комплекс средств защиты, развёрнутый на выделенной информационной инфраструктуре и физическом оборудовании и расположенный вне частной инфраструктуры организации. Фактически данный уровень защиты представляет собой комплексную защищённую интеграционную платформу, которая реализует на своей основе принципы нулевого доверия и различные функции, связанные с защищённым доступом пользователей к информационным ресурсам гибридной информационной инфраструктуры, а также интеграцией с различными внешними ресурсами и внутри инфраструктуры.

Третий уровень защиты представляет собой пользовательские устройства с разной степенью защищённости. К ним относятся защищённые АРМ, на которых установлен комплекс средств защиты, позволяющий пользователям при работе на этих устройствах заниматься задачами администрирования или работать с конфиденциальными данными, базовые АРМ, на которых установлен минимально достаточный комплекс средств защиты, а также основная часть — потенциально незащищённые устройства.

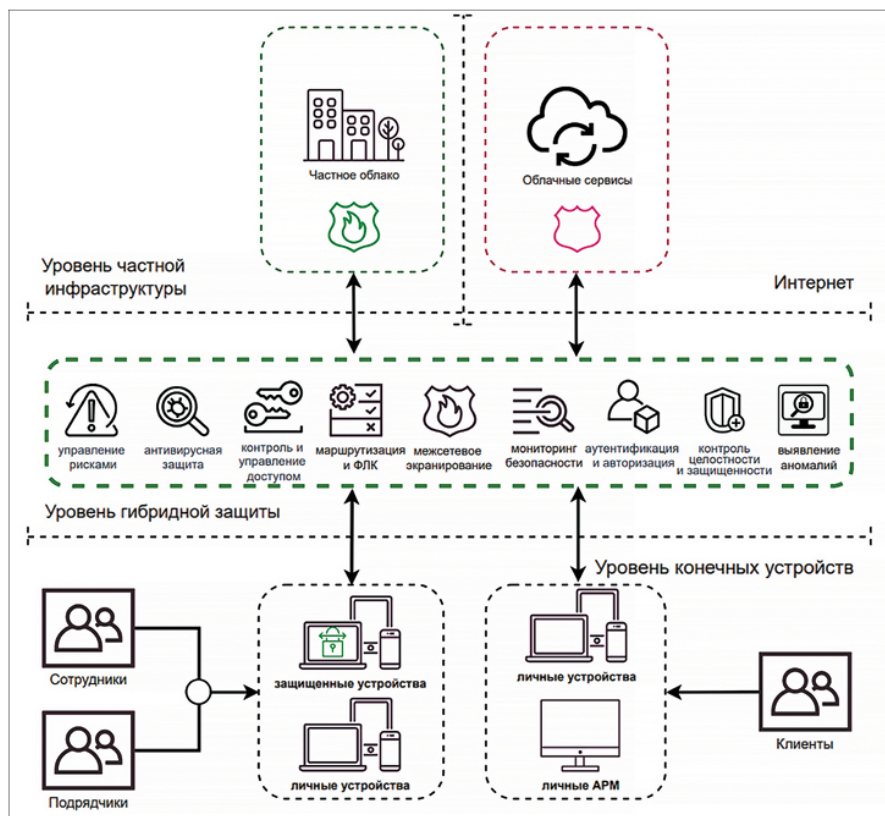


Рисунок 2. Архитектурная концепция обеспечения безопасности гибридной облачной инфраструктуры

Основной акцент при построении второго уровня защиты должен быть сделан на следующих аспектах безопасности:

- 1) реализация процессов предоставления безопасного доступа к информационным ресурсам с различной степенью конфиденциальности;
- 2) обеспечение единообразного процесса создания интеграционных взаимодействий, а также контроля и управления взаимодействиями;
- 3) выявление различных угроз безопасности в инспектируемом трафике, а также мониторинг аномального поведения пользователей.

Предложенная архитектура системы защиты информации должна решить задачи реализации гибридной облачной инфраструктуры в части обеспечения достаточного уровня защищённости при использовании публичных облачных сервисов, а также предоставить возможности управления и контроля уровня информационной безопасности инфраструктуры в целом. Она базируется на следующих фундаментальных положениях:

- ♦ использование облачных сервисов с сохранением высокого уровня защищённости;
- ♦ целостность и унификация политик для всех облачных сервисов;
- ♦ расширение и усиление инфраструктуры безопасности;
- ♦ широкие возможности предоставления безопасного доступа для пользователей;
- ♦ обеспечение возможности работы с личными устройствами пользователей.

Основная задача при создании данной гибридной системы защиты — адаптация классических информационных инфраструктур к условиям гетерогенности внутренних и внешних взаимодействий, применения облачных сервисов, предоставляемых в рамках различных моделей, а также специфического пользовательского доступа. Дальнейшие исследования в данной области будут направлены в сторону реализации основных аспектов безопасности с учётом специфики работы с облаком, а также обеспечения работы всей системы в целом.

ВАШЕ БЛАГОРОДИЕ, ГОСПОЖА УТЕЧКА

ПРИЧИНЫ, ПОСЛЕДСТВИЯ, ЧТО ДЕЛАТЬ?



**Андрей
ЖАРКЕВИЧ**
редактор
ООО «Антифишинг»

Утечки данных — чрезвычайно опасное явление. Ущерб от них по самым скромным оценкам может составлять десятки миллиардов рублей. Попытки побороть это явление с помощью технических средств в большинстве случаев оказываются неэффективными, поскольку главная причина утечек — человеческий фактор. В этой статье подробно разберём, чем опасны утечки, рассмотрим их основные причины, а также поговорим о возможных решениях проблемы и их ожидаемой эффективности.

ПОДРОБНЕЕ О ПРОБЛЕМЕ

Многие компании относятся к утечкам данных достаточно спокойно, считая их неизбежным злом или своего рода стихийным бедствием. Ущерб репутации — категория довольно расплывчатая, а штрафы не такие уж страшные, как показывает история с Яндекс.Едой, заплатившей за многомиллионную утечку 60 тыс. рублей.

В мае-июне 2022 года в даркнете было опубликовано рекордное количество баз данных российских компаний — более 50. В апреле их было 32, а в марте всего 16. Среди жертв, чьи базы попали в открытый доступ, оказались компании, относящиеся к интернет-сервисам доставки, медицине, телекому, интернет-ритейлу, онлайн-образованию, строительству и так далее.

Последствия этих утечек с большой вероятностью будут ощущаться в течение ближайших месяцев, а, возможно, и лет, как получилось с нашумевшей утечкой сведений о клиентах Сбербанка в октябре 2019 года (рис. 1).

Из материалов уголовного дела следует, что «выгрузка представляла собой архив с текстовыми документами, в которых хранятся записи о счетах и картах, об операциях по картам, остаток по счетам клиентов Банка, сгруппированные по территориальным банкам. Записи содержат также персональные данные клиентов, в том числе: фамилию, имя, отчество, паспортные данные, дату рождения, адрес места жительства, номер мобильного телефона, полный номер кредитной карты, место работы, остаток собственных средств». Всего каждая запись содержала 81 колонку, а в базе содержалось не менее 10,2 млн строк.

Информацией из этой утечки воспользовались телефонные мошенники, представлявшие себя «службой безопасности Сбербанка». По оценкам самого Сбера, ежемесячный ущерб граждан от телефонного мошенничества по всей стране в 2020 году составлял 3,5–5 млрд рублей.

Последствия утечки Сбера продолжали сказываться и в 2021 году. По оценкам МВД РФ ущерб от дистанционного телефонного мошенничества в России за 11 месяцев 2021 года составил 45 млрд рублей.

ДРУГИЕ ПОСЛЕДСТВИЯ УТЕЧЕК

Использование похищенных сведений мошенниками — далеко не единственная проблема. Перечислим некоторые возможные варианты.

Шантаж и вымогательство

Операторы вымогательского ПО (ransomware) применяют тактику двойного вымогательства: они не только шифруют информацию в сети или на устройствах жертвы, но и похищают важные сведения, после чего угрожают их обнародованием. Для этого создаются специальные сайты утечек, на которых преступники размещают фрагменты «слитой» информации, по которым жертва может убедиться в реальности угроз.

Черный пиар и SWAT

Наличие персональных данных открывает массу возможностей сделать человеку плохо. Представим, например, что мошенники позвонили Ивану от имени банка и попытались выманить у него деньги. Иван оказался бдительным, разыграл звонивших и посмеялся над ними. Мошенники обиделись и «сватнули»¹ Ивана: организовали ложное сообщение о минировании торгового центра и от имени Ивана потребовали выкуп.

К Ивану приехала полиция, и он вынужден был объяснять, что понятия не имеет, о чём идёт речь, отдавать на экспертизу компьютерную технику и терпеть другие неудобства.

Другой вариант, о котором уже написали в СМИ, — использование номеров реальных

¹ Слово «сват» — калька с английского SWAT — Special Weapons And Tactics, означающего различные подразделения специального назначения. «Сватнуть» — организовать ложный вызов полиции.

ФИО	Паспорт	Номер карты	ОСБ	Филиал	Лимит кредита	Недоисп. лимит	Ссуда всего	Ссуда текущая	Ссуда к погашению	Превышение лимита	Просроченная
ИРОВИЧ	65 04	4279011	7003 0637		140000.00	474.39	142444.34	133944.59	5581.02	0.00	0.00
ГЕЕВИЧ	09 14	4279011	8599 0227		64000.00	64000.00	0.00	0.00	0.00	0.00	0.00
ЛЕКСАНДРОВ	75 18	4279011	8597 0397		42000.00	1727.44	41108.34	38661.66	1610.90	0.00	0.00
ЗАЛЕРЬЕВИЧ	80 05	4279011	8598 0169		84000.00	84000.00	0.00	0.00	0.00	0.00	0.00
АНДРОВИЧ	75 00	4279011	8597 0502		75000.00	49000.00	26000.00	24960.00	1040.00	0.00	0.00
НЬЕВНА	65 15	4279011	7003 0681		125000.00	4481.74	120596.53	120518.26	0.00	0.00	0.00
НДРОВНА	75 05	4279011	8597 0540		200000.00	139021.94	61054.80	60978.06	0.00	0.00	0.00
ЕОНИДОВИЧ	65 07	4279011	7003 0799		100000.00	61504.44	39167.00	36955.73	1539.83	0.00	0.00
ОРЬЕВНА	80 05	4279011	8598 0158		150000.00	150000.00	0.00	0.00	0.00	0.00	0.00
АСОВНА	80 11	4279011	8598 0781		180000.00	180000.00	0.00	0.00	0.00	0.00	0.00
ТОРОВНА	67 14	4279016	5940 0057		125000.00	125000.00	0.00	0.00	0.00	0.00	0.00
ЕВНА	67 12	5484016	1791 0052		50000.00	29439.27	20560.73	20055.09	505.64	0.00	0.00
ИМИРОВИЧ	67 10	4279016	1791 0110		77000.00	87.22	78536.47	68047.50	2835.31	0.00	6029.97

Рисунок 1. Фрагмент похищенной базы клиентов Сбербанка. Источник: t.me/dataleak

людей для подстановки при мошеннических звонках. Обманутые люди пишут заявления в полицию, указывая номер, с которого получили звонок. В результате совершенно непричастным людям приходится давать объяснения, а ещё их номера могут попасть в один из чёрных списков, которые ведут многие сервисы, например Яндекс, Сбер, Тинькофф. Такой абонент при звонке будет определяться «нежелательным» или вообще блокироваться приложением.

Нелегальные схемы

Один из самых популярных способов нелегального применения персональных данных — создание дропов — подставных лиц. На дропа могут оформить банковские карты, чтобы выводить или обналичивать через них не вполне легальные средства или покупать товар, зарегистрировать ООО или ИП для проведения различных незаконных операций. Данные дропов часто используют для анонимизации людей, предпочитающих не показывать свою реальную личность в сети.

Некоторые люди добровольно становятся дропами из-за различных жизненных трудностей. Но есть и те, чьи «услуги» мошенники получают путем социальной инженерии.

Пример. На Авито размещается вакансия очень простой работы на дому. Требуется принимать товары от интернет-магазина и пересылать их по указанному адресу. Для «трудоустройства» у кандидата просят сканы паспорта и других документов якобы для проверки в службе безопасности. В результате мошенники получают все необходимые данные для оформления дропа.

Информация из утечек позволяет создавать дропов значительно проще, что превращает подобные данные в настоящий клад для дроповодов.

ПРИЧИНЫ УТЕЧЕК

Принято считать, что часть утечек происходит по техническим причинам, но чаще всего настоящими виновниками инцидентов являются люди. Например, для доступа к базе данных

лаборатории «Гемотест», содержащей сведения о 554 млн заказов, которая появилась в продаже на теневом форуме в начале мая 2022 года, использовалась уязвимость сервера баз данных.

Это выглядит вполне технической причиной, но в действительности произошедшее стало возможным по недосмотру администратора БД, который не установил исправления для уязвимости или не закрыл внешний доступ к базе для посторонних. А это уже человеческий фактор — некорректные действия или бездействие сотрудника.

Опрошенные «Известиями» эксперты по кибербезопасности считают, что «свыше 90% утечек — не результат мастерства хакеров, а вина сотрудников».

Рассмотрим, что может привести к тому, что люди сознательно или по незнанию допускают утечку информации.

Желание заработать

Самый распространённый мотив всех киберпреступлений — финансовый. Информацию называют новым золотом, поэтому продажа на сторону конфиденциальных данных компании многим кажется простым способом улучшить благосостояние. Особенно греет душу начинающих «хакеров» тот факт, что после копирования данные остаются на месте. Это позволяет сохранить душевный комфорт и создаёт ложное чувство безнаказанности.

