



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАНКОВ

JOURNAL

№1 (40)

2021



16

Наталья КАСПЕРСКАЯ
АРПП «Отечественный софт»
5% против 95%

34

Анатолий АКСАКОВ
Государственная дума РФ
**Итоги 2020 года
вдохновляют**



68

Анастасия ХАРЫБИНА
AKTIV CONSULTING
Сомнения прочь!

82

Евгений НОВИКОВ
Министерство энергетики РФ
**Безопасность
ТЭК нуждается
в координации**

107

Марина БРОДСКАЯ
BIS Journal
**Онлайн по-русски
forever?**

ИМПОРТОЗАМЕЩЕНИЕ: SPLIT TIME



Проекты Медиа Группы «Авангард»

Онлайн и офлайн-мероприятия

Отраслевой журнал BIS Journal

Интернет-телекомпания BIS TV

Энциклопедия безопасника

ib-bank.ru



**Окупись в мир
информационной
безопасности!**



АВАНГАРД
медиа группа



Олег СЕДОВ

приглашённый редактор номера

ТЕМА ДЛЯ ГЕРОЕВ

«Импортозамещение: Split time» — слаломист на обложке и главная тема этого номера обозначили вектор азарта и точность границ. 2021–2024 — участок трассы, гонка внутри гонки, госпрограмма как вид спорта. Кто-то делает ставки, кто-то делает дело!

А впрочем... Шаг за шагом мы приближаемся к оценкам того, что назвали импортозамещением. Рано или поздно нам придётся ответить, насколько это нам удалось. Учитывая, что вовлечённых в этот процесс много, то и критерии успеха у каждого будут свои. Никто же не хочет оказаться за бортом успеха, а потому вовсе не очевидно, что риторика пафосных планов и амбиций импортопревосходства уступит место фактам, практикам и трезвым оценкам. Популизм всегда найдёт для себя лазейку, где-то между истинной и сомнениями. А потому, тот кто решается на откровенный разговор на тему импортозамещения — уже герой!

У вас в руках номер BIS Journal, который бесстрашно прогнул эти трудные вопросы на примере финансового сегмента.

Очень точно полярность взглядов на эти вопросы отметила в своей статье Елена Покатаева: «Что поможет сойти с иглы импортозависимости: кнут, пряник, выстрел в ногу?» Мы так увлеклись кнутами в виде проверок, отчётности и штрафов, что для нас пряник стал отложенным ожиданием кнута. Но Россия — страна крайностей: на войну с песнями, а под венец в слезах. Так что одним только выстрелом в ногу тут не обойтись. Живого места не останется! Хотя в отчётности все будет выглядеть нарядно. Но еще ни один отчёт не отразил реальной связки эффективности бизнеса с успехами импортозамещения.

Кроме того, у нас появилась нетронутая, но уже набившая оскомину тема — влияние пандемии на старые задачи и приоритеты. Мы еще не знаем, как, но понимаем, что прежнего мира уже не будет. Перемены происходят под действием внутренних или внешних факторов. Но тут влияние одновременно с обеих сторон. В результате, стёртые границы, вынужденно «временно» снятые запреты и ограничения... Все это меняет нас и окружающие нас условия.

В том числе и оказывает влияние на приоритеты импортозамещения. Как? А вот это уже тема для следующих откровений, которые потребуют не меньшей смелости!

ОБЩЕСТВЕННЫЙ РЕДАКЦИОННЫЙ СОВЕТ

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

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

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

ЭКСПЕРТНАЯ ГРУППА

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

РЕДАКЦИЯ ЖУРНАЛА

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

УЧРЕДИТЕЛЬ-ИЗДАТЕЛЬ

ООО «Медиа Групп» «Авангард»
 Адрес: 127473, Россия, Москва, 3-й Самотечный переулок, д.21
 Тел.: +7 499 271-70-85
 Интернет-версия: ib-bank.ru/bisjournal
 E-mail: bis@ib-bank.ru

Зарегистрирован 13 августа 2010 года Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзором).
 Свидетельство ПИ № ФС 77-61378 от 10 апреля 2015 г.

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

Подписан в печать 20.01.2021. Тираж 5000 экз.
 Заказ № 112021. Цена договорная. Отпечатан в типографии «Московский Печатный Двор», 123298, г. Москва, 3-я Хорошевская 18, корп. 1, офис 201А

© BIS Journal, 2021



НОВОСТИ

4 Законодательство, криминал

ТЕМА НОМЕРА ИМПОРТОЗАМЕЩЕНИЕ В БАНКАХ: 2021–2024

- 8 Елена Покатаева (BIS Journal)
Импортозамещение в банках: между «да» и «нет»
- 13 Тимур Аитов (Торгово-промышленная палата РФ)
Административное наказание против уголовного
- 16 Наталья Касперская (АРПП «Отечественный софт»)
5% против 95%
- 19 Николай Куликов (SMART technologies)
Эволюция против революции
- 21 Сергей Вихорев (ИТ-экспертиза)
Срединный путь против выстрела в ногу
- 23 Ренат Юсупов (Kraftway)
Внутренний нарушитель против внешнего
- 25 Павел Шуст (АЭД)
Карта «Мир» против западных конкурентов
- 26 Светлана Аппалонава (АПЭАП)
Мимикрия под отечественное против отечественного
- 29 Светлана Легостаева (Консорциум «Вычислительная техника»)
Пандемия против инерции
- 30 Григорий Сизоненко (Группа компаний ИВК)
Примеры против слов
- 31 Борис Иванов (Рикор)
Давайте вспомним про Египет
- 32 Сергей Нейгер (Перспективный мониторинг)
А есть ли проблема?

РЕГУЛЯТОРЫ

- 34 **Законотворчество**
Анатолий Аксаков (Государственная дума)
Добро пожаловать в новую — цифровую — финансовую реальность
- 38 **Обучение**
Вадим Уваров (Банк России)
Прицел обучения — практика

БАНКИ

- 40 **Вредные советы**
Екатерина Рачкова (Банк ВТБ)
Заставьте клиента поработать
- 42 **Технологии**
Илья Дружинин (Ассоциация ФинТех)
Без швов
- 45 **Экосистемы**
Кристина Лаврентьева (Сбербанк)
Новые инструменты

УГРОЗЫ И РЕШЕНИЯ

- 48 **Промышленность**
Гарда Технологии
Кибербезопасность промышленности
- 52 **Промышленность**
Марина Сорокина (ИнфоТеКС)
«Мы помогаем цифровому предприятию стать реальностью»
- 54 **Управление доступом**
Сергей Кузнецов (Thales)
В будущее — без паролей!
- 56 **Интервью**
Олег Иванов, Евгения Колодина (ГК «ЦИБИТ»)
От проблемы к точке роста
- 59 **Импортозамещение**
Корней Реут (BIS Journal)
UserGate. От партитуры к божественному звучанию

УГРОЗЫ И РЕШЕНИЯ

- 62 Киберучения**
Сергей Нейгер (Перспективный мониторинг)
Киберучения для обучения
- 64 Риски**
Екатерина Степанова (АМТ-ГРУП)
Управление рисками?
- 66 Пентест**
Валерий Филин, Павел Стеблянко (CITUM), Владимир Соловьев (ДиалогНаука)
Автоматизация пентеста — мировой тренд
- 68 Аудит**
Анастасия Харыбина, Павел Семёнов (AKTIV.CONSULTING)
Сомнения прочь!
- 72 Аутсорсинг**
Анна Михайлова (Группа компаний Angara)
Работаем вместе, работаем хорошо
- 74 Квантовая криптография**
Игорь Наливайко (Кванттелеком)
Бизнес-ветвь потомков Ландавшица

ИНФРАСТРУКТУРА

- 76 Деловые мероприятия**
Александр Бодрик (BIS Journal)
SOC-Форум Live 2020
- 79** Алексей Лукацкий (BIS Journal)
Скачок в сторону зрелости
- 82** Евгений Новиков (Министерство энергетики РФ)
Безопасность ТЭК — 2020
- 84** Валерий Куликов (BIS Journal)
The Standoff 2020
- 88 Электронная подпись**
Григорий Стрижаков, Вячеслав Чертков
Передача и передоверие

ИНФРАСТРУКТУРА

- 91 АСУ**
Валерий Хурматуллин (Радиотехнический институт им. академика А. И. Минца), Дмитрий Колесников (Сбербанк), Андрей Колесников (концерн «Автоматика»)
При объединении систем

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

- 94 Исследования**
Ольга Лимонова, Андрей Жаркевич (Антифишинг)
Мифы и легенды повышения осведомлённости
- 98 Обучение персонала**
Ольга Лимонова, Андрей Жаркевич (Антифишинг)
«Отделка щенка под капитана»

ОБРАЗОВАНИЕ И КАРЬЕРА

- 104 Международный обзор**
Марина Бродская (BIS Journal)
«Все на борьбу с неграмотностью!»
- 107 Обзор**
Марина Бродская (BIS Journal)
Онлайн по-русски
- 111 Обзор**
Марина Бродская (BIS Journal)
Туманный Лондон закрыл школы

СУБЪЕКТЫ

- 114 История**
Дмитрий Ларин (историк криптографии)
Север против юга
- 120 История**
Борис Столпаков (историк криптографии)
Перед закатом Империи

В УСКОРЕННОМ РЕЖИМЕ

Минцифры РФ предложило ускорить на год (до 2023-го) переход на российский софт для объектов КИИ. Соответствующие поправки в проект указа размещены на портале проектов нормативных правовых актов.

Проект от октября прошлого года предполагал, что субъектам КИИ до начала 2024 года необходимо будет осуществить переход на преимущественное использование российского ПО, а до начала 2025 года — на преимущественное использование оборудования российского производства.

В ведомстве пояснили, что сроки перехода скорректированы в результате доработки проекта указа и в соответствии с предложениями, поступившими в рамках проведения общественного обсуждения проекта, в том числе поступившей позиции о готовности российских разработчиков обеспечить отрасли экономики российскими решениями.



НАШЕЛ — УДАЛИЛ!

Госдума приняла в третьем чтении закон, обязывающий социальные сети с 1 февраля 2021 г. самостоятельно находить и удалять контент, содержащий призывы к экстремизму, явное неуважение к обществу и государству, детскую порнографию, пропаганду наркотиков и т.п.

Законом вводится понятие «социальная сеть» — интернет-ресурс, распространяющий информацию посредством создания персональных страниц. Полномочиями по ведению реестра социальных сетей предлагается наделить Роскомнадзор. После включения соцсети в реестр, ее владелец будет обязан обеспечить приведение правил соцсети в соответствие с законом. Если число пользователей соцсети в течение трех месяцев будет ниже 500 тыс. человек в сутки, то соцсети будут исключаться из реестра.