Именно перспектива нелегального заработка заставила сотрудника Сбербанка Зеленина С. А. придумать способ обойти корпоративную систему защиты от утечек (DLP, Digital Leak Prevention). Он помещал слитые данные в электронные письма, но не отправлял их. Черновики писем с почтового сервера синхронизировались с почтовым клиентом на служебном ноутбуке, после чего можно было сохранить вложения и скопировать их на внешний носитель.

Шантаж

Строго говоря, в большинстве случаев цель шантажа также финансовая. Операторы вымогательского ПО угрожают опубликовать похищенные данные, требуя выкуп. Системный

Сейчас при утечке персональных данных административная ответственность направлена на изначально добропорядочных игроков — операторов, у которых эти данные украли, а истинные виновники утечек остаются в стороне

администратор грозит руководству опубликовать компрометирующую информацию, чтобы получить компенсацию за сверхурочную работу.

Проблема с шантажом состоит в том, что уплата выкупа или компенсации совсем не гарантирует, что информация не будет опубликована.

Но бывают ситуации, когда объектом шантажа становится сотрудник, имеющий доступ к требуемой заинтересованным лицам информации. Когда речь идет о жизни и здоровье близких, корпоративная этика и даже перспектива нарушить закон отходят на второй план.

Обида на работодателя

Обиженные сотрудники способны создать компании много проблем, особенно если имеют доступ к чувствительным данным. Предполагают, что именно обида на работодателя заставила сотрудника Яндекс.Еды опубликовать в открытом доступе сведения о 49 млн заказов сервиса.

Политические взгляды

Политически мотивированные инциденты получили широкое распространение после начала СВО на Украине. Организация утечек и публикация данных для некоторых сотрудников стали способом проявить свою гражданскую позицию. При этом они не осознавали, что своими действиями наносят вред не столько государству или компании, сколько обычным людям, данные которых были выставлены на всеобщее обозрение.

Недостаток профессиональных знаний

К этой категории можно отнести утечки, связанные со случайно оставленными в публичном доступе базами данных. Например, 3 апреля 2022 года на площадке Amazon была обнаружена свободно доступная база Elasticsearch, содержащая SMS от различных сервисов и банков. Объем базы составлял около 4,5 Тб. Среди операторов были Google, Тинькофф, Аэрофлот, Юла, Microsoft. Номера телефонов получателей скрыты звездочками, но содержимое сообщений, включая одноразовые коды для двухфакторной аутентификации и восстановления паролей, хранится в неизменном виде.

Совершенно очевидно, что причиной инцидента стал недостаток знаний администратора баз данных компании-владельца базы. Он не воспользовался средствами ограничения доступа сервиса Amazon и даже не включил аутентификацию в самой базе данных.

КАК ЗАЩИТИТЬСЯ?

Проблемы с утечками заставили законодателей задуматься об ужесточении ответственности за подобные инциденты. Как заявил глава Роскомнадзора Андрей Липов, «по нашему мнению, только так можно остановить вал преступлений, связанных с утечками и незаконной продажей чувствительной для россиян информации».

Замглавы Роскомнадзора Милош Вагнер сообщил, что ведомство считает целесообразным ввести уголовную ответственность за торговлю утекшими персональными данными. Он подчеркнул, что «основная трагедия этих утечек в том, что, как только данные появились в общем доступе и стали доступны неограниченному кругу лиц, предотвратить их распространение без жестких мер практически невозможно. Сейчас при утечке персональных данных административная ответственность направлена на изначально добропорядочных игроков — операторов, у которых эти данные украли, а истинные виновники утечек остаются в стороне».

Страх серьезного наказания остановит многих желающих заработать на торговле чувствительной информацией, но не поможет исключить случайные утечки из-за неправильной конфигурации сервисов, политически мотивированные утечки и утечки по вине обиженных или запуганных сотрудников.

Тотальная установка технических средств защиты в виде современных систем DLP также решит проблему лишь частично, поскольку ни одно подобное решение не остановит системного администратора, который имеет все полномочия по управлению.

В качестве дополнительных мер для решения проблемы утечек компаниям следует рассмотреть выявление потенциальных инсайдеров, формирование групп риска по различным критериям, повышение уровня грамотности и развитие навыков в сфере информационной безопасности.

Понимание последствий своих действий как с технической, так и с законодательной точки зрения остановит большую часть финансово мотивированных сотрудников и тех, кто до недавнего времени получал доход от перепродажи чувствительной информации.



Артём ЗУБКОВ
директор ФСРБИТ

СВЯЗЬ ПОКОЛЕНИЙ КАК ФУНДАМЕНТ БУДУЩЕГО

НАГРАЖДЕНИЕ ПОБЕДИТЕЛЕЙ ИНТЕЛЛЕКТУАЛЬНЫХ СОРЕВНОВАНИЙ ШКОЛЬНИКОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 2021/22 УЧЕБНОГО ГОДА ПРОШЛО В НОВОМ МУЗЕЕ КРИПТОГРАФИИ

Прошедший учебный год вместил в себя сразу несколько интеллектуальных соревнований, имеющих непосредственное отношение к криптографии. Это XXXI Межрегиональная олимпиада школьников им. И. Я. Верченко, конкурсы проектно-исследовательских работ школьников «Шифры Победы» и «Математика шифров Победы», а также интернет-викторины «Криптографический фронт Великой Отечественной». Эти мероприятия стартовали ещё осенью, а в преддверии Дня Победы и профессионального празд-

ника криптографической службы России были подведены итоги и настало время награждения победителей, призёров и активных участников. Традиционно для этого торжественного события выбирается одна из знаковых площадок. В прошлом году это был Центральный музей ВС РФ, а в этом — только что открывшийся в Москве Музей криптографии.

21 апреля в его здании встретились представители и разных поколений — от школьников до академиков, и разных направлений деятельности в области ИБ — науки, образования,

промышленности. Всего было более 100 гостей. В том числе в церемонии награждения приняли участие представители компаний «Системы и технологии», «ИнфоТеКС», «Код Безопасности», «Линфо». Организатором награждения выступил Фонд содействия развитию безопасных информационных технологий.

Программа праздника была весьма насыщенной. Для школьников она началась с небольшой лекции о практике шифрования данных в подразделениях Красной Армии. Затем 12 команд соревновались в решении



**ФОНД
ПРЕЗИДЕНТСКИХ
ГРАНТОВ**

Публикация подготовлена при поддержке гранта Президента Российской Федерации на развитие гражданского общества №21-1-009977, предоставленного Фондом президентских грантов



заданий квеста «Математика шифров Победы», примерив на себя роли сотрудников подразделений шифровальной связи. Задания строились на реальных документах времён Великой Отечественной войны, хранящихся в архивах Минобороны России. Среди них — переговорная таблица, гидрометеорологический код КН-1 и шифр «Горизонт», шифр «АМ» для передачи сводок на артиллерийские батареи.

Многие участники уже имели некоторое представление о способах шифрования, применявшихся во время Второй мировой войны и в более ранние

периоды. Оно могло сформироваться и при подготовке к олимпиаде по криптографии, и при изучении военных архивов в ходе конкурсов «Шифры Победы» и «Математика шифров Победы».

По окончании квеста школьники и учителя смогли осмотреть часть экспозиции музея. Разумеется, наибольший интерес представляли экспонаты XX века. Технологии организации связи, ручные шифры, первые шифровальные машины были близки к уже имеющемуся бэкграунду школьников. Не меньший интерес вызвала экспозиция и у взрослой аудитории, существенную

часть которой составляли специалисты в области криптографии.

Грамоты и памятные подарки победителям всех перечисленных соревнований вручал вице-президент и действительный член Академии криптографии РФ, заслуженный деятель науки Сачков Владимир Николаевич. Он многие годы возглавляет оргкомитет олимпиады им. И. Я. Верченко. И тут невозможно не отметить два интереснейших факта. Во-первых, Владимир Николаевич — один из соавторов знаменитой шифрмашины «Фиалка», являющейся одним из центральных экспонатов музея. Во-вторых, Иван Яковлевич Верченко несколько лет работал над созданием аппаратуры шифрования телефонной связи как раз в здании, где расположен музей.

Призёры Межрегиональной олимпиады школьников имени И. Я. Верченко по математике и криптографии могут поступить в вуз без вступительных испытаний или получить максимальное количество баллов за экзамен по предмету, соответствующему профилю Олимпиады. Организаторы Олимпиады — Академия криптографии РФ, Академия ФСБ России.

В этом году призёрами олимпиады стали 47 человек.

МУЗЕЙ КРИПТОГРАФИИ — ОДИН ИЗ ПРОЕКТОВ НПК «КРИПТОНИТ»

Создатели музея задались целью показать, как глубоко криптография интегрирована в современную жизнь и как она способна изменять общество и влиять на ход истории.

В музее собрана историческая коллекция шифровальной техники, других средств шифрования и передачи секретной информации, архивные документы. Помимо статичных экспонатов и мультимедийного контента, в экспозицию Музея криптографии включены также интерактивные и кинетические инсталляции, обучающие игровые экспонаты.

Уместно заметить, что если о роли криптографии в современной жизни обычные люди хотя бы слышали, то лишь немногие осведомлены о роли криптографии в важных исторических событиях и геополитике XX века.

Зданию музея почти 140 лет. С 1946 по 1954 год в нём находилась «Марфинская лаборатория», где создавали технику секретной телефонной связи. Среди её ведущих сотрудников был и И. Я. Верченко, именем которого названа олимпиада школьников. В 1955 году лабораторию преоб-

разовали в Научно-исследовательский институт автоматики, который в новом статусе продолжил разработку разнообразной аппаратуры шифрования. Именно в этом НИИ был создан «ядерный чемоданчик» — автоматизированная система управления ядерным арсеналом СССР.

К концу 1950-х институт расширил свою территорию, были построены новые корпуса. В старом здании остались бюро технической эстетики, профком, химическая лаборатория, помещение ЭВМ и некоторые другие отделы.

В 2019 году здание было передано Музею криптографии. Открытие музея состоялось в декабре 2021 года.



Ксения ТРОХИМЕЦ
заместитель
директора
департамента
специальных
проектов hh.ru

ПРОБЛЕМА ДЕФИЦИТА ИБ-СПЕЦИАЛИСТОВ ОБОСТРЕТСЯ

АНАЛИТИКИ HH.RU СПЕЦИАЛЬНО ДЛЯ
BIS JOURNAL ПРОАНАЛИЗИРОВАЛИ
СЕКТОР ИБ НА РЫНКЕ ТРУДА

За период с января по май 2022 г. на hh.ru компании-работодатели опубликовали 12 041 вакансию для ИБ-специалистов, что на 12% ниже показателя аналогичного периода прошлого года.

Отрицательная динамика вызвана серьёзной «просадкой» в количестве вакансий в апреле 2022-го: их было на 1 тыс. меньше, чем в апреле 2021-го (1900 против 2900). Несмотря на отрицательные темпы прироста спроса на ИБ-специалистов, дефицит кадров в этом секторе усугубляется: на одну открытую ИБ-вакансию приходится менее одного резюме (0,4 в течение 2021 и 0,7 в течение 2022). Для сравнения, в ИТ-сфере в течение 2021 года конкуренция составляла 1,8, в 2022 — выросла до 2,3. По подсчётам аналитиков hh.ru, для достижения минимально приемлемой и комфортной ситуации с наймом в данном сегменте (т.е. на одну открытую вакансию приходилось бы четыре резюме, тогда у работодателя есть адекватный выбор среди кандидатов по уровню

требуемых навыков и опыту) рынку труда требовалось дополнительно порядка 120 тыс. ИБ-специалистов в 2021 году и свыше 30 тыс. в первые месяцы 2022 года. Сегодня же разрыв спроса и предложения остаётся кратным, и речь по-прежнему идёт о недостатке нескольких тысяч специалистов ежемесячно.

Ситуация вынуждает работодателей снижать требования к будущим сотрудникам в ИБ-подразделениях. Если в 2021 году свыше половины (51%) вакансий были открыты строго для специалистов с опытом от 1 до 3 лет, то в 2022 их стало 48%. Доли вакансий для опытных специалистов (свыше 6 лет) и молодёжи без опыта остаются прежними — 3 и 13% соответственно, что отражает готовность компаний обучать сотрудников.

Вместе с этим за год компании стали более чётко описывать требования к необходимым навыкам. Доля упоминаний навыков и знаний основ ИБ в вакансиях выросла с 18 до 31%, владение техническими средствами информационной защиты — с 5 до 8%,

средства криптографической защиты информации теперь встречаются в 7% ИБ-вакансий.

Медиана предлагаемой зарплаты ИБ-специалистов выросла на 6%, до 63 100 руб. против 59 500 руб. в 2021 году. Ожидания по зарплате, напротив, снизились на 4%, хотя остаются существенно выше рыночного уровня — с 78 300 руб. до 75 100 руб.

Географически рынок труда в ИБ агрегируют Москва и Петербург — на них приходится 52% всего объёма вакансий, причём столица нарастила свою долю за год почти на 3 п.п. Далее с большим отрывом идут компании из Новосибирской и Московской областей (по 3%). В остальных регионах равномерное распределение ИБ-вакансий.

В разрезе бизнеса чётко выделяются три отрасли по уровню спроса на ИБ-специалистов — это непосредственно ИТ-компании (доля в 2022—29%, +2 п.п.), финансовый сектор (12%, +1 п.п.) и телеком (8%, —3 п.п.). Госсектор нарастил долю в ИБ-вакансиях до 2% в начале 2022 года.

О HEADHUNTER

HeadHunter (hh.ru) — крупнейшая платформа онлайн-рекрутинга в России, клиентами которой являются свыше 515 тыс. компаний. Цель HeadHunter — помогать компаниям находить сотрудников, а людям — работу и делать так, чтобы процесс поиска сотрудников и работы был быстрым и доставлял обеим сторонам только положительные впечатления. Обширная база компании содержит свыше 55 млн резюме, а среднее дневное количество вакансий в течение 2021 г. составило свыше 933 тысячи ежемесячно. По данным SimilarWeb, hh.ru занимает третье место в мире по популярности среди порталов по поиску работы и сотрудников. HeadHunter — аккредитованная Министерством цифрового развития ИТ-компания, включена в Реестр аккредитованных ИТ-компаний России.

ДЛЯ ЧЁРНОГО КОЛЛЕДЖА НАСТУПИЛИ ЧЁРНЫЕ ДНИ

ПРОБЛЕМЫ УЧЕБНЫХ ЗАВЕДЕНИЙ, СВЯЗАННЫЕ С ИБ

С OVID-19 подвиг учебные заведения Великобритании к тотальной переоценке своих систем и созданию центров кибербезопасности для защиты территорий и пользователей

СНАЧАЛА ОЦЕНИ СВОЮ ИБ

«За последние два года высшие учебные заведения Великобритании стали объектами многочисленных кибератак. Серьёзной угрозе подверглись стандарты обучения и защиты научных данных. Громкие атаки на британские университеты привели в состояние повышенной готовности всю сферу образования», — отмечает Кирк Беллерби, руководитель отдела высшего образования Великобритании в издании Education Technology.

Киберпреступники оценили большой объём онлайн-коммуникаций, которые проходят между студентами, преподавателями, сотрудниками университетов и другими обитателями университетских кампусов. Используя фишинговые атаки, они получают конфиденциальную информацию, включая пароли и доступы в локальные сети, взламывают глобальные университетские сети и крадут данные. А также с помощью программ-вымогателей блокируют доступ к сети и, угрожая опубликовать личные данные жертвы или организации, требуют выкупа.

Чтобы помочь гражданам и организациям защититься, правительство Великобритании предоставило организациям всех форм собственности систему оценки кибербезопасности — схему, которая поможет любому учреждению улучшить свою ИБ. Цель программы — сертифицировать организации, вложившие средства в киберзащиту, и предоставить им оптимальную методику, чтобы они могли эффективно использовать свои инвестиции в кибербезопасность.

ЗАЩИТА ОКОНЕЧНЫХ УСТРОЙСТВ

Быстрый переход к удалённому и гибриднему обучению принёс с собой новые угрозы. В кампусах и домах появилось множество оконечных устройств (компьютеров и смартфонов), подключённых к университетской сети, тысячи студентов выходили в глобальную сеть с помощью персональных устройств и домашних сетей Wi-Fi. Такая децентрализованная ИТ-инфраструктура содержит многочисленные уязвимости и открывает безграничные возможности для злоумышленников.

Децентрализованная ИТ-инфраструктура не позволяет университетам собрать информацию об устройствах, подключённых к их сети. Это приводит к сложностям с обновлением ПО и выявлением уязвимых устройств. В случае кибератаки часто невозможно быстро отреагировать на инцидент и предотвратить ущерб. Но этого легко избежать, внедрив комплексную защиту оконечных устройств.

При развёртывании такой защиты можно автоматически собирать данные со всех конечных точек сети, что позволит ноутбукам создавать политики решений, а также проводить обновления и исправления ПО по мере необходимости. Один из британских университетов внедрил подобную систему и сократил почти до нуля число устройств с не обновлённым ПО.

КАДРЫ

Технологические проблемы — не единственные. Вузы борются за сохранение квалифицированных специалистов, но им не хватает ресурсов. В частных компаниях ИТ-специалистам предлагают лучшие финансовые условия и льготы, поэтому они часто уходят из университетов. Оставшиеся в университетах сотрудники не имеют достаточных ресурсов, перегружены работой

и мало квалифицированы. Им трудно управлять сложными системами.

ПРАВИТЕЛЬСТВЕННАЯ СХЕМА

Из-за сложной архитектуры типичной университетской сети необходимо, чтобы ИТ-департаменты начали использовать стратегии, заложенные в правительственной схеме кибербезопасности. Им необходимо использовать инструменты, которые могут в режиме реального времени сканировать ИТ-ресурсы и проводить инвентаризацию всех активов.

Также стратегия безопасности университета должна строиться на защите двух наиболее важных областей: обучение студентов и научные данные. Чтобы придерживаться правительственного списка требований к кибербезопасности, необходимо внедрить надёжные стратегии управления всеми устройствами в сети. Это обеспечит базу для предотвращения кибератак.

В МАНЧЕСТЕРЕ

Университеты Ланкастера и Манчестера, компании Barclays Eagle Labs, Plexal и консорциум специалистов по кибербезопасности вошли в новый проект, получивший название DiSH (digital innovation security hub) — Центр безопасности цифровых инноваций.

Хаб откроется при штаб-квартире правительственной связи Heron House в Манчестере. Его цель — стимулирование инноваций в ИТ- и ИБ-секторах. Проект создаст больше тысячи рабочих мест и поддержит 500 стартапов. Открытие запланировано на лето 2022 г.

DiSH повысит статус университетов Ланкастера и Манчестера, позволит им эффективно взаимодействовать со специалистами в области ИБ по всему коридору от штаб-квартиры GCHQ в Манчестере до Самлсбери, где расположены Национальные силы

кибербезопасности, и двигаться дальше на север и северо-запад. Университеты планируют создавать региональную исследовательскую систему в сфере кибербезопасности и инновационную экосистему.

DiSH будет включать коворкинг на площади 11 тыс. кв. футов, предложит доступ к сетям, программам развития бизнеса и наставничеству от отраслевых экспертов.

Центр будет содействовать развитию социальной мобильности за счёт инноваций. Предприятия и предприниматели могут заявить о своей заинтересованности в получении навыков кибербезопасности, им предложат профессиональное обучение и наставничество. Для включения в программу надо будет заполнить анкету.

По мнению Грэма Бастина, директора Северо-западного отделения Barclays, навыки в области кибербезопасности становятся всё более важными для функционирования бизнеса, правительства и общества в целом. Благодаря совместной инициативе DiSH, Barclays вместе с партнёрами надеется найти и поддержать талантливых предпринимателей, а также привнести кибернавыки на северо-запад Англии.

В УЭЛЬСЕ

Университет Кардиффа получит £9,5 млн на создание Центра киберинноваций (CIN). Финансирование выделяют правительство Уэльса и заинтересованные организации в рамках Соглашения о столичном регионе Кардифф.

Ожидается, что инвестирование первых £6 млн в CIN будет стимулировать трансформацию и рост кластера кибербезопасности в Южном Уэльсе. Предполагается активное партнёрство с компаниями Airbus, Alacrity Cyber, CGI, Thales NDEC, Tramshed Tech, а также с Университетом Южного Уэльса.

Также CIN рассчитывает привлечь в течение пяти лет ещё £15 млн обучить более тысячи специалистов в области кибербезопасности и создать региональный центр по созданию ИТ- и ИБ-продуктов, обучению и повышению квалификации специалистов.

Концепция Центра разработана под руководством профессора Пита



Университет Кардиффа в Уэльсе

Бернапа, специалиста в области науки о данных и кибербезопасности Школы компьютерных наук и информатики. Профессор Бернап имеет большой опыт исследований в области кибербезопасности мирового уровня и их воплощения в коммерческие продукты.

Правительство Уэльса гордится тем, что софинансирует миссию Центра и содействует превращению столичного региона Кардиффа в один из ведущих киберкластеров Великобритании к 2030 г.

Университеты Кардиффа и Южного Уэльса официально признаны национальными центрами кибербезопасности и академическими центрами передового опыта в области исследований и образования. Их исследовательская работа способствовала появлению новых малых и средних предприятий. Из них уже выросли и крупные компании. Это создаёт устойчивую цепочку поставок в Уэльсе, уже оценённую деловыми и государственными партнёрами. Поэтому Уэльс стал отличной национальной экосистемой кибербезопасности. А созданный Центр киберинноваций дополнил экосистему кибербезопасности Южного Уэльса, войдя в систему кибербезопасности Великобритании в целом.

ЛОНДОН. ВАКАНСИЯ

Показательное объявление. «Департамент военных исследований Лондонского Королевского колледжа приглашает на работу преподавателя по кибербезопасности, готового поддерживать и развивать направление ИБ, а также проводить высококачественные исследования.

Прошедший конкурс кандидат должен запустить постдипломные программы обучения на уровне модуля 6 по кибербезопасности, а также разработать и внедрить модули уровня 7 по киберсиле и стратегии, а также кибердипломатии. Ожидается, что учащиеся по этим направлениям будут проводить исследования в области ИБ и работать со школьниками.

Наша вакансия — отличная возможность для кандидата помочь сформировать повестку дня в области кибербезопасности в департаменте мирового класса, находящемся в центре международных академических и политических сетей.

Должность предусматривает срочный контракт на полный рабочий день сроком на 12 месяцев.

Ключевые обязанности: планирование, организация и проведение учебной деятельности как для студентов,

так и для аспирантов в рамках департамента; разработка и использование различных методов оценки обучения учащихся и предоставление обратной связи; проведение высококачественных исследований в предметной области; публикация результатов в высокорейтинговых журналах, имеющих мировое признание, и участие в основных международно признанных академических сетях.

Сотрудник должен работать с аспирантами-исследователями и/или научным персоналом, посещать профессиональные встречи и конференции, чтобы делиться опытом, представлять результаты исследований. Повышать национальный и международный авторитет департамента. Вести административную работу в рамках департамента и выполнять иные обязанности в разумных рамках.

Кандидат на должность должен иметь учёную степень доктора наук по указанному направлению, иметь опыт преподавательской работы с использованием инновационных программ и технологий, вести программу исследований и иметь достижения в распространении исследований. Приветствуется широкий круг общения в неакадемической профессиональной сфере, коммуникативные навыки, как устные, так и письменные, а также умение работать самостоятельно и в составе команды.

Также желательны: успешный опыт получения грантов, руководства аспирантами, заполненная анкета и характеристики с предыдущих мест работы.

Место работы — Лондон, центр. Доход — £38,826 — £45,649 в год, включая лондонскую надбавку. Заявки на конкурс принимаются до 26 июля 2022 г.»

США. ЧЁРНЫЙ КОЛЛЕДЖ

В мае 2022 года прекратил своё существование Колледж Линкольна в Иллинойсе. Учебное заведение настигли финансовые проблемы, вызванные пандемией COVID-19, однако основной причиной стали атаки программ-вымогателей в декабре 2021 г.

Чёрный колледж, или Колледж гуманитарных наук штата Иллинойс просуществовал в сельской глубинке 157 лет, пережил многочисленные рецессии,

крупный пожар в 1912 г., пандемию «испанки» 1918 г., Великую депрессию, Вторую мировую войну и финансовый кризис 2008 г.

Глобальные проблемы начались с приходом COVID-19. Резко сократилось число учащихся, что поставило колледж перед необходимостью крупных инвестиций в технологии дистанционного обучения. Однако окончательный удар был нанесён 19 декабря 2021 г., когда компьютерная сеть организации подверглась атаке программы-вымогателя. Пострадали разделы приёмной комиссии и финансовая часть.

Сбой в системах продолжался полтора месяца. Системы полностью восстановили в марте, но была сорвана работа приёмной комиссии и затруднён доступ ко всем институциональным данным. Колледж не сумел набрать студентов на весенний семестр, а перспективы зачисления на осень 2022 г. оказались под вопросом.

В марте колледж проинформировал, что будет вынужден закрыться в конце весеннего семестра, если не получит крупного пожертвования или предложения о партнёрстве. 5 апреля президент колледжа Дэвид Герлах обратился к Илону Маску через Twitter с просьбой о поддержке и спасении колледжа.

Для продолжения работы требовалось \$50 млн. Попытка собрать часть суммы — \$20 млн в рамках кампании Go Fund Me провалилась: собрали всего \$2252.

По словам главы колледжа Д. Герлаха, виновники краха колледжа живут в Иране. Учебное заведение стало жертвой базирующейся там банды вымогателей. Колледж заплатил выкуп в размере \$100 тыс., чтобы восстановить доступ к затронутым системам. Однако даже после выплаты этой суммы потребовались месяцы, чтобы полностью восстановить работоспособность системы.

По данным компании Emsisoft, в 2021 г. злоумышленники-вымогатели атаковали 26 колледжей США и 62 школьных округа. После половины инцидентов были украдены персональные данные. Хакеры-вымогатели часто крадут данные перед шифрованием систем и шантажируют жертв, требуя

многомиллионные выкупы ещё и под угрозой утечки данных.

По данным NBC, Чёрный колледж Иллинойса — первое высшее учебное заведение США, закрытое из-за программ-вымогателей.

ТУРЦИЯ. ЛЕТО — ЭТО МАЛЕНЬКАЯ ЖИЗНЬ

Türk Telekom, один из лидеров в области информационных и телекоммуникационных технологий в Турции, владеющий крупнейшим центром кибербезопасности в стране, продолжает поддержку профессионального роста молодёжи.

Летом 2022 г. при Türk Telekom проходит летний лагерь для тренировки навыков будущих экспертов в области кибербезопасности. Это третий подобный лагерь, занятия длятся 10 дней в августе.

Лагерь предоставляет молодым людям, которые хотят совершенствоваться в области кибербезопасности, отличную возможность повысить квалификацию и продолжить карьерный рост.