ПРЕДУСТАНОВКА РОССИЙСКОГО ПО ВСЁ БЛИЖЕ

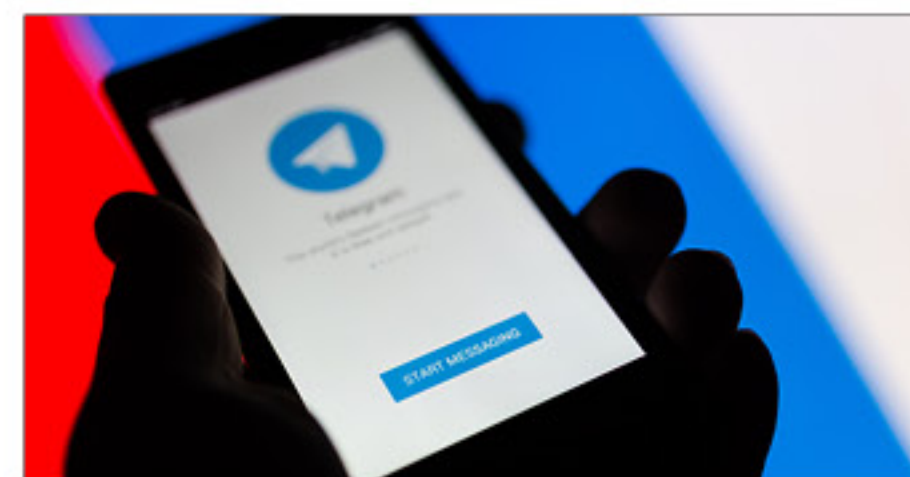
Государственная Дума приняла в первом чтении законопроект об административных штрафах до 200 тысяч рублей за продажу отдельных видов электронных устройств без предустановленных российских программ и приложений.

Согласно поправке в Кодекс об административных правонарушениях, «продажа отдельных видов технически сложных товаров с предварительно установленными программами для электронных вычислительных машин с нарушением установленного законодательством» требования о предварительной установке российских программ повлечет наложение административного штрафа на должностных лиц в размере от 30 тыс. до 50 тыс. рублей, на юридических лиц — от 50 тысяч до 200 тысяч рублей.

Сам закон о предустановке российского ПО был подписан президентом еще в 2019 году и должен был

вступить в силу с 1 июля 2020 года. Однако в марте планы поменялись и срок вступления закона перенесли на 1 января 2021 года. В начале декабря Госдума приняла закон, согласно которому еще на три месяца откладывается срок вступления в силу норм об обязательной предустановке российского ПО.

При этом Минцифры уже сформировало перечень российских приложений, которые рекомендованы для предустановки на электронные устройства. Среди них приложения Mail.ru Group и «Яндекса», «Госуслуги» и платежная система «Мир».



БИОМЕТРИЯ В ЗАКОНЕ

Государственная Дума приняла в третьем (окончательном) чтении закон об использовании Единой биометрической системы (ЕБС) для удаленной идентификации при получении широкого спектра финансовых и госуслуг.

Закон предоставляет кредитным организациям с базовой лицензией право собирать биометрические данные в ЕБС (сейчас закон обязывает их это делать) и вводит такую обязанность для банков с универсальной

лицензией. Последние должны будут дать возможность клиентам-физлицам открывать счета (вклады) в рублях и получать кредиты в рублях без личного присутствия после идентификации клиента.

Банк России получает право устанавливать условия сбора биометрии в зависимости от видов банковских подразделений. Закрепляется и право регулятора на срок до года вводить запрет на проведение идентификации в случае неоднократного нарушения требований «антиотмывочно-го» законодательства.

Кроме того, документ предусматривает сбор биометрии через МФЦ и возможность оказания госорганами таких услуг только с использованием ЕБС. При этом ЕБС получит статус государственной информационной системы.

Закон вступит в силу уже с 1 января — за исключением положений, для которых настоящей статьей установлены иные сроки вступления их в силу.



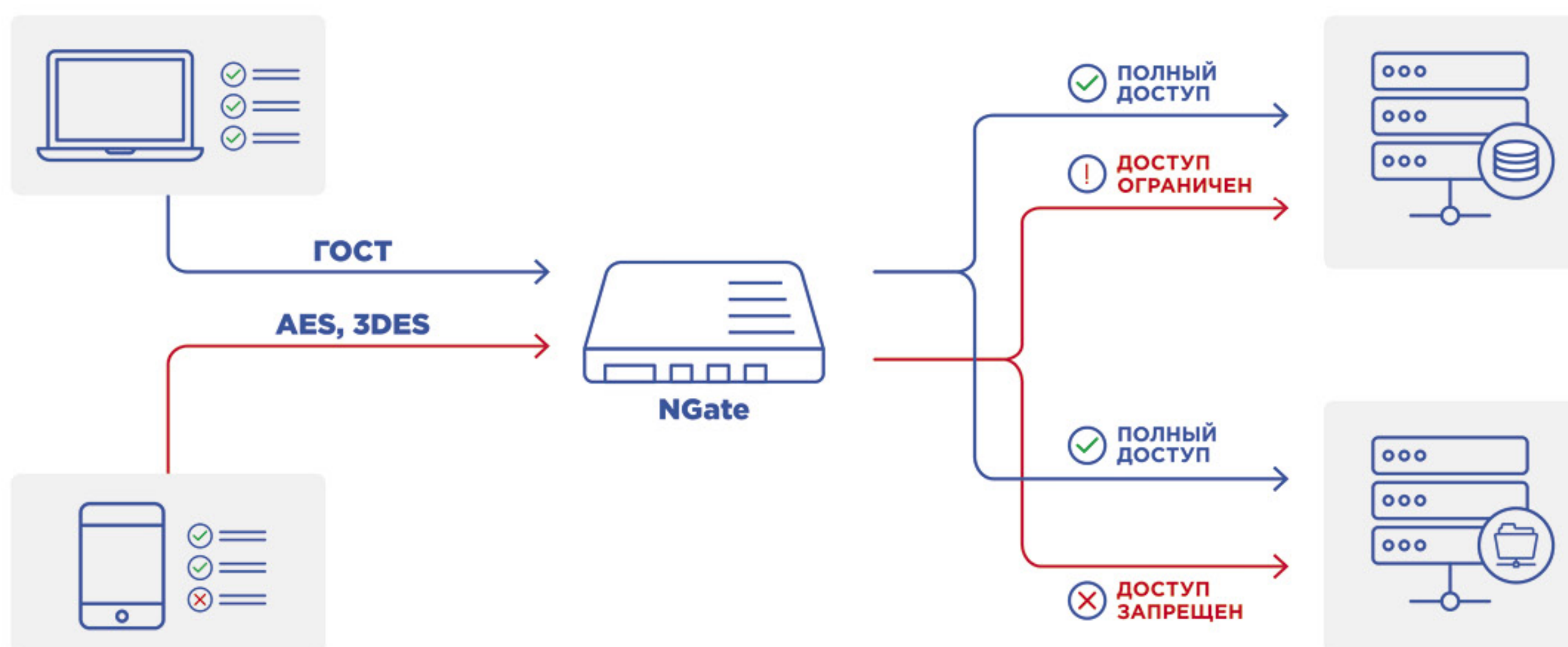


КриптоПро NGate — это универсальное высокопроизводительное средство криптографической защиты сетевого трафика, объединяющее в себе функционал:

TLS-сервера доступа
к веб-сайтам

Сервера портального
доступа

VPN-сервера



NGate обладает широкими возможностями по управлению доступом удалённых пользователей к ресурсам организации, а также обеспечивает снятие с веб-серверов нагрузки по обработке TLS-соединений и исключает необходимость проведения исследований по оценке влияния. NGate реализует российские криптографические алгоритмы, имеет сертификаты ФСБ России и может использоваться для криптографической защиты конфиденциальной информации, в том числе персональных данных, в соответствии с требованиями законодательства РФ.

NGate может быть особенно полезен следующим типам организаций:

- Субъекты критической информационной инфраструктуры;
- Государственные и муниципальные органы и государственные организации;
- Операторы персональных данных;
- Банки и другие организации финансового сектора;
- Иные организации, которым необходимо обеспечить защиту передаваемой информации и удаленного доступа.

Примерами объектов, доступ к которым можно защитить с помощью NGate, являются:

- Публичные веб-сайты, в том числе государственные порталы, электронные торговые площадки, веб-сайты организаций, ДБО и т.д.;
- Внутренние ресурсы и информационные системы организаций;
- Средства объектов (в том числе значимых) КИИ;
- Единая биометрическая система;
- Облачные ресурсы и информационные системы;
- Системы видеоконференцсвязи;
- Платформы телемедицины.



КРУПНАЯ РЫБА ИЗ ДАРКНЕТА

Немецкие правоохранители сообщили об отключении «вероятно, крупнейшего нелегального рынка в даркнете» под названием DarkMarket и аресте гражданина Австралии, предположительно управлявшего им.

По информации от властей, на площадке продавались запрещённые вещества, фальшивые деньги, краденые данные кредитных карт, анонимные SIM-карты и вредоносы.

DarkMarket насчитывал полмиллиона пользователей (включая более чем 2400 продавцов), а его заработки достигали 170 млн долларов.

ПОД ПОДПISКУ О НЕВЫЕЗДЕ

Москвич похитил свыше миллиона рублей дистанционно. Он работал в компании по обслуживанию электронных платежей.

У мужчины имелся доступ к электронным базам данных, где он обнаружил «спящие» электронные кошельки. Следствие полагает, что фигурант переписал платежные пароли клиентов и в нерабочее время удалённо переводил их денежные средства на свой счёт; далее обналичивал (за 15 дней — более 270 переводов).

Следователем возбуждено уголовное дело по признакам преступления, предусмотренного статьёй 158 УК РФ («Кража»). Основанием послужило заявление о хищении денежных средств, поданное представителем компании, где работал подозреваемый.

На сегодняшний день злоумышленнику избрана мера пресечения в виде подписки о невыезде. Предварительное расследование продолжается.

РОКОВЫЕ 20 ДОЛЛАРОВ

Россиянин Кирилл Фирсов признал себя виновным в киберпреступлениях в США. Ему назначено тюремное заключение сроком до десяти лет и штраф в размере до 250 тысяч долларов.

Фигурант был администратором площадки deer.io, где продавались краденые данные кредитных карт и другие персональные данные. Фирсов торговал номерами соцстрахования, датами рождения и адресами американских граждан.

Судя по материалам дела, сайт функционировал с 2013 по 2020 год, а его доход составил 17 млн долларов.

По большей части его жертвами были россияне, но около 1,2 млн долларов удалось заработать на продаже информации о гражданах США, что и позволило ФБР задержать Фирсова по приезду в страну. За три дня до этого ведомство осуществило «контрольную закупку» у него на сайте — приобрело информацию о 1100 геймерах за 20 долларов в биткоинах.



«ЗАКРЕПИЛАСЬ» НА НОВОМ МЕСТЕ

Советский районный суд Волгограда рассмотрит уголовное дело в отношении сотрудницы мобильного оператора. Она обвиняется в незаконном использовании сведений, составляющих коммерческую тайну.

Фигурантка работала в компании менеджером активных продаж. В ноябре прошлого года она перешла работать в конкурирующую организацию. Имея логин и пароль для доступа к информресурсам с прошлого места работы,

обвиняемая скачала на чужой компьютер данные 164 абонентов сотовой связи — для увеличения объёмов продаж на новом месте.

Женщина обвиняется в неправомерном доступе к охраняемой компьютерной информации (ч.2 ст. 274.1 УК РФ) и в незаконном получении и разглашении сведений, составляющих коммерческую, налоговую или банковскую тайну (ч.3 ст. 183 УК РФ).



ЛУЧШИЕ В РОССИИ - 2020

В Москве прошла церемония награждения лауреатов национальной премии «Лучшие в России 2020». Подводились итоги сразу в трех категориях - «Компания года», «Персона года» и «Финансовый Олимп». Организатор премии - новостной портал Anews.

Заслуженные награды и признание профессионалов получили:

ПЕРСОНА ГОДА 2020

Финансист. Медийная персона года - Евгений Коган, президент инвестиционной группы «Московские партнеры».

Управленец - Александр Гинцбург, директор НИЦЭМ им. Н. Ф. Гамалеи.