Türk Telekom как организация с крупнейшим центром кибербезопасности в Турции заинтересована в передаче знаний в области ИБ молодёжи и подготовке кадровых ресурсов в рамках Национальной концепции кибербезопасности Турции. Компания даёт возможность молодым людям получать знания в области кибербезопасности, которая сегодня становится основой национальной и личной безопасности.

Занятия проводят известные представители отрасли. Участники проходят базовую подготовку, включая введение в кибербезопасность, основы сетевой безопасности, безопасность операционных систем, телекоммуникаций, беспроводных сетей и мобильной связи. Они также получают всесторонние знания по тестам на проникновение, учатся определять кибератаки, реагировать на них, искать киберугрозы и т.д.

Тройка лучших учеников, победивших в конкурсе, который проходит в рамках лагеря, получает ценные призы на сумму 60 тыс. турецких лир.

*По материалам ИноСМИ
подготовила Марина Бродская*

МИНИСТРЫ, ВЫМОГАТЕЛИ, ГЕРОИ...

ТРЕТЬ ИЗ РАБОТАЮЩИХ НА ПЛАНЕТЕ КИБЕРБЕЗОПАСНИКОВ ГОТОВЫ СМЕНИТЬ РАБОТУ. ТЕМ ВРЕМЕНЕМ ХАКЕРЫ НАХОДЯТ НОВЫЕ ПУТИ ДЛЯ ОБОГАЩЕНИЯ

В АВСТРАЛИИ ПОЯВИЛСЯ МИНИСТР КИБЕРБЕЗОПАСНОСТИ

31 мая 2022 г. в Австралии появился министр по вопросам кибербезопасности. Бывший стипендиат программы Фулбрайта и выпускница Гарварда Клэр О'Нил стала министром внутренних дел страны и министром кибербезопасности.

Клэр О'Нил вошла в парламент в 2013 г. как член лейбористской партии от округа Хотэм (Мельбурн). Находясь в оппозиции, она занимала посты теневого министра по уходу за престарелыми и теневого министра по инновациям, технологиям и будущему труда. Ещё один специалист по кибербезопасности и коммуникациям — Тим Уоттс — назначен помощником министра иностранных дел.

При прежнем коалиционном правительстве вопросы кибербезопасности входили в компетенцию МВД. Экс-министр МВД Карен Эндрюс часто делила полномочия в этой сфере с помощником министра обороны Эндрю Хасти, который занимался вопросами национальной безопасности и обороны.

Ушедшее в отставку правительство Австралии активно решало проблемы кибербезопасности. Был принят закон, который повысил роль правительства в решении вопросов ИБ, одновременно возлагая на организации и предприятия большую ответственность за принятие решений и смягчение последствий кибератак.

В ходе предвыборной кампании премьер-министра Энтони Альбанезе критиковали за то, что он уделяет недостаточно внимания вопросам кибербезопасности. Позже он «исправился» и заявил, что будет уделять приоритетное внимание ИБ как важнейшему элементу политики

национальной безопасности лейбористов. Назначение профильного министра стало первым шагом в этом направлении.

АТАКА НА СКОТОБОЙНИ

В 2021 г. международный мясоперерабатывающий гигант JBS Foods был взломан предположительно российскими хакерами, которые требовали выкуп в размере \$11 млн. Кибератака привела к остановке глобальных операций компании на пять дней, включая остановку нескольких австралийских скотобойен. Позднее представители JBS Foods заявили, что компания заплатила преступной группировке \$14,2 млн в биткоинах, чтобы положить конец кибератаке, которая остановила деятельность заводов по всему миру.

Пострадали и другие предприятия пищевого сектора. О закрытии производства после кибератаки 2020 г. сообщал один из крупнейших в Австралии переработчиков молока и пива компании Lion. Toll Group, один из крупнейших дистрибьюторов продуктов питания в Австралии, был дважды взломан и закрыт в 2020 г.

Австралийский центр кибербезопасности отмечает, что чаще всего хакеры используют вредоносное ПО, программы-вымогатели, проводят DDoS-атаки и осуществляют кибершпионаж. Атаки вредоносных программ стали обычным для хакеров способом получения выкупа.

Через несколько месяцев после взлома JBS Foods в Австралии были приняты законы, включающие продукты питания и напитки в список важнейших отраслей национальной промышленности. Были введены нормативы обязательного информирования о кибератаках и усилены обязательства по кибербезопасности для активов национального значения.

По данным австралийского Центра кибербезопасности, в 2021 году киберпреступность выросла на 13%, а потери составили \$33 млрд. Около четверти из 67,5 тыс. сообщений о киберпреступлениях были связаны с критической инфраструктурой Австралии. Целью хакеров становились здравоохранение, распределение продуктов питания и энергетика.

Эксперты отмечают тенденцию: за последние три-пять лет между национальными киберпреступными группами стало намного больше координации. Например, восточноевропейские группировки занимаются киберпреступностью как услугой, а некоторые из них получают защиту и поддержку на уровне государства.

В ЗАМБИИ ХАКЕРАМ УКАЗАЛИ НА ВЫХОД

Центральный банк Замбии заявил, что отказался выплачивать выкуп хакерской группе, известной как Hive, причинившей ущерб банковским системам страны.

«Наши основные системы работали и по-прежнему работают, — заявил Грег Нсофу, директор по информационным и коммуникационным технологиям Банка Замбии. — Хакерам удалось похитить не так уж много конфиденциальных данных». По его словам, произошла утечка только некоторых тестовых данных. «Мы защитили основные системы, и нам не было необходимости даже вступать в разговор о выкупе, — сказал Нсофу. — Мы указали хакерам на выход».

13 мая Центральный банк Замбии заявил, что он подвергся кибератаке, которая 9 мая нарушила работу некоторых ИТ-приложений, включая веб-сайт ЦБ и систему мониторинга изменений.



Отчёт ISACA State of Cybersecurity 2022

Некоторое время веб-сайт банка был недоступен для пользователей.

Программа-вымогатель Nive, впервые обнаруженная в июне 2021 г., уже рекомендовала себя как одно из самых агрессивных средств-вымогателей, говорится в отчёте японской компании по кибербезопасности Trend Micro. По данным ФБР США, это ПО используется для кражи данных и шифрования файлов жертв, получающих письма с требованием выкупа. Известно, что группировка Nive использует партнёрские программы, привлекая сторонних хакеров. Жертвами вымогателей в 2021 г., по данным Group-IB, стали 355 компаний. Многие платить выкуп отказались.

В ПРОФЕССИИ МНОГО РАЗОЧАРОВАННЫХ

Более трети специалистов по кибербезопасности в мире планируют сменить профессию из-за разоча-

рования в ней. Такая ситуация усугубит нехватку кадров в отрасли, что скажется на способности организаций эффективно защищать свои системы, говорится в отчёте по итогам исследований, проведённых по заказу компании Trellix.

Опрос специалистов по кибербезопасности показал, что главными причинами разочарования стали отсутствие чёткого карьерного роста (35%), общественного признания работы (31%) и ограниченная поддержка со стороны коллег и начальства.

Несмотря на то что подавляющее большинство опрошенных (92%) занимаются любимым делом, 36% респондентов отметили, что чувствуют недостаток признания своей работы. 12% заявили, что из-за этого планируют сменить сферу деятельности.

Согласно отчёту ISACA о состоянии кибербезопасности за 2022 г.,

опубликованному в марте, основными причинами ухода специалистов по кибербезопасности с работы были:

- ♦ наём в другие компании (59%);
- ♦ недостаточное финансовое стимулирование в виде заработной платы или бонусов (48%);
- ♦ ограниченные возможности продвижения по службе и саморазвития (47%);
- ♦ высокий уровень стресса, связанный с работой (45%);
- ♦ отсутствие моральной поддержки со стороны руководства (34%).

«В отрасли уже не хватает 2,72 млн человек, — прокомментировал итоги исследования генеральный директор Trellix Брайан Пальма. — Обучение и воспитание новых кадров требует охвата большей аудитории, изменения подходов к проблеме в государственном и частном секторах».

Сокращение кадрового дефицита в сфере кибербезопасности является

не только бизнес-императивом, но и важным вопросом для национальной безопасности и повседневной жизни. Необходимо устранить барьеры для входа в профессию и вдохновлять уже работающих в сфере ИБ людей, чтобы они получили поддержку на местах.

В попытке удержать персонал в сфере ИБ респонденты заявили, что поддержка развития навыков (85%) и получение сертификатов (80%) чрезвычайно важны. Однако 94% опрошенных считают, что работодатели должны делать больше для программ наставничества и начинать профориентацию ещё в школе.

ОДНАЖДЫ В НИГЕРИИ

Интерпол задержал трёх граждан Нигерии за хранение поддельных документов: счетов-фактур и официальных писем. Позже их обвинили и в кибермошенничестве: они использовали трояны удалённого доступа (RAT), в частности Agent Tesla.

«Эти люди использовали RAT для перенаправления финансовых транзакций и воровства конфиденциальных данных у нефтяных и газовых компаний в Юго-Восточной Азии, Северной Африке и на Ближнем Востоке», — говорится в заявлении Интерпола.

Один из мошенников, Хендрикс Оморуме, приговорён к одному году тюремного заключения. Двое находятся под следствием.

Обвиняемые систематически использовали Agent Tesla для взлома компьютеров организаций и перевода денег на свои банковские счета.

Вредоносная программа Agent Tesla на базе.NET впервые появилась в 2014 г. Она распространяется через фишинговые электронные письма, позволяет перехватывать любые действия на компьютере, включая кейлоггинг, захват экрана, и красть учётные записи и другую конфиденциальную информацию.

Аресты были проведены в рамках глобальной правоохранительной операции под кодовым названием «Пчёлка-убийца» с участием Интерпола и властей из 11 стран Юго-Восточной Азии, включая Бруней, Камбоджу, Индонезию, Лаос, Малайзию, Мьянму, Филиппины, Сингапур, Таиланд и

Вьетнам. Это уже третья подобная операция. Предыдущие — Falcon I и Falcon II — были проведены в 2020 и 2021 гг. сотрудниками Интерпола и компаниями Group-IB, Palo Alto Networks и Trend Micro.

В поле зрения правоохранителей попал и лидер нигерийских хакеров группировки SilverTerrier. Его задержали в рамках спецоперации Delilah, инициированной в мае 2021 г. и успешно завершённой в 2022 г. При участии правоохранителей Австралии, Канады и США сотрудники Интерпола идентифицировали личность лидера группировки, отследили его действия в сети, контролировали перемещения по миру. На основании этой информации нигерийская полиция задержала подозреваемого в международном аэропорту в Лагосе и предъявила обвинение.

КОРЕЙСКИЕ ХАКЕРЫ РАБОТАЛИ НА ШПИОНА

После десяти лет расследования прокуратура Центрального округа Сеула выдвинула окончательные обвинения против пяти человек. Подозреваемые вступили в сговор с северокорейскими шпионами и киберпреступниками для взлома компьютерной сети NongHyup — одной из крупнейших финансовых групп Южной Кореи.

Троих арестовали в декабре 2021 г., двоим, оставшимся на свободе, предъявили обвинения в мае 2022 г.

«В июне-июле 2011 г. обвиняемые встретились с северокорейским шпионом в Даньдуне (КНР) и, получив инструкции, вернулись в Южную Корею. Они собрали секретные сведения о финансовой группе NongHyup, включая IP-адреса компьютерной сети компании, и передали их северокорейскому хакеру, — говорится в заявлении прокуратуры. — Хакеры КНДР использовали эти сведения для организации кибератаки на компанию, но в конечном итоге потерпели неудачу».

Значительного прогресса в расследовании хакерской атаки на NongHyup южнокорейские сыщики добились после перехвата в 2018 г. отчёта северокорейского хакера своим хозяевам. Взяв след, полиция и прокуратура работали

вместе и не торопясь, но с гарантией провели аресты людей, принимавших участие в подготовке атаки.

ПРОСТО ГЕРОЙ (ПОЧТИ КАК В КИНО)

Ветеран кибербезопасности, работавший с крупнейшими государственными агентствами США, устроился простым преподавателем в Академию округа Ричмонд.

Дэниел Джексон, поработавший за 20 лет службы в АНБ, Министерстве обороны и Киберцентре в Форт-Гордоне, теперь делится своим опытом со студентами родного округа. Для будущих безопасников это может стать стартом к профессиональному успеху. Тем более что инициативу преподавателя поддерживает компания Cisco Systems и местное сообщество экономической зоны Центрального района реки Саванна, объединяющего 14 округов, где большинство населения имеет доходы ниже федерального уровня бедности.

По воспоминаниям самого Джексона, в школе он не имел знаний, чтобы сознательно выстроить своё будущее. Он ушёл в армию, где его заставили работать с радио и антеннами, позже занимался обслуживанием компьютеров, настройкой коммутаторов и маршрутизаторов. Становиться серьёзным безопасником у него и в мыслях не было. Теперь он хочет передать свои знания и опыт школьникам.

Джексон планирует не только преподавать, но и в целом улучшить профориентацию в округе: наладить местное профессиональное, техническое и сельскохозяйственное образование. К работе он подключил АНБ, Министерство обороны и Киберцентр в Форт-Гордоне. Cisco Systems готова построить в школах лаборатории для обучения школьников азам информационных технологий и кибербезопасности.

Энтузиаст своего дела, Джексон считает, что вложения в образование могут помочь решить многие проблемы его малой родины: обуздать насилие, заполнить вакансии на промышленных предприятиях и снизить процент отсева из средней школы.

Обзор подготовила
Анна Катанкина



Екатерина РАЧКОВА
управляющий
директор
Управления
по обеспечению ИБ
Банка ВТБ (ПАО)

ХАВАЛА

СВОЙ СРЕДИ ЧУЖИХ, ЧУЖОЙ СРЕДИ СВОИХ

Не криптовалютой единой пытались и пытаются решить свои проблемы клиенты, по тем или иным причинам испытывающие сложности с доступом к классическим платёжным механизмам. Так, задолго до банковской системы западного образца в мире возникли расчётные системы, отличительной чертой которых была возможность трансграничной передачи денег и других материальных ценностей без сопроводительных финансовых документов, исключительно на доверии участников процесса.

«ЛЕТАЮЩИЕ ДЕНЬГИ»

Самой старой из таких систем считается китайская фэй-чен, или «летающие деньги», возникшая в эпоху династии Тан (618–907 годы н.э.). Торговцы, возившие свой товар вдоль Великого шёлкового пути, поняли, что брать с собой тяжёлые медные монеты (стандартная связка весила около трёх килограммов), занимавшие к тому же много места, неудобно, и стали использовать бумажные чеки, удостоверявшие факт совершения какой-либо сделки. Платёжеспособность их владельца гарантировалась подворьями провинциальных властей в

столице. Поскольку все основные торги велись именно там, купцы обменивали выручку в монетах на «летающие деньги» в представительстве своей провинции, а оказавшись дома, производили обратную операцию. Правительство династии Тан неоднократно пыталось запретить «летающие деньги», но в 812 году они были официально приняты в качестве действительного средства обмена.

Позже подобные системы появились на Филиппинах (падала), в Таиланде (пэй-кван), в Сомали (кса-вилаад) и других странах, но наиболее известной стала распространённая на Ближнем Востоке, в Африке и Азии хавала.

ХАВАЛА В ИСТОРИИ

Хавала, традиционно ассоциируемая с исламским банковским правом, на самом деле появилась в Индии в VIII веке н.э., когда при необходимости перевода денег в другой город караванщики начали перевозить с собой некое подобие современных дорожных чеков (хунди), которые до относительно недавнего времени были распространены в сельской местности, где банковская система развита слабее, чем в городах, и считались в Индии обычным финансовым инструментом.

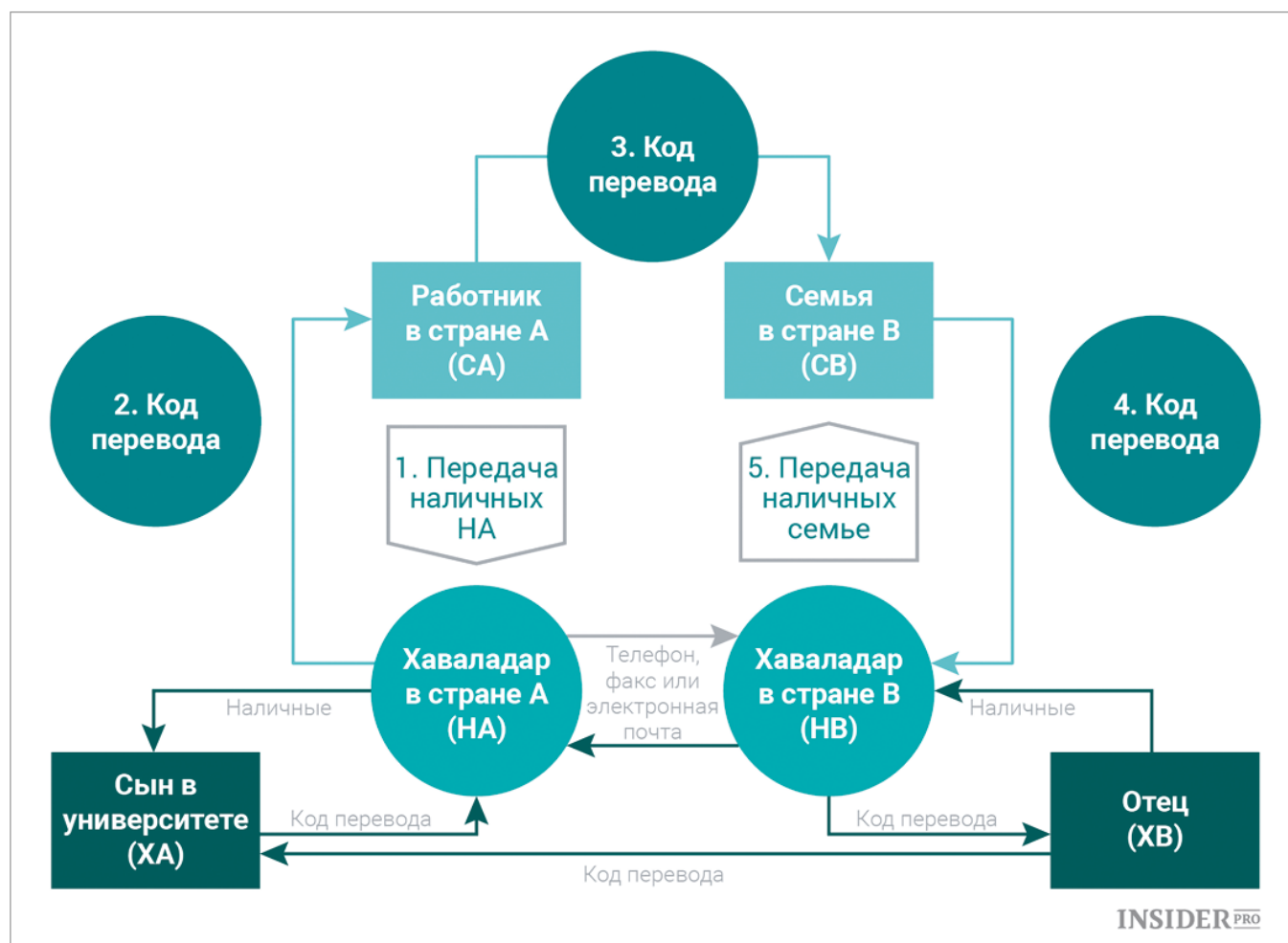


Рисунок 1. Схема действия современной хавалы

ХАВАЛА СЕГОДНЯ

В современном мире хавала представляет собой основанную на доверии систему денежных переводов с использованием однократных уведомлений по электронной почте, факсу или телефону.

Операторами хавалы являются брокеры системы (хаваладары). Отправитель отдаёт деньги брокеру в одной стране и получает от него секретный код, который должен будет передать тому, кому предназначается перевод. В качестве кода может использоваться номер купюры или даже определённая последовательность рукопожатий (очень распространённый способ в регионах с большой долей неграмотного населения).

После того как брокер отправителя свяжется со своим партнёром в стране получателя перевода, получатель в другой стране сможет забрать отправленную сумму у брокера в другой стране в местной валюте, предъявив секретный код. Удостоверение личности в любом случае не требуется, что позволяет клиентам сохранять анонимность (рис. 1).

Отличительной чертой хавалы является отсутствие обмена какими-либо долговыми инструментами между брокерами: сделки проходят исключительно на доверии и под гарантии всей системы. Поскольку хавала не зависит от правового обеспечения и контролирующих органов государства, она может работать даже при отсутствии юридических норм и банковской системы вообще.

Брокеры рассчитываются между собой по клиринговой схеме, через определённые периоды. Для закрытия сальдо могут использоваться золото, драгоценные металлы или оказываться услуги. Такой способ организации расчётов называется простой обратной хавалой. Существуют также варианты трёхсторонних соглашений с брокерами. Хаваладары могут входить в состав сети, распространённой на несколько юрисдикций. При этом участниками подсчитывается соотношение платежей и поступлений средств за определённый период для сведения своих соответствующих счетов.

В системе хавала финансовые транзакции осуществляются методом взаимозачёта и при личных встречах (что случается значительно реже). Поэтому государственным органам отследить эти транзакции не представляется возможным.

СО СТОРОНЫ РЕГУЛЯТОРОВ

Здесь следует отметить, что международными регуляторами ведётся работа по выделению критериев выявления операторов подобных расчётных систем на основании совокупности факторов. Так, довольно широкий перечень индикаторов для выявления подозрительных систем типа «хавала» и других провайдеров аналогичных услуг был создан Группой разработки финансовых мер борьбы с отмыванием денег (ФАТФ/FATF, <http://www.fatf-gafi.org/>) — межправительственной организацией, разрабатывающей и популяризирующей свои принципы для защиты мировой финансовой системы от угроз отмывания денег, финансирования терроризма и финансирования распространения оружия массового уничтожения (рекомендации ФАТФ являются общепризнанными международными стандартами по противодействию отмыванию денег и финансированию терроризма (ПОД/ФТ)).

Данный перечень приведён в разделе 3.6.4 отчёта ФАТФ за октябрь 2013 года «Роль систем „Хавала“ и других аналогичных услуг в отмывании денег и финансировании терроризма»¹.

С ТОЧКИ ЗРЕНИЯ ИБ

С точки зрения информационной безопасности уязвимым местом хавалы являются каналы передачи данных между хаваладарами, а также между получателем и отправителем денежных средств, в случае если требуется передача секретного кода. Передаваемые данные должны быть защищены от подмены, должна быть

обеспечена их конфиденциальность, а между брокерами установлен надёжный протокол взаимной аутентификации. Также считается, что при построении системы по этническому и территориальному признакам хавала хорошо защищена от мошенничества и недобросовестных участников сделок. Информация в сообществах распространяется мгновенно, и скомпрометированный хаваладар выбывает из экономических отношений в рамках сети хавала навсегда.

ВОЗМОЖЕН ЛИ РЕНЕССАНС ХАВАЛЫ?

Особое развитие в настоящее время хавала получила в Пакистане. По некоторым оценкам, на долю этой страны приходится свыше полутора тысяч точек хаваладас, обеспечивающих перевод денег от работающих за рубежом пакистанцев. Так, в одной только Испании работает около 200 отделений хавалы, обслуживаемых в основном выходцами из Пакистана.

Считается, что важную роль в распространении хавалы в странах Запады сыграла готовность компаний сотрудничать с исламскими финансовыми институтами при разработке нефтяных месторождений и добыче нефти, развитии новых отраслей производства и в сфере сельского хозяйства. Работа в исламских странах с местными финансовыми организациями неизменно приводила к контактам с системой хавала — в силу специфики общественно-экономических отношений. Многие юридические и финансовые компании, такие как Norton Rose, Freshfields, Clyde and Co., Clifford Chance, имеют отдельные подразделения, специализирующиеся на особенностях исламской банковской системы (так называемые Islamic Finance teams).

* *

И хотя в России хавала имеет «криминальное прошлое» (имеются в виду уголовные дела 2007–2010 гг. и платёжная система братьев Гаджиевых), сейчас она вполне может получить второе рождение и новый легальный ренессанс.

¹ С данным отчётом в переводе Международного учебно-методического центра финансового мониторинга можно ознакомиться по ссылке https://www.feds-fm.ru/content/files/documents/fatf/роль_хавалы_в_одфм_fatf_2013.pdf

НА ПРИНЦИПАХ ИСЛАМСКОГО БАНКИНГА

При Правительстве РФ предложили создать структуру для развития цифровой валюты на принципах исламского банкинга. С такой инициативой выступил глава духовного управления мусульман РФ и совета муфтиев России Равиль Гайнутдин в ходе XII заседания группы стратегического видения «Россия — Исламский мир».

Он подчеркнул, что в нынешних условиях России необходимо усилить работу с исламским миром, в том числе в халыль-индустрии, создании правовых условий для исламского банкинга и стимулирования экономического сотрудничества. По его словам, на многие годы основным внешним рынком для России становится именно мусульманский мир.

Источник: <https://www.business-gazeta.ru/news/550638>



АССОЦИАЦИЯ
БАНКОВ
РОССИИ

ХІХ Международный банковский форум «Банки России - ХХІ век»

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

На пленарных сессиях и круглых столах форума традиционно выступают руководители Банка России, федеральных министерств и ведомств, члены Совета Федерации и депутаты Госдумы, топ-менеджеры банков и ведущих компаний финансового рынка.

21-24 сентября 2022 года

г. Казань



Оргкомитет:
Тел. +7 (495) 785-29-93, 785-29-88
e-mail: event@asros.ru
www.asros.ru





**Борис
СТОЛПАКОВ**
историк
криптографии,
кандидат физико-
математических наук

МАТЕМАТИЗАЦИЯ КРИПТОГРАФИИ В СОБЫТИЯХ И ЛИЦАХ

О МАТЕМАТИКЕ, МАТЕМАТИКАХ
И ПРОШЕДШЕМ ВРЕМЕНИ

В июле 2022 года Петербург готовился принять участников Международного математического конгресса. Отечественные математики могли стать гостеприимными хозяевами такой встречи во второй раз. Впервые в нашей стране мировой математический конгресс собрался в Москве в августе 1966 года.

ПРИЗНАНИЕ АВТОРИТЕТА СОВЕТСКОЙ НАУКИ

Это было время триумфа советской науки. Достаточно упомянуть запуск первого искусственного спутника Земли, полёт Ю.А. Гагарина и первый выход человека в открытый космос. Москва тогда по праву стала одним из важнейших мировых научных центров. Каждый год здесь проходили крупные международные встречи учёных. Летом 1966 года Москва приняла участников четырёх мировых конгрессов: микробиологов и кристаллографов, океанографов и математиков. Торжественное открытие Математического конгресса состоялось в кремлёвском Дворце съездов (ныне Государственный Кремлёвский дворец). Фотографы зафиксировали редчайшую ситуацию — присутствие учебной доски с мелом на главной сцене страны (илл. 1).