Топ-менеджер - внедрение цифровых технологий в страховой отрасли - Ольга Сорокина, заместитель генерального директора по развитию бизнеса Страхового Дома ВСК.

КОМПАНИЯ ГОДА 2020

ПАО «Татнефть», ЗАО «Трансмашхолдинг», ИК «БКС Мир инвестиций», Страховой Дом ВСК, АО «НПФ Эволюция», АО «Почта Банк», Система быстрых платежей от ЦБ РФ, БК «Лига Ставок», Высшая школа управления финансами, NAVIEN, AMF - международная сеть доставки цветов и многие другие.



Александр Тарновский, генеральный директор Страхового Дома ВСК



Ольга Журавская, первый вице-президент БК «Лига Ставок», учредитель Благотворительного фонда «Созвездие Добра»



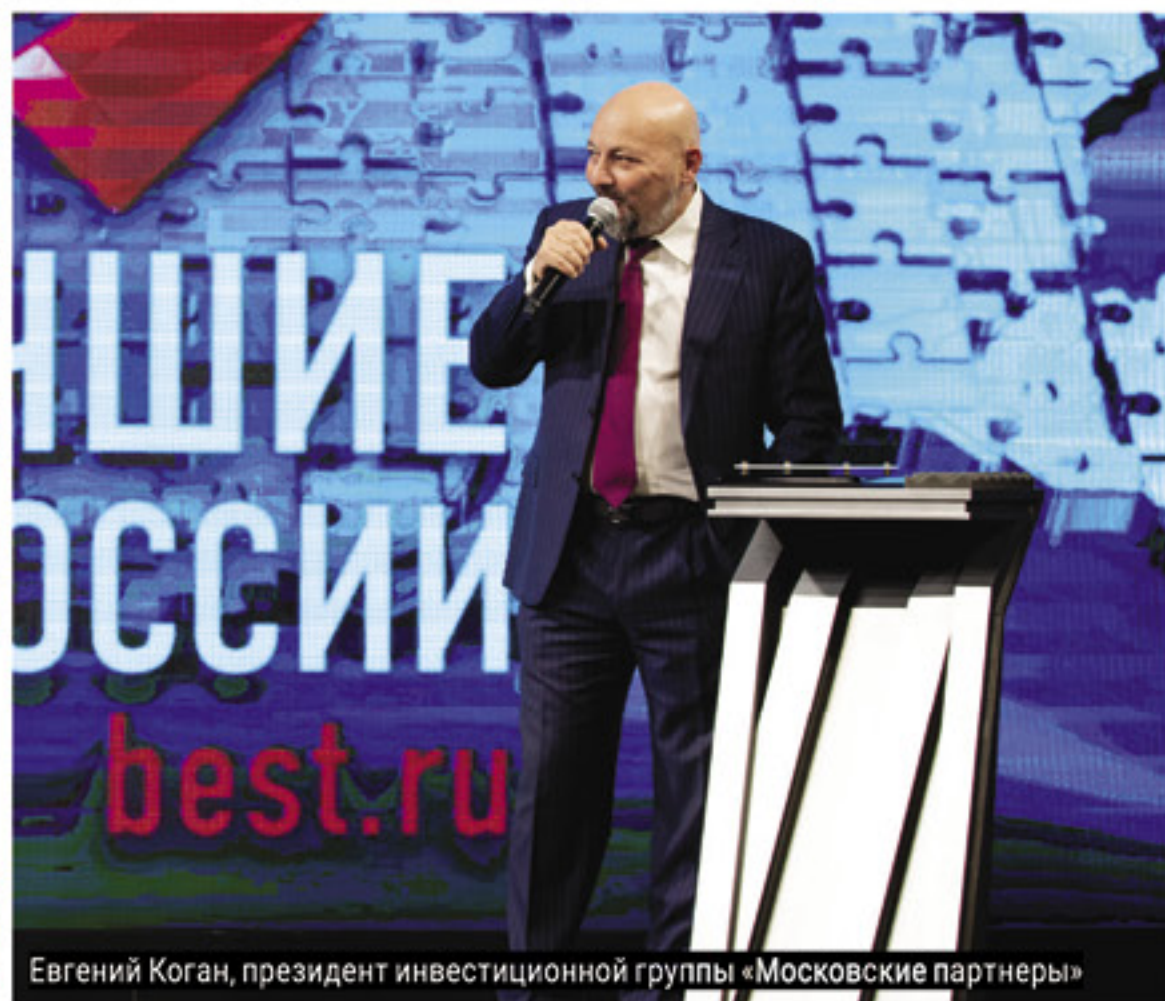
Андрей Языков, генеральный директор АО «НПФ ЭВОЛЮЦИЯ»



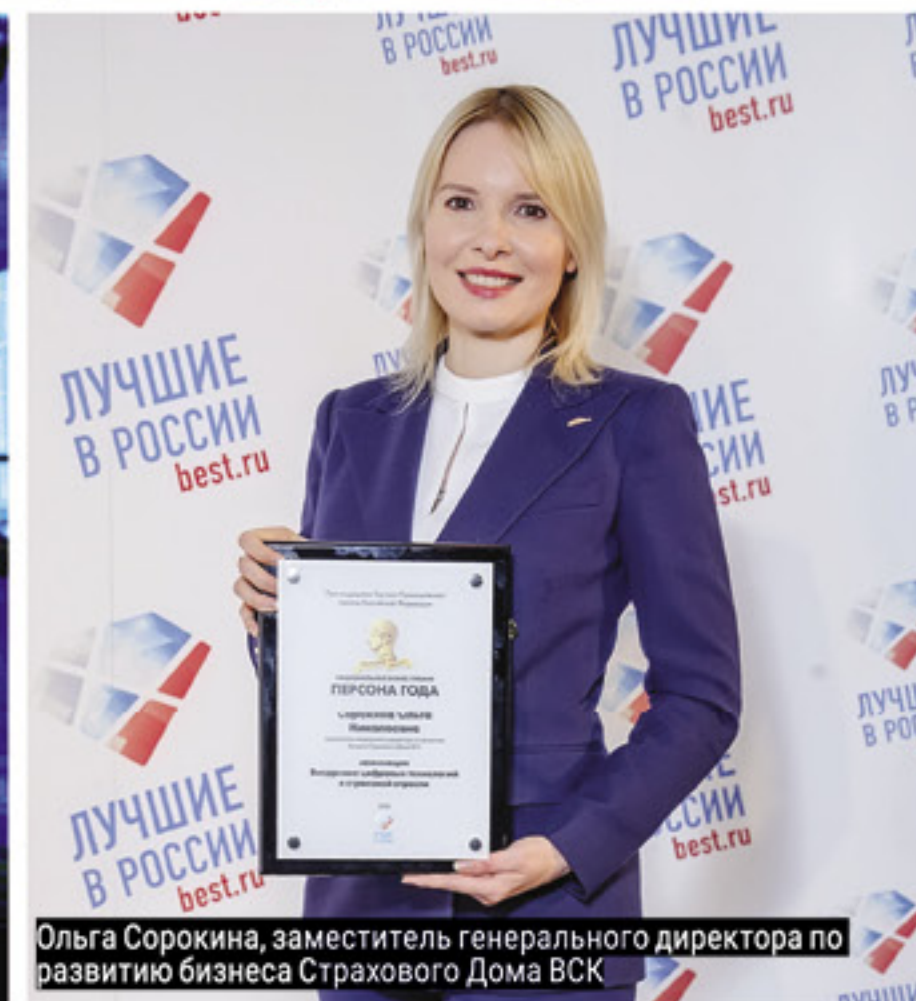
Никита Голубев, директор по маркетингу компании Навиен



Олег Чихладзе, директор по брокерскому бизнесу «БКС Мир инвестиций»



Евгений Коган, президент инвестиционной группы «Московские партнеры»



Ольга Сорокина, заместитель генерального директора по развитию бизнеса Страхового Дома ВСК

ИМПОРТОЗАМЕЩЕНИЕ В БАНКАХ: МЕЖДУ «ДА» И «НЕТ»

ЧТО ПОМОЖЕТ СОЙТИ С ИГЛЫ ИМПОРТОЗАВИСИМОСТИ:
КНУТ, ПРЯНИК, ВЫСТРЕЛ В НОГУ?

Тема импортозамещения ИТ-оборудования и программного обеспечения всё прочнее обосновывается в верхних строках бизнес-новостей, и всё чётче проявляется сопротивление навязываемой государством стратегии со стороны отраслей.

Так, банковскому сектору удалось добиться сдвига даты перехода на преимущественное использование отечественных программных и аппаратных продуктов с начала 2022 года на 1 января 2024 года для программного обеспечения и на 1 января 2025 года — для оборудования. Однако даже эти сроки в Ассоциации банков «Россия» считают слишком жёсткими и ссылаются на собственные расчёты, которые говорят о значительном сокращении капитала банков в случае исполнения требований государства. По оценкам ассоциации, доля используемого иностранного ПО и ИТ-оборудования в отрасли составляет сегодня в среднем 85 %, затраты на реализацию

требований государства превысят 700 млрд руб., что составляет 5–7 % всех денежных средств отрасли. Это значит, делают выводы эксперты банковской ассоциации, что из объёма кредитования отрасли будет изъято 5–7 трлн руб., и это, безусловно, негативно отразится на экономике страны.

Иными словами, банки говорят о такой высокой стоимости миграции ИТ-инфраструктуры на отечественные продукты, которая приведёт к недофинансированию реального сектора отечественной экономики. В то же время ИТ-сообщество уверено, что если процесс по выходу из технологической зависимости будет отложен, то в технологической зависимости от зарубежных вендоров окажется не только отрасль ИТ, но и экономика страны, а также система государственного управления. С этой своей «болью» авторитетные ИТ-лидеры также обращаются к государству. Кто прав в этом споре?



**Елена
ПОКАТАЕВА**
специальный
корреспондент
BIS Journal

РЕАЛЬНАЯ КАРТИНА

Следует отметить, что в числе «диссидентов» импортозамещения не только банкиры. В 2020 г. должна была завершиться программа импортозамещения ПО в государственном секторе. Однако согласно данным исследования, которое провела в конце прошлого года компания «СерчИнформ», почти половина госзаказчиков (47 %) признали, что ещё не приступили к импортозамещению. И только 13 % таких структур сообщили о замещении большей части ИТ-инфраструктуры. В коммерческом секторе только для трети опрошенных компаний актуален вопрос импортозамещения, и это крупные организации с госучастием. Из них 43 % ещё ничего не замещали, а активно процесс идёт у половины опрошенных. Таким образом, за первоначально установленными сроками в рамках импортозамещения успевает только каждая

десятая компания, делают вывод исследователи «СерчИнформ» (рис. 1).

Примечательно, что, согласно данным исследования, коммерческий сектор не только не отстаёт, но даже несколько опережает госсектор по результативности соответствующих мероприятий. Это сигнализирует не столько об отсутствии у организаций желания заменять импортные ИТ-решения отечественными, сколько о наличии системных проблем в самой сфере импортозамещения в сфере ИТ.