Почётным председателем Конгресса избрали академика И.Г. Петровского, известного математика, ректора МГУ. Московский государственный университет предоставил аудитории своего главного корпуса для заседаний 4280 участников Конгресса и многочисленных гостей. Одну треть участников

составили советские математики, американцев приехало вдвое меньше, британцев, французов и немцев вместе было около тысячи. Университет нередко принимал участников научных форумов, без особенных усилий обеспечивая необходимый комфорт. Ведь учёба и жизнь студентов в высотном корпусе МГУ были изначально обустроены по самым высоким мировым меркам. Удивительно, но впечатляющий и поныне обширный учебно-научный комплекс МГУ на Воробьёвых горах принял студентов всего через 8 лет после окончания Великой Отечественной войны, 1 сентября 1953 года.

ОБЯЗАТЕЛЬНЫЙ ФУТБОЛ, ПЛАКАТЫ И ПОЧТОВЫЕ МАРКИ

На Конгрессе не обошлось и без традиционного футбольного матча. Сборная советских математиков уверенно победила сборную остального мира со счётом 5:2.

Символика Конгресса была популярна в Москве в те августовские дни (илл. 2). Запечатлелась она и в почтовых марках (илл. 3).

«ЛЕКЦИЮ ПРОЧТЁТ АКАДЕМИК КОЛМОГОРОВ»

Общественный интерес к Математическому конгрессу в значительной степени был связан с активной государственной поддержкой в 1960-е годы физико-математического образования молодёжи. В СССР была создана целая система физматшкол, классов «с математическим уклоном», как тогда говорили,

кружков и олимпиад. Предметные олимпиады впечатляли своим действительно олимпийским уровнем. В 1963 году открыли физико-математические школы-интернаты в Москве, Ленинграде, Киеве и Новосибирске, а в 1964 году — Всесоюзную заочную физматшколу при мехмате МГУ. Проведение Математического конгресса в Москве стало стимулом для дальнейшего активного привлечения молодёжи в науку. Пример подавали самые маститые математики. Так, в октябре 1968 года в газете «Московский университет» появилось объявление о предстоящем выступлении А.Н. Колмогорова в Актовом зале МГУ. Темой стали «Математические структуры и реальный мир». Заметка была озаглавлена «Лекцию прочтёт академик А.Н. Колмогоров». В её содержательной части можно обнаружить, вероятно, авторство Андрея Николаевича:

«Одним из центральных понятий современной математики является общее понятие структуры. В лекции будет популярно объяснён смысл этого понятия. Математические структуры находят применение при изучении реального мира и в человеческой практике в качестве моделей реальных явлений. Но при формальном изложении математики скрывается другая сторона дела — реальное происхождение математических структур.

В лекции А.Н. Колмогорова будет дан обзор простейших математических структур, в частности, лежащих в основе школьного курса математики, в плане их возникновения при изучении реального мира и практики».



Иллюстрация 1. На пленарном заседании в Кремле

По отзывам очевидцев, в самом начале лекции, окинув взглядом первые ряды слушателей, Андрей Николаевич заявил, что предполагал встречу с более молодой, не искушённой в математике аудиторией. А поскольку в зале присутствуют и опытные математики, то для поддержания их интереса к происходящему он немедленно скорректирует план своего выступления. Эти слова вызвали заметное оживление в зале. У присутствовавших на лекции в памяти осталось ощущение глубокой заинтересованности именитого учёного и в научном, и в неформальном общении с учащейся молодёжью.

Имя академика Колмогорова было хорошо знакомо многим школьникам. Особенный интерес у них вызывал «колмогоровский» физико-математический интернат при МГУ. А. Н. Колмогоров уделял ему много внимания, подбирая преподавателей, заботился о питомцах (илл. 4).

Многие выпускники интерната ежегодно обильно пополняли не только мехмат МГУ, но и ряды будущих криптографов, обучавшихся на Техническом факультете ВШ КГБ. Это учебное подразделение позднее было преобразовано и расширено, став основой известного ныне Института криптографии, связи и информатики (ИКСИ) — головного среди вузов России учебного заведения по

подготовке специалистов в области информационной безопасности. Первый выпуск инженеров-математиков на дневном отделении Технического факультета состоялся именно в 1966 году.

1960-Е ГОДЫ — ПИК ИНТЕРЕСА К ФИЗИКЕ И МАТЕМАТИКЕ

Интерес молодёжи к математике и физике в значительной степени был связан со стремительным развитием радиотехники и вычислительной техники, обеспечившим и космические



Иллюстрация 2. Приметы Конгресса



Иллюстрация 3. Марка с символикой московского Математического конгресса

полёты. В 1961–1962 годах первые автоматические межпланетные станции уже отправились к Венере и Марсу. Зашифрованная телеметрия с этих станций принесла на Землю первые сведения о дальнем космосе. Тогда, в начале 60-х, среди школьников стало популярным конструирование миниатюрных приёмников из доступных в розничной продаже радиодеталей, в том числе транзисторов. Это было увлечение сотен тысяч подростков, если не миллионов.



Иллюстрация 4. А. Н. Колмогоров со школьниками. Фото середины 1960-х годов

Возможно, некоторым из читателей покажется неожиданным, но в 1950-е и 60-е годы советские разработки вычислительной техники были среди лидирующих в мире. Так, БЭСМ-6 демонстрировала рекордное быстродействие — 1 млн операций в секунду. Да и первый в мире компьютер 3-го поколения (по технологии интегральных схем) создали в 1963–1964 годах в Ленинградском НИИ радиоэлектроники на основе гибридных интегральных схем собственной разработки. Согласно воспоминаниям специалистов, это был бортовой авиационный компьютер «Гном».

ДОБРЫЕ ТРАДИЦИИ — КЛЮЧ К УСПЕХУ

Проведение в 1966 г. Математического конгресса в Москве, безусловно, свидетельствовало о высоком научном авторитете московской математической школы, созданной трудами Дмитрия Фёдоровича Егорова и его учеников, прежде всего Николая Николаевича Лузина. Научной школы, отметившей тогда свой полувековой юбилей. В настоящее время уже тысячи специалистов, причастных к математике, причисляют себя к наследникам этой школы.

Нелишне заметить, что и развитие советской криптографии обеспечили и определили тоже представители школы Егорова — Лузина.

Как известно, в конце 1940-х годов в обстановке послевоенной ограниченности ресурсов государства все силы были сконцентрированы на создании ракетно-ядерного щита и его информационной защиты. Математический институт им. В.А. Стеклова АН СССР играл в этом деле активную роль. В решении сложных научно-технических задач, связанных с ракетно-ядерной проблематикой, принимала участие львиная доля сотрудников института, собранных в его отделении прикладной математики под руководством выдающегося учёного М.В. Келдыша. Чуть позже, в 1953 году, для академической поддержки в решении задач криптографического направления в институте был создан отдел прикладных расчётов. Его возглавил заместитель директора Математического института академик К.К. Марджанишвили.

В это же время в недрах Главного управления Специальной службы (ГУСС) при ЦК ВКП(б) начала складываться советская криптографическая школа, сразу установившая высокую планку для уровня математической проработки перспективной шифровальной аппаратуры. Спектр задач, требовавших первоочередного решения, был очень широк.

ЧТО МАТЕМАТИКИ ПРИВНЕСЛИ В КРИПТОГРАФИЮ?

Представьте себе сложно устроенную аппаратуру. Как её анализировать? Вероятно, для этого нужно создать сначала математические модели её работы — хотя бы и в виде систем сложнейших уравнений, но всё же позволяющих производить расчёты. Далее необходимо учесть, что аппаратура действует в реальных условиях, то есть сигнал, выходящий из неё, распространяется в пространстве, в определённой среде, обладающей теми или иными не вполне ясными и меняющимися свойствами. Таким образом, в дело вступает уже физика. Учёт её требований заметно усложняет задачи моделирования.

Но и это были ещё не все основные задачи. Чего хотят потребители шифровальной аппаратуры? Чтобы выход сигнала в пространство выглядел случайным процессом, чтобы никто посторонний не увидел в нём никакой закономерности. Поэтому надо создавать алгоритмы проверки на случайность и развивать теорию статистических критериев такой проверки. Это тоже большое направление, которое начало активно развиваться в 1940-е годы. К нему примыкают и проблемы гарантии качества ключей для шифров, а также постоянная потребность в эффективных способах выработки больших массивов случайных чисел.

ДЛЯ ТЕХ, КОМУ ИНТЕРЕСНО

Как ведут себя случайные последовательности, составленные всего из двух знаков 0 и 1? Попробуем проверить свою интуицию. Всем знакома игра с подбрасыванием монеты и угадыванием выпавшей стороны. Представим себе игру двух участников, каждый из которых после очередного бросания «идеальной»

монеты получает или платит выигрыш — 1 в зависимости от результата бросания. При этом выпадение «герба» даёт выигрыш первому игроку, а выпадение «решки» даёт выигрыш второму. Лидером в данный момент считается тот, у кого сумма выигрыша положительна. Пусть игра прекращается, например, после 1000 подбрасываний монеты. Вопрос: долго ли будет лидировать каждый игрок? Оказывается, если игры (по тысяче бросаний монеты) будут проведены многократно, то чаще всего ответ на вопрос получится таким — почти всё время лидировал лишь один игрок. Каждому читателю предоставляется возможность оценить свою интуицию. Заметим, что криптографы-математики, как отечественные, так и зарубежные, обнаружили и обнаруживают доныне много неожиданных фактов.

ДЛЯ ТРУДОЁМКИХ РАСЧЁТОВ

Наконец, для весьма трудоёмких расчётов при моделировании работы шифровальной аппаратуры нужна вычислительная техника. Значит, требуется создание вычислительных машин. Как известно, первые мощные вычислительные устройства были созданы в годы Второй мировой войны именно для нужд криптографии. В СССР значительных успехов на этом поприще добился В.С. Полин (1908–1975).

Владимир Степанович происходил из потомственных тульских оружейников. Физик по образованию, криптографом он стал по военному призыву в июне 1941 года. К началу 1950 годов В.С. Полин по праву считали лидером в создании и использовании вычислительных устройств в криптографических исследованиях. Тогда удачно совпали по времени яркие идеи по конструированию цифровых ЭВМ, появление новой элементной базы и разработка оригинальных алгоритмов для реализации криптографических методов анализа шифров. Весомый вклад В.С. Полина и его учеников в развитие специализированной вычислительной техники в 1957 году был отмечен Ленинской премией. В 1959–1964 годах под непосредственным руководством В.С. Полина была создана полупроводниковая вычислительная машина «Весна», ставшая лидером по производительности в своём классе.

ДОСТОИН СТАТЬ СИМВОЛОМ

Таким образом, трудно представить себе другое научно-техническое направление, где для математиков возникало бы столько разнообразных практических задач. И ещё труднее представить себе руководителей, способных систематизировать это разнообразие, упорядочить его по степени неотложности и направить усилия немногочисленных специалистов, привлечённых к решению конкретных проблем. Одним из таких руководителей стал Иван Яковлевич Верченко (1907–1995) (илл. 5).

Ныне его имя символизирует в некотором смысле послевоенную математизацию криптографии. Закономерно, что популярные среди школьников межрегиональные олимпиады по математике и криптографии, по информатике и компьютерной безопасности стали олимпиадами имени И. Я. Верченко. Хотя бы кратко упомянем некоторые события его жизни, ярко связанные с математикой и криптографией.

Иван Яковлевич родился неподалёку от Луганска в семье рабочего железной дороги. В 1925 г., восемнадцати лет, после фабрично-заводской школы начал трудиться на динамитном заводе. Уже вскоре в производственной аварии потерял правую руку до локтя. Долго лечился, заново учился писать и трудоустроился писарем на заводе в Мариуполе. После нескольких лет упорных занятий в 1929 г. поступил на физико-математический факультет МГУ. Трудно сказать, на какую специальность рассчитывал Иван Верченко, ведь университетское образование тогда переживало всю тяжесть эпохи перемен. Так, в 1929 г. Главпрофобр решил выпускать из университетов инженеров и в 1930 г. исключил из учебного плана физмата ряд теоретических дисциплин. Тогда же ректорат был преобразован в дирекцию, но вновь появились кафедры и стало обязательным посещение лекций и семинаров, а для проведения общественных студенческих мероприятий установили специальные дни. В 1931 г. вместо факультетов образовали отделения и лекции перестали считаться главной формой обучения, вместо них воцарился бригадно-лабораторный метод. Удивительно,

что в такой обстановке молодой, но уже познавший суровую прозу жизни человек с далёкой периферии увлёкся глубинами абстрактной математики. Более того, своими способностями и энергией он привлёк внимание профессора А. Н. Колмогорова, почти своего ровесника. Ко времени окончания Иваном Яковлевичем университета, в 1934 г., они опубликовали две совместные статьи в самом престижном издании — Докладах Академии наук СССР. Затем последовали учёба в аспирантуре под руководством Колмогорова, успешная защита кандидатской диссертации в 1937 г. и педагогические труды в Ростовском-на-Дону университете. Как известно, там лекции Ивана Яковлевича слушал и будущий писатель, а тогда студент Александр Солженицын. Хорошо известна также их встреча в конце 1940-х годов в Марфино уже на криптографическом поприще.