«СДВИГОВ ВПРАВО БОЛЬШЕ НЕ БУДЕТ»

Эти проблемы известны государству, и в законодательной сфере идёт активная работа по двум направлениям: дальнейшее усиление импорто-независимости для объектов критической информационной инфраструктуры (КИИ), в числе которых — банки, и поддержка отечественных

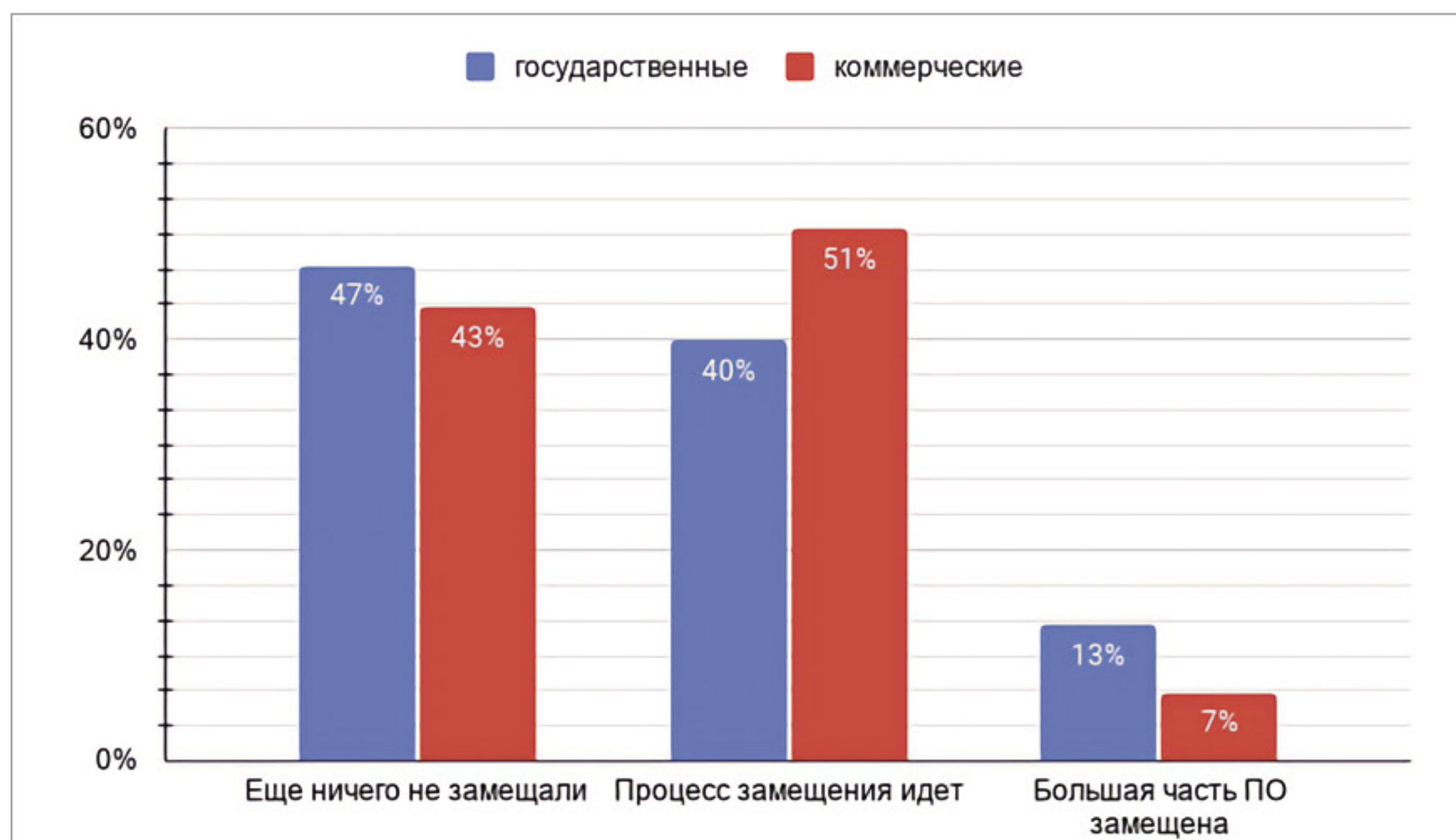


Рисунок 1. Уровень импортозамещения ПО в российских компаниях. Источник: Исследование импортозамещения ПО в госсекторе, «СерчИнформ», сентябрь–ноябрь 2020 г.

производителей радиоэлектронной продукции и микроэлектроники. Оба этих направления развиваются согласованно. И, принимая во внимание текущий уровень импортозамещения, а также наличие объективных тормозящих проблем, 2024 год выглядит приемлемой датой, к которой должны быть завершены основные мероприятия по перестройке сквозных рыночных процессов (разработка — продажа — внедрение) в сторону импортонезависимых ИТ-решений.

«Все банки мы в любом случае переведем на отечественное программное обеспечение. Они в этом смысле подчиняются регулятору, соответствующие решения приняты», — рассказал BIS Journal Василий Шпак, директор департамента радиоэлектронной промышленности Минпромторга России, и пояснил: «Они хлопотали, чтобы сроки были перенесены вправо по оси времени. Но я уверен, что сдвигов вправо больше не будет». При этом директор ДРЭП Минпромторга России не исключил, что «наши зарубежные партнёры эту точку могут подвинуть влево, в сторону сокращения сроков».

МИФЫ И РЕАЛЬНОСТЬ ГЕОПОЛИТИЧЕСКИХ УГРОЗ

В середине января Министерство торговли США выпустило внутреннее постановление, в котором признало враждебными правительства России, Китая, Ирана, КНДР, Кубы, а также венесуэльского лидера Николаса Мадуро. Постановление позволяет американскому Минторгу ужесточить контроль за сделками в сфере информационных технологий.

А несколько раньше появился доклад американского же Центра стратегических и международных исследований, в котором обосновывается необходимость серьёзного изменения стратегии США в отношениях с Китаем и Россией командой нового президента этой страны. Комментируя новые варианты поведения в отношении России, Александр Лосев, член президиума Совета по внешней и оборонной политике, отмечает, что американские стратеги ставят задачу всемерного ослабления России за счёт создания такой конкурентной среды, в которой Российская Федерация не только не сможет развиваться, но и будет происходить ухудшение экономического состояния страны.

Такую стратегию Александр Лосев характеризует как войну на уровне чуть ниже настоящей большой войны, а её инструментами станут экономические санкции, информационные войны, кибервойны и кибердиверсии, вплоть до ограниченных военных действий не на территории США.

Радикальное ослабление России за счёт кибервойн и кибердиверсий — это уже далеко за пределами отказа в официальной поддержке ИТ-продукта, что сегодня считается наибольшим геополитическим риском в ИТ-сфере.

ИЗМЕНЕНИЯ В СТРАТЕГИИ ИМПОРТОЗАМЕЩЕНИЯ

Василий Шпак утверждает, что правительство РФ, понимая эти риски, готовит серьёзные изменения в стратегии и практике импортозамещения в сфере ИТ. Планируется, что они будут объявлены в начале года. Не раскрывая деталей

Рисунок 2.
Кажущийся
и возможный сценарии
импортозамещения.
Источник: АНО
«Цифровая экономика»,
июль 2020 г.

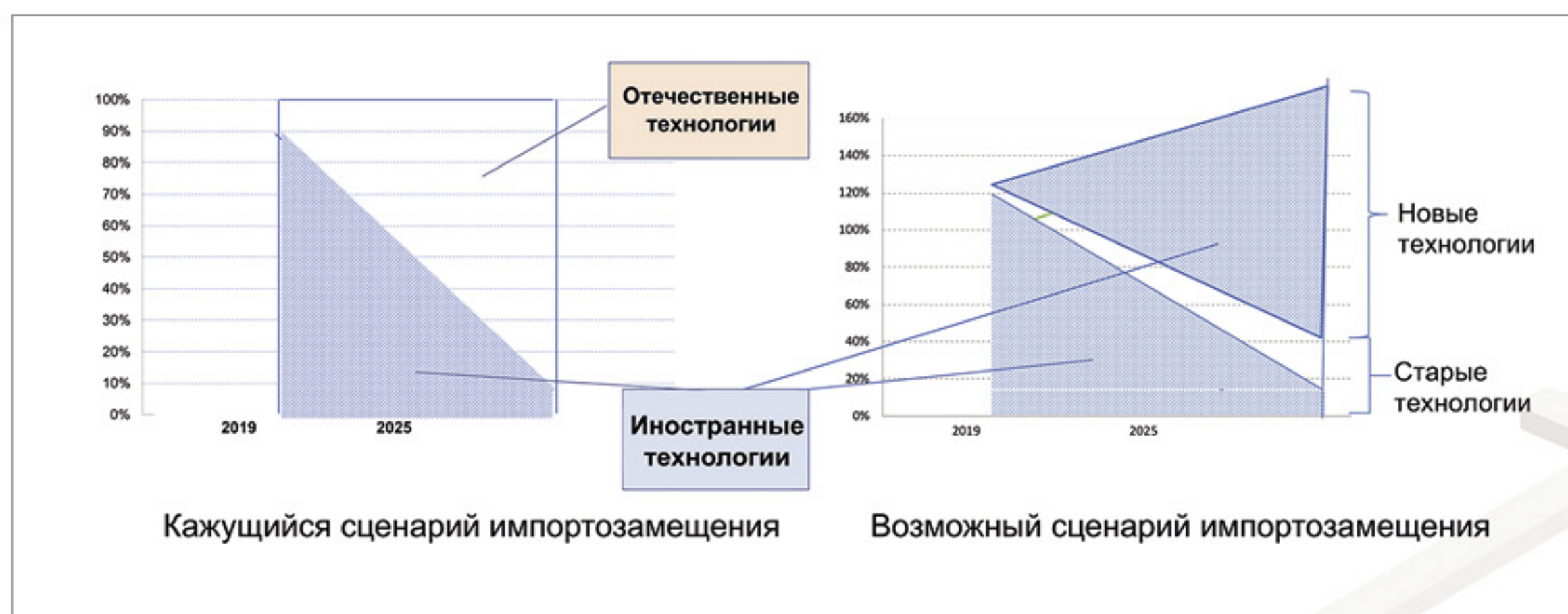
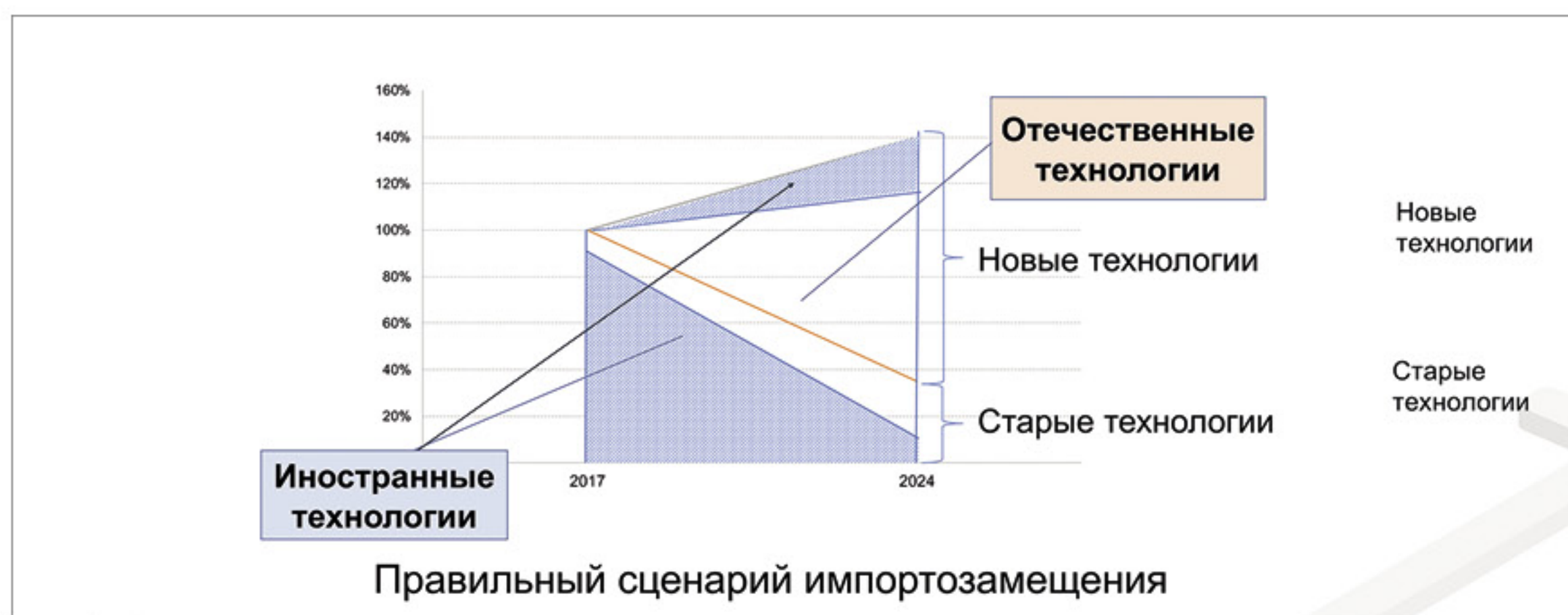


Рисунок 3.
Правильный сценарий
импортозамещения.
Источник: АНО
«Цифровая экономика»,
июль 2020 г.



того, что ещё не объявлено, Шпак отмечает, что речь идёт о том, что вместо нынешнего запрета закупок в 2024 г. будет введён запрет использования зарубежной ИТ-продукции. Он подчёркивает, что новые правила лишат смысла попытки некоторых крупных заказчиков закупить зарубежных продуктов на несколько лет вперёд.

Если так, то предстоящая «трёхлетка» потребует реальных действий от компаний, относящихся к сфере КИИ, в том числе банков. Причём объём поставленных масштабных задач потребует достаточно серьёзных усилий со стороны как игроков ИТ-рынка, так и российских предприятий, а также со стороны регулятора. При этом главным вызовом становятся системные целенаправленные действия при активной роли государства.

СЦЕНАРИЕВ ИМПОРТОЗАМЕЩЕНИЯ НЕМНОГО

Как отмечает Николай Зубарев, директор по направлению информационной безопасности АНО «Цифровая экономика», на практике могут реализоваться различные сценарии импортозамещения в сфере ИТ, в том числе весьма опасный, при котором отечественные вендоры без поддержки со стороны государства не смогут

победить в конкурентной борьбе зарубежных производителей и занять собственный российский рынок (рис. 2).

Главная причина — в низком текущем уровне проникновения отечественных ИТ-технологий. По оценкам АНО «Цифровая экономика», в прикладном ПО этот уровень варьируется от 15 до 60% в отдельных областях, в области информационной безопасности — от 40 до 90%, а в платформенных решениях составляет менее 5%. А ведь именно платформы — это сегодня ключевой элемент, становой хребет экосистемы цифровой экономики, которая создаётся в передовых странах мира.

Фактически платформа — «хозяин» цифровой экосистемы, и тот, кто владеет платформой, владеет, по сути, цифровой экономикой страны. Очевидно, говорит Николай Зубарев, что экосистема цифровой экономики должна базироваться на отечественных платформах (рис. 3).

Однако для того, чтобы осуществить технологическую трансформацию требуемого масштаба в банковском секторе, всем участникам преобразований — банкам, ИТ-производителям и государству — необходимо найти чёткие и правильные ответы на ряд вопросов по различным аспектам импортозамещения.

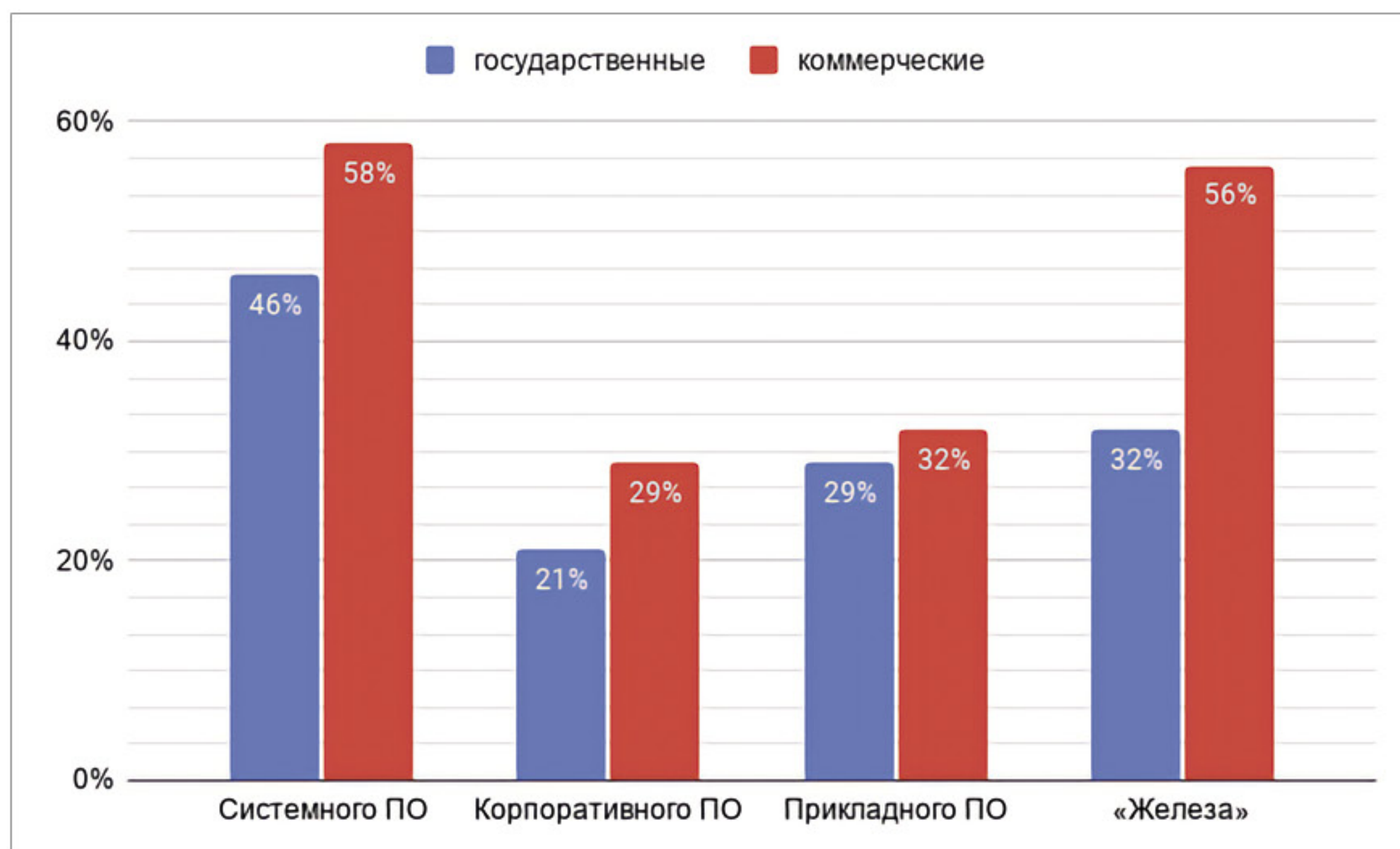


Рисунок 4. Труднее всего даётся импортозамещение...
Источник: Исследование импортозамещения ПО в госсекторе, «СерчИнформ», сентябрь–ноябрь 2020 г.

АСПЕКТ 1. БАНКОВСКАЯ СПЕЦИФИКА

Импортозамещение в банковской сфере имеет существенную специфику, которая, в числе прочего, обусловлена двойной ролью банков в экономических процессах страны. С одной стороны, это коммерческие организации, зарабатывающие деньги и вовлечённые в глобальные финансовые процессы. С другой — банки выполняют важную роль финансирования реального сектора экономики РФ. Такая двойная ответственность диктует особые отношения между банковскими структурами и государством в вопросах импортозамещения. Какой тип регулирования со стороны государства обеспечит банкам условия для реального, а не «бумажного» импортозамещения? Какую роль в этих процессах должны играть профессиональные сообщества, как банковские, так и ИТ-компаний?

АСПЕКТ 2. ЭФФЕКТИВНОСТЬ ОТЕЧЕСТВЕННЫХ ИТ-РАЗРАБОТЧИКОВ

Согласно данным исследования компании «СерчИнформ», сложнее всего поддаётся импортозамещению системное ПО: операционные системы, СУБД (рис. 4). «Быстро это не сделаешь — потребуются годы на отладку, доработку и интеграцию ПО в крупные компании», — комментирует Алексей Парфентьев, руководитель отдела аналитики компании «СерчИнформ», и замечает далее: «Переход на отечественное оборудование на деле вообще не стартовал, так как

базового железа (процессоров, жёстких дисков, плат и чипсетов) в промышленных масштабах пока не производится».

Исходя из того, что на настоящий момент не все компоненты ИТ-инфраструктуры банков имеют стопроцентный российский аналог, импортозамещение представляет собой не разовую акцию, а эволюционный процесс, развивающийся во времени. Управление такими процессами обычно осуществляется на основе дорожных карт. Кто должен заняться созданием дорожной карты импортозамещения в банковском секторе? Если это коллективное творчество ИТ-сообщества и банковских специалистов, то кто должен в конечном счёте нести ответственность за исполнение мероприятий отраслевой дорожной карты: ведомство, отвечающее за хайтек-технологии, или финансовый регулятор? И кто оплатит весь этот «пир творчества»? Тем более что этих решений должно быть немало, они должны конкурировать между собой.

АСПЕКТ 3. ЭФФЕКТИВНОСТЬ ВЗАИМОДЕЙСТВИЯ ПОСТАВЩИКОВ ИТ-РЕШЕНИЙ И БАНКОВ

Во время презентации стратегии развития электронной промышленности летом 2019 г. Василий Шпак сообщил, что одной из форм развития электронной промышленности является создание консорциумов. Это движение только началось: в течение всего 2020 года создавались новые консорциумы, которые объединяют производителей и поставщиков той или иной продукции, например вычислительной

техники или телекоммуникационного оборудования, они подписывали партнёрские соглашения друг с другом и с регуляторами в лице Минпромторга и Минцифры. Но как их «цеховые» интересы эффективно согласовать с «интересами» представителей банковского сектора?

А ведь, по сути, поставлена весьма амбициозная задача — создать практически с нуля целую отрасль со сформированными и отлаженными бизнес-цепочками производителей, интеграторов и заказчиков отечественной электроники и программных средств. Причём создаваться эта отрасль должна в условиях жёсткой конкуренции с зарубежными поставщиками, отчаянно стремящимися сохранить свои доли российского рынка. В этой конкуренции — в буквальном смысле не на жизнь, а на смерть — главная регулирующая роль отводится реестрам отечественной продукции и квотам при закупках.

Критерии определения отечественной продукции по-прежнему далеки от идеальных. Не прекращаются скандалы с появлением в реестрах продукции из разряда «переклейки шильдиков». Летом прошлого года Юрий Борисов, заместитель Председателя Правительства РФ, дал поручение подготовить изменения в ФЗ-488 «О промышленной политике» — ввести понятия «промышленная продукция российского происхождения» и «российский производитель». Но эти важные изменения пока ещё не получили законной силы.