НАЧАЛО СОВЕТСКОЙ ШКОЛЫ МАТЕМАТИЧЕСКОЙ КРИПТОГРАФИИ

На криптографическое поле, в МГБ СССР, И. Я. Верченко попал по приглашению Управления кадров ЦК ВКП(б) в 1947 г. А все военные годы он трудился инженером-конструктором в КБ Яковлева, при этом продолжая активно заниматься математикой. В 1949 г. эти занятия вылились в защиту докторской диссертации под руководством А. Н. Колмогорова в Математическом институте им. В. А. Стеклова.

С образованием ГУСС в 1949 г. И. Я. Верченко стал в нём заместителем начальника по науке Научно-исследовательского института № 1 (НИИ-1). В феврале 1951 года решением Политбюро ЦК ВКП(б) при НИИ-1 ГУСС была создана аспирантура. С этого времени началась регулярная работа по подготовке криптографических кадров высшей квалификации, продолжающаяся и по сей день. С самого начала эту деятельность энергично возглавил И. Я. Верченко.

Как известно, после смерти И. В. Сталина ГУСС было упразднено и его функции передали в 1954 году новообразованному 8-му Главному управлению КГБ СССР. Но ещё в 1953 г.

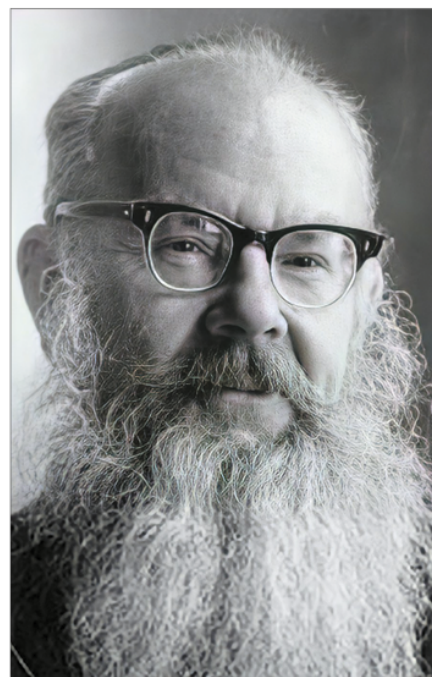


Иллюстрация 5. И. Я. Верченко

Иван Яковлевич покинул специальную службу и вернулся к преподаванию математики. Всё же с началом в 1962 г. вузовской подготовки криптографических кадров на Техническом факультете ВШ КГБ этот факультет возглавил И. Я. Верченко. Его руководство продолжалось 10 лет, до 1972 года.

А в 8-м ГУ КГБ, собравшем немало выпускников МГУ и других ведущих вузов, криптографическая школа стала формироваться вокруг Владимира Яковлевича Козлова (1914–2007). Свойства характера, недюжинные организаторские и математические способности позволили ему создать вокруг себя доброжелательную творческую атмосферу, весьма напоминающую академическую и университетскую. Сам выпускник мехмата 1937 г. и профессор МГУ с 1952 г. В. Я. Козлов не только воспринял традиции математической школы через своего учителя Н. К. Бари, но и сумел достойно использовать их в сообществе криптографов.

В 1966 г., памятным проведением Математического конгресса, В. Я. Козлова избрали в члены-корреспонденты АН СССР. Впереди было ещё много званий и наград, но главным его достижением стал весомый вклад в уверенное и надёжное развитие советской и российской криптографии.

ПИСЬМА И БУМАГИ ИМПЕРАТОРА ПЕТРА ВЕЛИКОГО

САМАЯ ДОЛГАЯ ИЗДАТЕЛЬСКАЯ ПРОГРАММА,
СВЯЗАННАЯ С КРИПТОГРАФИЕЙ

9 июня 2022 года исполнилось 350 лет со дня рождения Петра I (1672–1725), первого всероссийского императора. Это событие напоминает нам и о другом юбилее, связанном с историей криптографии в России.

150 ЛЕТ НАЗАД

150 лет назад, в 1872 г., в ознаменование двухсотлетия Петра Великого было положено начало системному изданию документов, связанных с его личностью и деяниями. В комиссию под председательством министра народного просвещения Д. А. Толстого, образованную для сбора материалов, вошли знаменитости — С. М. Соловьёв и другие крупнейшие российские историки и общественные деятели. Вероятно, в начале своих трудов члены комиссии недостаточно ясно представляли себе объём и сложность предстоящей работы. Многочисленные, как казалось, опубликованные документы составляли лишь капли в море письменного наследия Петра I. Членам комиссии необходимо было разыскать, скопировать и собрать многие тысячи документальных свидетельств, разбросанных по архивным и частным собраниям, в том числе и зарубежным.

ПОЧЕРК ПЕТРА ВЕЛИКОГО

Первый том издания, озаглавленного «Письма и бумаги императора Петра Великого», вышел лишь в 1887 г. В предисловии была отмечена «трудность найти лиц, умеющих правильно читать связный и неразборчивый почерк Петра Великого». С этим легко согласиться, на илл. 1 приведён императорский автограф.

Для нас интересно извещение в предисловии о печатании шифрованных писем и помещении ключей к ним в приложениях.

Действительно, с той давней поры на страницах многотомного издания «Писем и бумаг...» появилось много документов криптографического

характера. Они стали основой современных представлений о защите информации в России в петровское время.

ИЗДАНИЕ ПРОДОЛЖАЕТСЯ

Издание крупноформатных томов с подробно комментированными источниками продолжается до сих пор, хотя

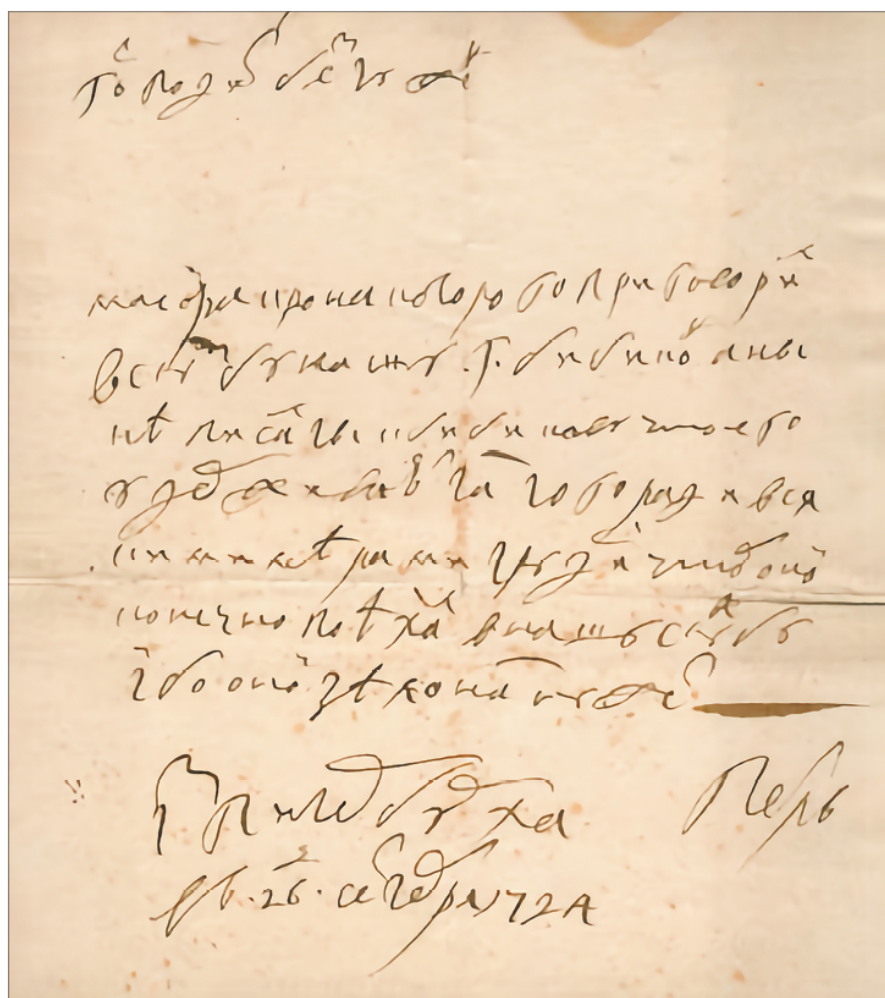


Иллюстрация 1. Автограф Петра I

и с перерывами. Предстоит ещё работа над документами последнего десятилетия жизни Петра I. Главная проблема прежняя — эти рукописи сложно прочитать. Правда, в последнее время появились сообщения о возможном применении для ускорения чтения новых технологий распознавания образов.

ДИПЛОМАТИЯ ВНЕ КОНКУРЕНЦИИ

За прошедшие полтора столетия шифрованная переписка представлена в «Письмах и бумагах...» уже довольно богато. Эта тайная переписка связывала, прежде всего, Петра I и его ближайшее окружение, а также дипломатическое ведомство — Посольский приказ и Посольскую канцелярию — с российскими представителями за рубежом.

На илл. 2 можно видеть пример ключа к дипломатическому шифру — цифирную азбуку 1700 г., составленную Петром I, для переписки с послом в Константинополе П.А. Толстым.

Кроме официальных представителей, Россия имела в Турции своих тайных политических агентов — иерусалимских патриархов Досифея и позже Хрисанфа. Через Досифея шла переписка России и с молдавским господарем. Патриарх Хрисанф предложил канцлеру Г.И. Головкину тайную азбуку для переписки. Она была принята царским двором с некоторыми поправками, по поводу чего Хрисанф писал Головкину: «Приняли мы цифирь, которая прислана в дополнку нашей, и zelo изрядно». Кроме того, Хрисанф предложил использовать при переписке ещё некоторые условности. «А чтоб нам чащей писать к великому государю и к вашему высочеству и безопасно, — писал он Головкину, — зделали мы сию цифирь. Посылаем и образ печати. И как придёт к вам какое письмо, в котором есть та печать, ведомо буди, что есть наше писание. А с лица печать какая-нибудь, только бы что была сия внутри. К тому же: которое письмо имеет с лица круг, то к великому государю; а которое имеет треугольный знак, есть к высочеству вашему. И сие всегда да будет за подлинное». Велась шифрованная переписка и с министрами и вельможами союзных государств.

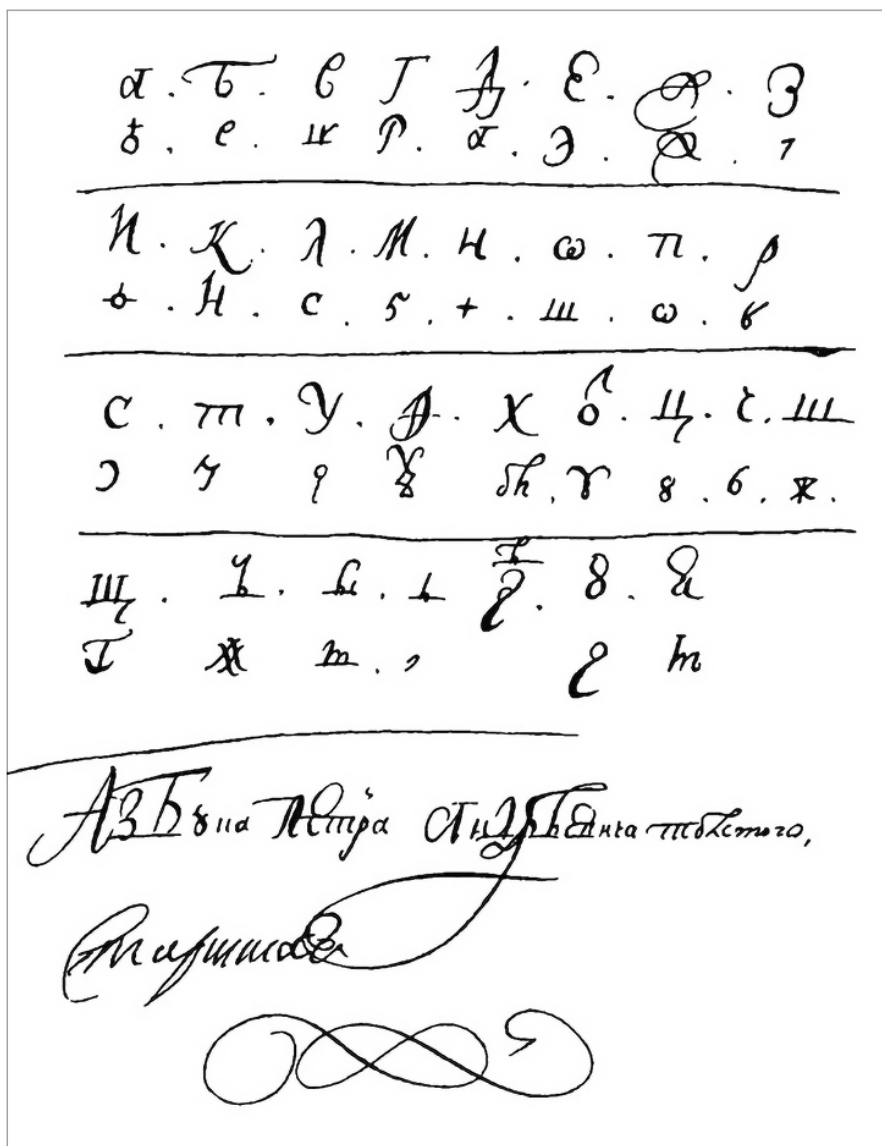


Иллюстрация 2. Азбука П.А. Толстого, 1700 г.

«ИЗВОЛЬТЕ КО МНЕ СИЮ ЦИФИРЬ ПИСАТЬ...»

Высший командный состав армии и флота также имел шифры для переписки с царём. Иногда возникали проблемы с расшифровкой. Так, фельдмаршал Г.Б. Огильви жаловался Петру I: «... никого здесь нет, который бы французское ваше мог разуместь, понеже Рен ключ от того потерял... Извольте ко мне сию цифирь писать, чтоб я мог разуместь...». Царь объяснил, почему он перешёл от шифрованной переписки на немецком языке к переписке на французском: «Французскую азбукою к вам писали для того, что иной не было. А которую вы перво прислали, и та не

годна, понеже так, как простое письмо, честь мочно. А когда другую прислал, то от тех пор ею, а не французскою к вам пишем. А и французской ключ послан».

В шифрованной переписке велика доля военных сообщений. Нередко доставка таких сообщений требовала смекалки. Так, А.С. Келин, комендант осаждённой шведами Полтавы, получил шифрованное письмо Петра I за неделю до Полтавского сражения редким способом. Шесть экземпляров письма прилетели в полых бомбах, так как осада Полтавы не давала иной возможности для их доставки. В послании говорилось: «Когда сии письма получите, то дайте в наши шанцы сегодня

8δλ42φ 7:09δ43Д0935V7:δ:Х45V
а когда будешь 8Lhδ94Д9:5V, тогда Х:
2δ8.XV:2Д4XhωV и что-в выбрали 42454
Д4 Х:2δ:Z: Lh6:8h94 и по совершении
ономъ когда 7:3XhλVД4Д4Xφ2:7:Х:Д0
лежащая Z:δ:293 таксхδ :2Д4XhωV47:Х
:Д80 и протчимъ δhL945V 6hω4φ3H Z:δ:
293 По сей δ:Д73Д3 δ4Д:δ3 3Д4 ХδХ53
Л3Д3 7:094Д0

Из Нарвы, в 28 д. июня 1708. Piter.

Иллюстрация 3. Письмо В. В. Долгорукому

знак, не мешкав, одним великим огнем и пятью пушечными выстрелами рядом..., что вы те письма получили». Через два дня Келин сумел известить Меньшикова в шифрованном письме о замеченной из Полтавы тревоге в шведском лагере и о перегруппировке неприятельских войск после манёвра русской армии.

Среди военной переписки большой объём шифрованных сообщений был связан с подавлением восстания на Дону в 1708 г. Правительственными войсками, направленными на Дон, командовал подполковник В. В. Долгорукий. Одна из депеш, адресованных ему царём, приведена на илл. 3. Конечно, её вид лишь условно соответствует подлиннику. Это пример воспроизведения шифрованных посланий в тексте «Писем и бумаг...».

Была ещё не менее объёмная шифрованная переписка по внутригосударственным вопросам, а также обширная частная секретная переписка.

ТРУДИЛАСЬ В РЕДАКЦИОННОЙ КОМИССИИ С 1946 Г.

В 150-летние труды по изданию «Писем и бумаг...» внесли свою лепту и академики, и менее маститые историки. Нашу особенную благодарность заслужили те, кто способствовал сбору и опубликованию криптографических документов. Среди них первой следует назвать Елену Петровну Подъяпольскую (1895–1986). В редакционной комиссии она трудилась с момента возобновления её работы в 1946 г. после многолетнего перерыва. Именно тогда, наряду с мучительным чтением петровских автографов, она обратилась к расшифровке и дешифровке тайнописи. В архивах ей удалось обнаружить помимо залежей шифрованной информации ещё до ста ключей к шифрам петровского времени. Свой опыт она изложила в обстоятельной статье «Шифрованная переписка в России в первой четверти XVIII в.».



Иллюстрация 4. Е. П. Подъяпольская

опубликованной в 1959 г. в академическом журнале «Проблемы источниковедения». С тех пор каждая публикация, связанная с секретной перепиской времени Петра I, неизменно использует её материалы.

Елена Петровна писала о секретной корреспонденции: «В наших архивах до сих пор лежат нетронутые или только початые пласты таких исторических материалов. Перед историками стоит настоятельная задача их использовать...». «В недалёком будущем, — мечтала Елена Петровна в 1959 году, — на помощь исследователю в деле расшифровки документов придёт „умная машина“ типа машины-переводчика. На долю исследователя выпадет задача раскрыть шифр и составить к нему ключ; на долю машины — заменить шифрованные значки, согласно шифрованной азбуке, буквами соответствующего алфавита, после чего исследователю останется отредактировать текст, составленный машиной».

ПОЧТИ 1700...

Е. П. Подъяпольская первой обратилась к популяризации криптографии среди молодёжной аудитории. В 1966–1970 гг. она опубликовала в журнале «Наука и жизнь» серию из пяти заметок под общим названием «Тайны тайнописи». Там она предложила для

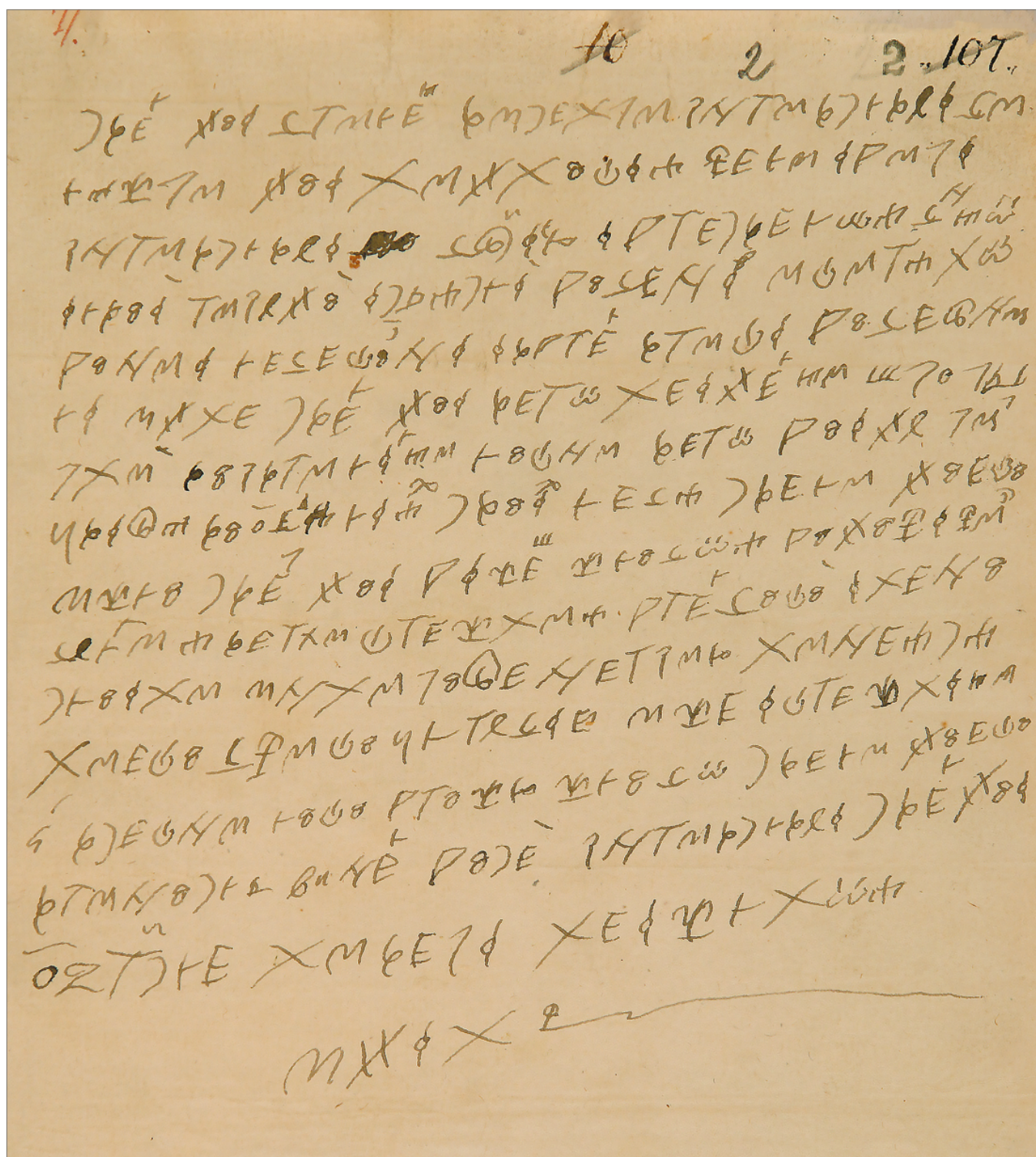


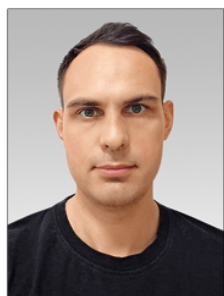
Иллюстрация 5. Письмо Софьи Алексеевны

дешифрования три послания петровского времени и письмо правительницы Софьи Алексеевны боярину Василию Васильевичу Голицыну, возглавившему в 1689 г. поход русских войск к Крыму. Последнее письмо

приведено на илл. 5 в более качественном виде по сравнению с картинкой из «Науки и жизни». Тогда читатели живо откликнулись на предложение Елены Петровны. Почти 1700 человек прислали свои дешифровки письма Софьи

Алексеевны уже в первые два месяца после его опубликования.

Возможно, некоторые из нынешних читателей тоже рискнут частью своего досуга, чтобы узнать, о чём и как писала Софья Алексеевна.



Александр ИГОНИН
эксперт BIS Journal

В ШАГЕ ОТ АУТСОРСИНГА

Не секрет, что многие отечественные компании испокон веку живут по принципу «денег нет, но вы держитесь» (вне зависимости от реальной прибыли). Переехав за рубеж, я с некоторым удивлением заметил, что такой же подход часто исповедуется и здесь. В этом смысле законы бизнеса, как и законы физики, интернациональны :)

Главный метод экономии тот же: использовать аутсорсинг или хотя бы аутстаффинг. Например, если компании нужен департамент ИБ, то она может:

1. Создать собственное ИБ-подразделение.

2. Делегировать ряд функций через аутстаффинг (то есть заменить своих сотрудников штатом подрядчика).

3. Отдать эти функции на аутсорсинг (при этом исполнители будут лишь минимально интегрированы в компанию).

основная битва обычно разворачивается между опциями два и три.

После пандемии компании стали куда охотнее разрешать «удалёнку» — даже в сфере ИБ, что раньше было практически немыслимым. И вроде бы логичен следующий шаг — отдать всё на полный аутсорсинг. С точки зрения менеджмента, это сущий рай: не нужно больше столько офисных площадей, возни с техникой и прочими проблемами. Можно наконец расслабиться, откинуться в кресле и просто читать ежемесячные, еженедельные, а то и ежедневные — это уж насколько паранойя позволяет — отчёты от подрядчика со сверкающими графиками и сияющими таблицами, наглядно демонстрирующими успехи, достигнутые в борьбе с киберугрозами. Но так ли всё светло и радужно в действительности?

Да, переход на аутсорсинг обычно приводит к заметному падению расходов. Дело не только в освобождённых офисных пространствах, но ещё и в том, что зарплата специалиста в холодной Сибири (или солнечной Индии) в разы ниже, чем в Москве (или Дубае). Однако надо понимать, что бесплатного сыра, как и серебряной пули, не существует и за всё в этой жизни приходится платить.

Первое, что страдает от перехода, — это знание инфраструктуры. Когда специалист находится на площадке и всё своё время посвящает одному заказчику, он будет глубже

и лучше понимать его сеть, технологии, особенности и проблемы. Ожидать того же от работника на аутсорсинге нельзя. И дело не просто в физическом отсутствии человека на площадке, но ещё и в размытии фокуса: с огромной вероятностью исполнители будут «размазываться» подрядчиком по нескольким клиентам, ведь экономить и оптимизировать хотят все, а не только вы.

Вторая проблема — коммуникация. С 2020 года множество совещаний переместилось из офлайна в Teams — и на мой взгляд, они стали гораздо менее эффективны. То, что можно за пятнадцать минут объяснить на пальцах или нарисовать на доске, в онлайн-встрече с непредсказуемыми результатами.

Конечно, информационная безопасность как функция ни в коем случае не должна быть вещью в себе, и затраты на неё должны всегда соизмеряться с пользой, которую она приносит. И если компания не может себе позволить больших расходов, то аутсорсинг — прекрасный выход. В остальных же случаях всегда нужно помнить, что он далеко не во всём хорош, что бы там ни обещали красочные презентации и пламенные речи экспертов и консультантов. Ожидания от аутсорсинга должны быть адекватны его реальным возможностям, а не рекламным буклетам.

Ваш покорный слуга сейчас с интересом наблюдает, как любимый заказчик стоит на этом перекрёстке и мучительно выбирает, по какому пути двинуться. Пожелаем же ему удачи!



Первого варианта все боятся как огня: тут и повышенные расходы на оплату труда, и кадровые сложности. Поэтому



SOC ФОРУМ

Практика противодействия кибератакам и построения центров мониторинга ИБ

15–16 ноября, г. Москва, ЦМТ

>> **ЦИФРЫ** за 2021 год

SOC-Форум

> 2000

офлайн-участников

> 10000

онлайн-участников

68

выступающих с докладами

33

часа контента

50

тонн оборудования

57

городов



Регистрация
скоро откроется

#socforum

Гибкая система управления учетными записями

AK | Ankey IDM

- отечественная разработка
- контроль избыточных прав доступа сотрудников
- контроль учетных записей в российских приложениях и системах
- экономия до 40% времени IT-службы
- единый интерфейс контроля прав сотрудников для служб IT, ИБ, бизнес-пользователей
- техническая поддержка 24/7



Реклама 18+



8 (800) 101-71-00

www.gaz-is.ru

GIS

ГАЗИНФОРМ
СЕРВИС