Однако наличие продукции в реестре должно быть не конечной точкой рыночной активности разработчиков, а, наоборот, отправным пунктом для старта главных мероприятий — модернизации ИТ-инфраструктуры и ИТ-систем заказчиков. Как сделать так, чтобы реестры отечественной продукции стали эффективным инструментом для создания нужных заказчикам ИТ-решений на базе отечественной продукции?

ВОПРОСЫ РАЗУМНОГО ГОСУДАРСТВЕННОГО ПРОТЕКЦИОНИЗМА

В отсутствие реальных стимулов для импортозамещения государству приходится выступать с позиции силы, принуждать отрасли к импортозамещению. Можно ли создать такое регулирование, при котором банкам станет «интересно» переходить на отечественную продукцию? Похоже, вопрос заключается в создании типовых протестированных ИТ-решений, которым банки могут доверять в ходе модернизации своей инфраструктуры. Это позволит реально оценивать сроки перехода на отечественную продукцию, стоимость такого перехода, а также соотношение отечественного/зарубежного. Но кто должен заниматься созданием таких решений? Государство? Отраслевые ассоциации? Совместные коллективы компаний-интеграторов и разработчиков? Кто сформулирует правильную постановку задачи? Сами банки? Банковские интеграторы?

И те, и другие работают в высококонкурентной среде, где знание актуальных потребностей заказчика — сильнейшее конкурентное преимущество, а значит, предмет коммерческой тайны.

Пожалуй, тут должны работать механизмы поощрения. «Будет не только кнут, но и пряник», — обещает Василий Шпак. Напрашивается тезис о том, что господдержка должна распространяться не только на отечественных разработчиков, но и на их клиентов из банковского сектора. На первый взгляд, звучит парадоксально. Но поддержка со стороны государства не обязательно должна иметь буквальное денежное воплощение. Например, речь может идти о коррекции маршрутов денежных потоков: вместо заграничного «пузыря» типа Tesla финансирование направляется на инвестирование российских производителей. Тогда задачей государства становится организация такого регулирования хайтек-рынка РФ, при котором банки получают не меньшую отдачу, чем от инвестиций в зарубежные компании.

Задачи такого уровня в постсоветской России до сих пор не решались. Но время пришло — геополитические тренды не оставляют большого пространства для выбора альтернатив. И это время настоящего диалога бизнеса и госвласти: не в интересах лоббирования коммерческих интересов влиятельных бизнес-структур, а в интересах модернизации экономики страны на основе отечественного хайтека. Это означает, что к реализации стратегии импортозамещения должны активно подключаться экспертные сообщества, работающие вместе с государством во имя реализации технологической импортонезависимости.

Редакция BIS Journal организовала виртуальный «мозговой штурм» и расспросила российских экспертов: что определяет суть нынешней ситуации с импортозамещением в банковской сфере, где скрываются главные проблемы и каким образом их нужно разрешать?

Картина получилась мощной, многослойной и заполнилась собой «пространство концепции» практически полностью. Каждое из мнений содержит ценное открытие, угол зрения, неожиданную информацию или предложение.

АДМИНИСТРАТИВНОЕ НАКАЗАНИЕ ПРОТИВ УГОЛОВНОГО

«АКЦЕНТ ДОЛЖЕН ДЕЛАТЬСЯ
НЕ НА ПРИНУЖДЕНИЕ ПОКУПАТЕЛЕЙ,
А НА ОРГАНИЗАЦИЮ СИСТЕМНОЙ РАБОТЫ»



Тимур АИТОВ
заместитель
председателя
комиссии
по цифровым
финансовым
технологиям
Торгово-
промышленной
палаты РФ

Цифры, которые приводят банкиры, описывая долю используемого иностранного ПО и ИТ-оборудования в отрасли, значительные, но они похожи на истину. Например, анализ проекта по импортозамещению в одном из банков топ-5 показал, что на переход потребуется около 10 млрд рублей. Причём это не все расходы, а только те, что касаются замены ПО. В пересчёте на всю банковскую систему России, возможно, понадобится 700 млрд рублей... Но кто знает, сколько банков останется в строю в ближайшей перспективе? Четверть существующих банков закончит 2020 год без прибыли, и этот тренд, увы, в нынешнем году сохранится. Поэтому точной цифры затрат на замену всего ПО в отрасли не знает никто. Ещё следует помнить, что при трансформации ИТ-ландшафта обязательно сработает известное правило бизнеса: любой новый проект требует ровно в два раза больше инвестиций, чем было получено заранее в ходе предварительной разумной оценки. Это, конечно, шутка, но в ней много правды.

Думаю, неверно утверждать, что банки принципиально не заинтересованы переходить на российское ПО. Они и сегодня не против отечественной продукции и, в общем-то, готовы отказаться от использования продуктов западных производителей. Проблема в другом — переходить им не на что. Что говорят во многих крупных банках после анализа проблемы? На российском ИТ-рынке сегодня отсутствуют продукты необходимой функциональности и должного качества. И здесь дело даже не в масштабе процессов и сложности задач банковского «крупняка».

Замена ПО — это комплексная задача. Существует много разных видов этого ПО. А если меняешь операционную систему, то

зачастую приходится менять и всё остальное, что под ней работает. Менять приходится не только мощные СУБД. Меняются многочисленные прикладные программы, системы безопасности и прочее. Напомню, что даже драйверы принтера — атрибуты универсальной ОС. «Кусочками» на мировом рынке давно ничего не продаётся, вместо этого предлагается вертикально-интегрированное ПО — целая экосистема ПО, как модно сейчас говорить. Вся эта экосистема ПО работает как единое целое как раз под управлением данной конкретной ОС. И вот этих бизнес-экосистем ПО у нас не хватает для реализации полноценного импортозамещения.

Конечно, выпускать их должны сами игроки рынка, а ориентиром для них должен быть спрос. Но есть проблема. Россия с точки зрения масштабов производства небольшая — нас 140 млн человек. А экономика ИТ-производства говорит, что производить полную линейку продуктов — вот эту всю экосистему — в отдельно взятой стране рентабельно в том случае, если население этого региона окажется раз в пять больше. Иными словами, для рыночного успеха производства ПО надо иметь порядка полу-миллиарда жителей. В ином случае комплексные проекты масштаба страны чаще всего оказываются невыгодными национальному бизнесу, потому что они не могут отбить затраты. Приведу похожий пример из другой области: для производства электромобиля в России нужны

Экономика ИТ-производства говорит, что производить полную линейку продуктов — вот эту всю экосистему — в отдельно взятой стране рентабельно в том случае, если население этого региона окажется раз в пять больше

огромные средства. Их тоже нужно отбить, поэтому нынешние планы по созданию электромобиля неминуемо потребовали госдотаций.

Нашим ИТ-компаниям тоже обязательно нужна финансовая помощь для разработки отечественных экосистем ПО. При этом государство должно выступать заказчиком — тогда дело сдвинется. Но это ещё не всё. Для успеха придётся срочно сменить существующие акценты в импортозамещении. Основной акцент должен делаться не на принуждение покупателей, а на организацию системной работы (которой сегодня нет) и на координацию и стимулирование производителей.

К примеру, существуют многочисленные директивы, обязывающие компании перейти на российское ПО и оборудование в сжатые сроки, — игроки про них знают, но все эти директивы зачастую слабо соотносятся с реальным положением дел на рынке, а также возможностями производителей. Как следствие, сроки выполнения переходов постоянно переносятся, и это справедливо не только в отношении банковского ПО. Свежий пример — в части оборудования для организации связи 5G, здесь тоже выпущена директива со своими сроками. Что оказалось при изучении вопроса? На рынке всего две (!) компании, которые выпускают телекоммуникационное оборудование российского производства (ТОРП), удовлетворяющее требованиям чиновников. Но двух компаний явно недостаточно для удовлетворения рыночного спроса!

К тому же государство всё никак не решит известную юридическую проблему, которая сильно мешает госкомпаниям, работающим по 223-ФЗ, закупать отечественные ИТ-продукты. Если говорить упрощённо, то 223-ФЗ предписывает покупать то, что «дешевле», а такая характеристика, как «отечественность» может применяться только «при прочих равных». Более того, даже в конкурсных требованиях нельзя написать, что решение должно быть отечественным, так как с точки зрения 223-ФЗ это будет рассматриваться как дискриминация. А теперь почувствуйте разницу: наказание руководителя компании за невыполнение директив — это максимум уменьшение размера годовой премии, а наказание за невыполнение 223-ФЗ — вплоть до уголовной ответственности.

Важность системной работы по переводу на отечественное понятна. Но как правильно её организовать? Кто-то должен серьёзно заниматься координацией активности игроков рынка и расстановкой приоритетов развития. Однако сегодня одно министерство мониторит ситуацию, другое смотрит за горизонт, а должной

координации активности игроков нет. Рынок, увы, сам по себе ничего не выправляет, и ситуация не меняется. Как следствие такого положения дел идёт дублирование разработок ПО, распыление средств.

Показательный пример: в реестр российского ПО попало около 60 операционных систем (они все узкоспециализированные). Отобьют ли разработчики расходы на разработку? Вряд ли. Очевидно, что ни одна из этих компаний-разработчиков не способна произвести продукт мирового уровня, что называется, с нуля. А если какой-то придирчивый клиент попросит доработать ОС и укажет, как это сделать (что уже хорошо!), то для разработчика даже это будет невыгодно — лишних денег у него нет, он рассчитывает на тиражирование продукта. Но если на рынке 60 операционных систем, то рассчитывать на массовый спрос по меньшей мере утопично.

Эту проблему разработчик может попробовать решить с помощью кредита. Но чтобы его вернуть, опять надо иметь гарантии, что кто-то купит его операционную систему. Круг замкнулся. Вот к чему приводит отсутствие координации.

Хотя, конечно, удачные примеры работы в наших непростых условиях есть. Упомяну, например, ГК Astra Linux, которая сертифицировала свою ОС для работы на всех используемых в России процессорах как зарубежного производства, так и отечественных («Эльбрус» и «Байкал Т1») и успешно продаёт свои продукты. Но есть ещё одна большая проблема, связанная с системным подходом.

Так, на рынке есть восьмиядерные процессоры с архитектурой «Эльбрус» российского производства, их разрабатывает и производит компания МЦСТ. Означает ли это, что банки имеют возможность полноценно перейти на отечественную ИТ-инфраструктуру? Увы, рассчитывать на это пока рано. Почему? Операционная система для платформы «Эльбрус» построена на базе ядра Linux, и это хорошо. Но что плохо? Под архитектуру «Эльбруса» написано очень мало прикладного ПО. Крупнейшие вендоры ИТ-рынка, такие как Oracle, и пальцем не шевельнут, чтобы их приложения смогли работать с «Эльбрусом». Иными словами, процессор хорош, но вокруг нет той экосистемы, о которой мы говорим. И как банку действовать в такой ситуации? Как обойтись без Oracle? Ведь на настоящий момент нет ни одной open source СУБД, способной с ним конкурировать. А если серьёзный банк захочет мигрировать на свободно распространяемую СУБД PostgreSQL, это будет

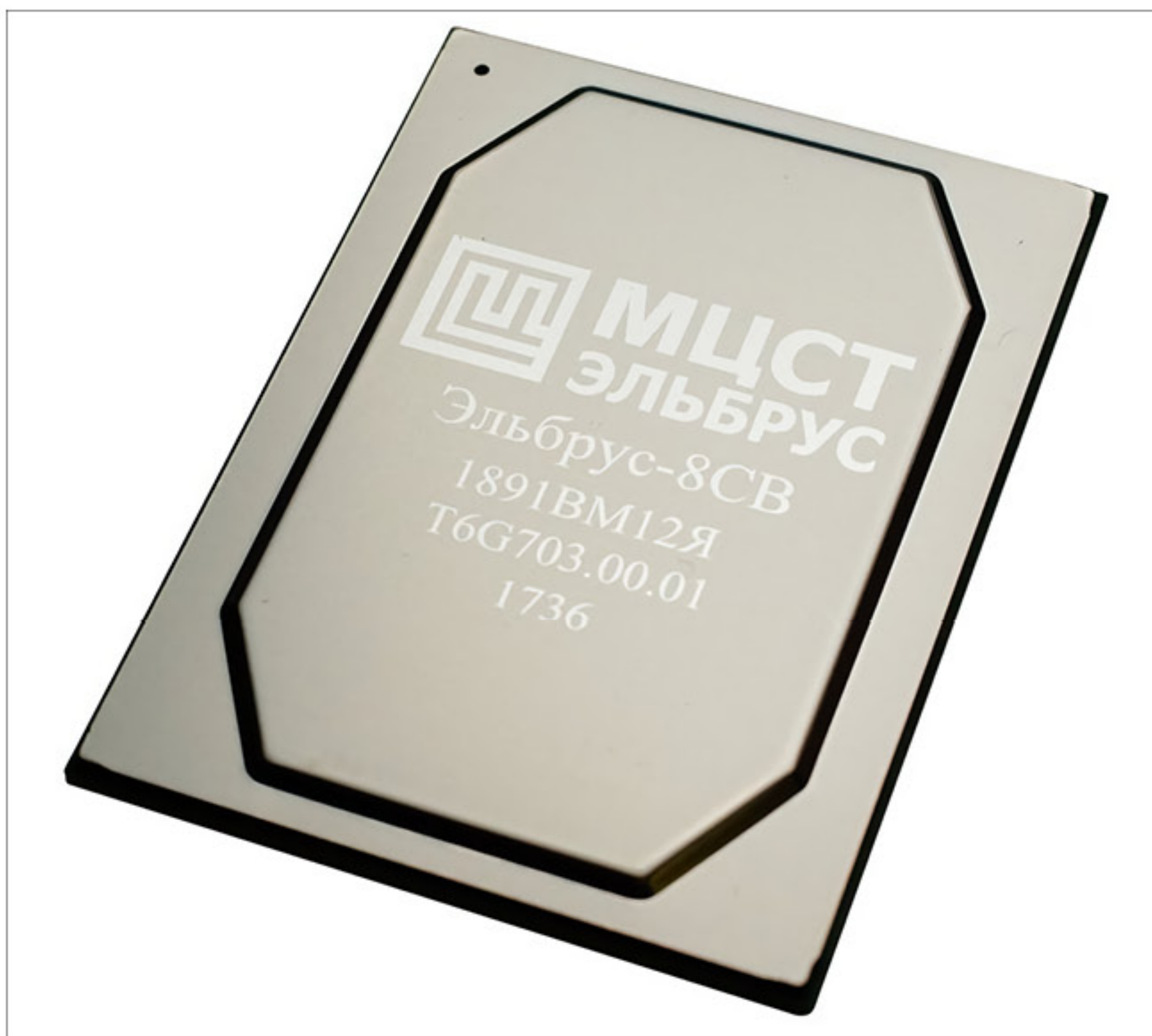
очень непросто, к тому же ему придётся переписывать всё существующее у него ПО. И кто ему за это заплатит? Как всегда, клиенты?..

В этой ситуации велико значение правильной постановки задач для перспективного развития отечественного ИТ-рынка. Это поле деятельности для российских экспертов, которых, что радует, у нас в стране много, и они в этих процессах уже задействованы. Но что обращает на себя внимание в этой связи? Всех толковых и активных экспертов, как правило, просят поработать бесплатно. Но ведь качественного прогноза бесплатно не получишь, и в этом одна из причин неудачных прогнозов развития.

Необходима не общественная, а сильная профессиональная экспертная команда, которая будет дорожить своей репутацией и отвечать головой за свои предложения. Нанятые эксперты, в отличие от «общественников», не будут заниматься продвижением собственных достижений, приоритетами для них станут государственные задачи. Конечно, работа на общественных началах — дело тоже полезное, вот только результат её до сих пор, увы, небольшой.

Следствием решения задач координации должна стать финансовая помощь игрокам, работающим над выполнением госзаказов по созданию взаимоувязанных бизнес-экосистем, в иных перспективных направлениях. Важно, чтобы все полезные с точки зрения государства ИТ-инициативы не оставались убыточными для их разработчиков, поэтому помогать ИТ-рынку государство обязано. Тем более что нашим игрокам всегда будет противодействовать внешний рынок. Он может, например, демпинговать в течение длительного времени. А бороться, скажем, с Microsoft нашим российским компаниям своими силами невозможно. Они, конечно, могут самостоятельно выпустить на рынок аналог MS Word, и этот аналог будет работать, более того, он уже есть на нашем рынке. Но более серьёзных задач внедрения таким образом не решить.

Есть ещё один важный риск. При массовой кампанейщине по замене ПО в сжатые сроки риски, связанные с нарушением непрерывности работы бизнеса, значительно превышают санкционные риски отключений. Эта тема пока мало обсуждается. Да, если пропадет техподдержка, то это плохо. Но если у банка есть лицензия, то программное обеспечение всё равно работает, а с «ключами» можно дополнительно подстраховаться и закупить их, скажем, на 10 лет вперёд. А если есть лицензия на ПО, то даже апгрейды можно получить обходным путём — через третьих лиц, на эти темы у нас в РФ даже конференции проводятся.



Под архитектуру «Эльбруса» написано очень мало прикладного ПО. Крупнейшие вендоры ИТ-рынка, такие как Oracle, и пальцем не шевельнут, чтобы их приложения смогли работать с «Эльбрусом»

Это, конечно, вынужденные меры, которые кому-то не понравятся. Но факт остаётся фактом: реально санкционные риски банкиров не очень-то пугают. Даже наш главный Банк России как работал на продуктах IBM, так и продолжает работать, а СУБД Oracle он использует для построения катастрофоустойчивого кластера в своей свежей ППС (перспективной платёжной системе).

Так что сами банки и без специальных мер принуждения или поощрения всякий раз тщательно тестируют выбираемые ИТ-решения и продукты, причём каждый банк делает это индивидуально. Вопрос один: были бы на рынке сами эти отечественные решения. Ясно, что схожие проблемы остро стоят практически во всех отраслях экономики России. Остаётся надеяться, что ситуация когда-нибудь изменится в лучшую сторону.



Наталья КАСПЕРСКАЯ
президент группы компаний InfoWatch,
председатель правления АРПП
«Отечественный софт»

5% ПРОТИВ 95%

«У НАС НЕТ СЦЕНАРИЯ, ПРИ КОТОРОМ МЫ МОГЛИ БЫ СОХРАНИТЬ ИМПОРТНЫЕ ИТ-СИСТЕМЫ»

Сегодня все мы наблюдаем, как развивается ситуация смены президентской власти в США — крупнейшей ИТ-империи мира. Не нужно иметь дар прозорливости, чтобы в последние 5–6 лет ясно видеть значительное ухудшение отношений между нашими странами. При этом США — основной источник информационных технологий, от которых мы очень сильно зависим. Во всех своих установочных документах и стратегиях они открыто называют Россию своим главным противником, как в геополитике, так и в киберпространстве. Поэтому импортозамещение в области ИТ — это насущная необходимость, причём очень срочная.

Чем мы рискуем? Если Россия не сократит цифровую зависимость от внешних недружелюбных игроков, то через какое-то время она потеряет и экономику. В конечном итоге тот, кто будет владеть цифровыми технологиями, будет владеть и экономикой. И в этом глубинный смысл понятия «цифровая экономика» — экономика будущего прямо зависит от цифровых технологий. А современные технологии устроены так, что ими владеет не тот, кто их купил, а тот, кто их разрабатывает, и чем дальше, тем сильнее эта зависимость от разработчика усугубляется.

Пользователь, который заплатил за ИТ-систему деньги, может ею пользоваться, может считать себя её полным хозяином, но на деле он не может её ни модифицировать, ни развивать, ни контролировать — контроль всегда остаётся в руках разработчика системы. По этой причине у нас нет сценария, при котором мы могли бы продолжать использовать импортные ИТ-системы на критически важных объектах сколько-нибудь долгое время. Удивительно, что сегодня в наших властных кругах и элите находятся люди, которые совсем не думают об этом очевидном риске.

Понятно, что заменять уже установленные и привычные ИТ-системы хлопотно и дорого. Это ведь не только покупка и установка новой системы, но и изменение бизнес-процессов, переобучение персонала и т.п. Но когда слышишь, как некоторые банкиры заявляют, что затраты на реализацию проектов импортозамещения

превысят 700 млрд руб., а из объёма кредитования отрасли будет изъято 5–7 трлн рублей — становится смешно. На чём основываются такие цифры? Почему именно 700 миллиардов, а не 600 или 300? Есть сомнения, что это результат какой-то более или менее серьёзной аналитики по всей банковской отрасли.

Кроме того, любое программное обеспечение можно покупать в рассрочку или вообще арендовать доступ к нему в облаке. Процесс импортозамещения при таких схемах приобретения будет постепенным, растянутым на несколько лет.

Но главная ошибка кроется в рассуждениях об «изъятии средств из экономики». Даже если допустить, что на импортозамещение будет потрачено именно 700 млрд рублей, то это деньги, остающиеся в нашей экономике, а не улетающие за границу. Эти деньги будут уплачены российским компаниям, которые выдадут зарплаты и премии сотрудникам, и все они (и компании, и сотрудники) будут тратить деньги на покупки в отечественных магазинах и обслуживаться в тех же банках. То есть деньги, потраченные на импортозамещение, будут двигать вперёд развитие отечественных компаний — разработчиков и интеграторов, насыщать деньгами отечественные рынки, стимулировать подъём российской экономики. А при покупке иностранных систем деньги безвозвратно уходят из нашей экономики за рубеж, это, действительно, потерянные средства.

Получается, что, осуществляя импортозамещение своей ИТ-инфраструктуры, банки выполняют своё предназначение — финансируют реальный сектор экономики, в данном случае — российский хайтек. Банки считаются кровеносной системой национальной экономики именно за способность поддерживать финансированием её реальные секторы. Применительно к ИТ это необычайно актуально, ведь у нас чудовищно недокредитованная отрасль! Мало кто знает, что доля кредитованности отрасли разработки программного обеспечения в России составляет примерно 5%, в то время как у девелоперов недвижимости, например, этот показатель — на уровне 90–95%. Это давно известная боль

ИТ-компаний — невозможность получить кредит из-за отсутствия материальных активов, которые можно взять в залог. А интеллектуальные активы банки, к сожалению, в залог не берут.

Проекты импортозамещения в сфере ИТ открывают перед банками новые возможности развития своего бизнеса. По сути, это инвестиции в развитие, с помощью которых они получают продукты и решения для его цифровизации, а также новых клиентов в лице ИТ-компаний, которым можно предложить специальные банковские продукты — кредиты и факторинг, тендерные гарантии для разработчиков. В этом симбиозе с ИТ-компаниями у банков появляется удобная возможность контролировать финансовое состояние своих поставщиков технологий, то есть быть уверенными в том, что они завтра не исчезнут и продолжают обслуживать банк. Такая схема долгосрочных взаимоотношений довольно распространена в ЕС и США.

Вообще, было бы очень здорово создать возможность льготного кредитования отечественных разработчиков и поставщиков ИТ-продуктов и решений на условиях исполнения обязательств в части внедрений и доработок этих решений. Полагаю, что такой подход к реализации стратегии импортозамещения, принятой на уровне страны, будет полезен всем: самим банкам, отечественной ИТ-отрасли и государству.

Противники импортозамещения любят рассказывать «страшилки» об импортозамещении, среди которых, кроме якобы высокой стоимости миграции на новую инфраструктуру, также фигурирует утверждение о том, что в России нет сравнимых по качеству и функциональности отечественных продуктов, что влечёт высокие риски для бизнеса. К этой «страшилке» следует относиться столь же критически, как и к «страшилке» о стоимости. В России есть аналоги практически для всех западных продуктов. В реестре отечественного ПО сейчас более 7000 наименований.

Замечу, что банковский сектор в смысле наличия отечественных решений находится уже в несколько лучшей ситуации, чем другие отрасли (например, промышленность). Ключевые автоматизированные банковские системы (АБС) — и так уже отечественные. Бухгалтерский софт — также. Проблемная точка в банках — платформенное и системное ПО, то есть операционные системы на клиентах и серверах, системы управления базами данных.

Но и здесь не требуется создания продуктов с нуля, а большей частью развитие, совершенствование, доведение существующих отечественных решений до уровня требований,

Проекты импортозамещения в сфере ИТ открывают перед банками новые возможности развития своего бизнеса. По сути, это инвестиции в развитие

предъявляемых современными финансовыми организациями. Эти задачи, как правило, решаются в ходе реальных проектов, когда клиенты проводят «пилоты», внедряют системы в филиалах, предъявляют свои претензии разработчикам, а те корректируют, исправляют, улучшают свои продукты.

Противодействие переходу на отечественное оказывается банками и их айтишниками ещё и потому, что они как заказчики привыкли к определённой модели использования программных систем по аналогии с западными образцами («сделайте мне как в продукте Microsoft») и зачастую не задумываются, что их реальные проблемы решаются по-другому и часто дешевле. «В продукте Microsoft» обычно 80% функциональности вообще не используется никогда, ещё 10% — используется изредка. А платить нужно за весь громоздкий комплекс «фич», «свистулек» и «фишек», а также отдельно и немало — за мировой бренд. Отечественные системы, как правило, имеют меньше функциональных «фишек», но зато они рядом и готовы быстро выполнять требования заказчиков по развитию и «подгонке» продукта. Поэтому работа с отечественными разработчиками выгоднее со всех точек зрения — качества, цены и т.д.

Добавлю ещё, что комитет по интеграции АРПП «Отечественный софт» ведёт работу по подготовке готовых интегрированных пакетов отечественных решений. Под пакетом я понимаю несколько продуктов, протестированных между собой на совместимость. Например, это может быть операционная система + СУБД + АБС + офисный софт + набор софта по информационной безопасности. Таких пакетов у АРПП около трёх десятков.

Что же касается рисков нарушения работоспособности ИТ-систем в процессе перехода на отечественное, то ещё большие риски существуют, если продолжать использовать импортные системы, особенно в условиях наложения всё новых санкций. Ведь прекращение обслуживания, доставки обновлений и тому подобные сюрпризы — это не теоретическая возможность. За последние несколько лет мы видели много примеров отказа западных поставщиков в обслуживании российских организаций, в том числе в банковской отрасли (например,



И хотя на этом пути есть препятствия, но дорогу осилит идущий. Если мы ничего не будем делать, а только ныть, что мы отстали на 20 лет, то будем и дальше усугублять нашу цифровую зависимость от внешних сил. А нужно действовать

отключение банка «Россия» от систем Visa и MasterCard в 2014 г.).

При аккуратном, поэтапном внедрении отечественных решений риски миграции можно свести к минимуму.

Упомяну ещё одну проблему импортозамещения последних лет — это мимикрия иностранных поставщиков и продуктов под отечественные путём смены названий и незначительных исправлений. Для борьбы с этим явлением в 2015 г. при Минкомсвязи РФ был

создан Экспертный совет по российскому программному обеспечению, который как раз занимается недопущением иностранных продуктов в единый реестр отечественного ПО.

Резюмирую: задача импортозамещения, поставленная правительством, вполне решаема. И хотя на этом пути есть препятствия, но дорогу осилит идущий. Если мы ничего не будем делать, а только ныть, что мы отстали на 20 лет, то будем и дальше усугублять нашу цифровую зависимость от внешних сил. А нужно действовать.

По этой причине мне кажется совершенно нецелесообразным и опасным сдвиг предельных сроков импортозамещения на 2024 г., то есть ещё на три года. У нас люди любят всё делать в последний момент, в ночь перед экзаменом, и при таком щедром сдвиге сроков можно ожидать, что в ближайшие три года работа по импортозамещению просто встанет. Этого нельзя допустить.

ЭВОЛЮЦИЯ ПРОТИВ РЕВОЛЮЦИИ

«САМОЕ УЗКОЕ МЕСТО — ЭТО СУБД УРОВНЯ
ORACLE/MS-SQL/DB 2»



Николай КУЛИКОВ
заместитель
генерального
директора
по развитию
компании SMART
technologies

Самый большой объём работ в рамках импортозамещения — это унаследованные системы. Банковские организации в течение последних 30 лет занимались разработкой программного обеспечения под свои нужды на устоявшемся наборе ПО, теперь им нужно оперативно перенести весь объём наработок на новый технологический стек, многие компоненты которого не имеют подтверждённых внедрений. Отсутствие доверия к части решений и сжатость сроков — ключевой вызов в рамках импортозамещения.

Понятно, что многие компоненты ИТ-инфраструктуры банков — сервера приложений, компоненты, клиентские и мобильные приложения — поддаются импортозамещению, и все банки активно работают в этом направлении. Многие банки переходят от лицензионных ИТ-решений на Open Source — с их помощью они могут снизить свою технологическую зависимость, оптимизировать затраты и т.д. Это происходит во всём банковском контуре, за исключением ядра любого банка — автоматизированной банковской системы (АБС). Там находятся компоненты, которые на данный момент отечественная ИТ-индустрия не производит.

Специфика ситуации заключается в том, что АБС — это сильно связанная информационная система, которая тяжело поддаётся горизонтальному масштабированию и разделению на микросервисы. Это определяет требования к наличию в инфраструктуре АБС высокопроизводительных серверов и реляционных БД, которые полностью могут использовать возможности таких серверов. К сожалению, аналогов серверов и подобных реляционных БД среди отечественных производителей нет.

Поэтому самое узкое место в импортозамещении — это реляционные СУБД уровня Oracle/MS-SQL/DB 2, работающие на

высокопроизводительном оборудовании. Не разрешив эти проблемы, мы не сможем обеспечить и тотальное импортозамещение.

Причём, что касается АБС на СУБД Oracle/MS-SQL/DB 2, то это решения, проверенные многократными внедрениями. Сегодня российские поставщики, к сожалению, не могут предложить полностью конкурентоспособного замещающего продукта. Есть хорошие активно развивающиеся решения, но их соответствие высоким требованиям банков не подтверждено использованием в высоконагруженных АБС.

Мы рассматриваем импортозамещение как эволюционный, а не революционный путь. Фактически, если использовать аналогию с автомобилем, мы должны заменить двигатель в работающем автомобиле: заменить «сердце» банка, не останавливая операции. Понадобится время, чтобы разработчики российских ИТ-решений достигли зрелости продуктов компаний Oracle, IBM, Microsoft и других, и их продукты смогли выдерживать нагрузки информационных систем крупных российских банков.

Что касается длительности эволюционного процесса импортозамещения в банках, то вероятность тотального импортозамещения в 2024 г. маловероятна.

Судите сами, смена любой АБС в банке — это, по оптимистичным оценкам, два года, при условии, что одна проверенная система меняется на другую. Скорее всего, сроки будут сдвинуты. Есть опасность, что возникнет соблазн бесконечно сдвигать сроки. Поэтому в данной ситуации нужно очень разумно-жесткое управление с целями. Банковская сфера — это элемент критической инфраструктуры, поэтому надёжность и стабильность — существенный сдерживающий фактор. Как подойти к решению этой задачи?

Понимая, что текущий технологический стек, на который планируется переходить, не позволяет полностью закрыть все потребности банков, нужно максимально обезопасить

от внешних воздействий те компоненты, которые слабо поддаются переносу. И иметь детально проработанные планы по эксплуатации компонентов в том случае, если иностранные вендоры откажут финансовым организациям в их поддержке.

Было бы логично, не делая громких заявлений, разработать некоторую карту/методологию зрелости импортозамещения внутри банка. Тогда, понимая степень зрелости отечественных ИТ-продуктов и возможностей их использования для замещения импортных компонент, можно сформировать программу постепенного наращивания степени «импортозамещённости» внутри банков. В этом случае банкам не придётся бежать широким фронтом, замещая подряд всё, что есть в ИТ-инфраструктуре. Наоборот, можно будет мотивировать и в то же время не перегружать банки, ставить разумные задачи по достижению конкретной степени зрелости импортозамещения в течение определённого срока. Банки будут последовательно менять компоненты, и в целом будет понятно, когда все мероприятия завершатся.

Иными словами, банк будет последовательно наращивать долю «импортозамещённых» продуктов. Параллельно будет развиваться сама технологическая база, например, появится адекватная российская реляционная СУБД, которая, возможно, будет работать на западном «железе». Или появится наше отечественное «железо», соответствующее требованиям банков. В любом случае это поможет скорректировать маршрут импортозамещения в сторону увеличения доли российского.

Фактически речь идёт о некоторой дорожной карте, в которой выделены нужные элементы и проставлены оценки критичности. Наличие такой стандартизированной карты/методологии позволит понимать степень прогресса.

В целом, с точки зрения ИТ-систем, банки между собой похожи. У них разные бизнес-стратегии, но группы банковских процессов одинаковы. Значит, скорее всего, методологию зрелости импортозамещения нужно строить от банковских функциональных областей: финансовая оценка клиентов, CRM и т.д. — и анализировать, какие технологические стеки используются для их реализации, и отсюда определять, насколько та или иная функциональная область «импортонезависима».

В этой связи интересен вопрос согласованности активности российских ИТ-разработчиков и банков. У банков — одна мотивация, у технологических компаний — другая, и они должны выстраиваться параллельно. Не думаю, что банки

сильно заинтересованы в управлении разработками решений. У них другая задача в рамках импортозамещения — управлять наращиванием доли импортозамещённых компонент, исходя из всех имеющихся на рынке возможностей.

Координация и синхронизация действий банков и разработчиков — это, скорее всего, задача государства или ЦБ. Все банки, по сути, достаточно зрелы в своих внутренних процессах, но они их поддерживают на базе зарубежного технологического стека. Необходимо в ходе пилотных проектов понять, какие российские решения и в каких банковских процессах были успешно использованы в рамках импортозамещения.

Важный вопрос — финансирование этой деятельности. На мой взгляд, это не могут быть только коммерческие инвестиции. Ведь речь идёт о долгосрочных вложениях в создание продуктов, которые потом будут использоваться на рынке и обеспечивать функционирование критической инфраструктуры. Банк — это коммерческая структура, которая должна инвестировать деньги в то, что рано или поздно принесёт отдачу. И тут вопрос: когда и как этот новый отечественный продукт себя окупит? Так что здесь скорее простор для государственных и венчурных инвестиций.

Также это могут быть льготы, дотации — всё, что будет максимально мотивировать российских разработчиков создавать прорывные отечественные продукты. Обеспечение эволюционного процесса управляемого и поступательного импортозамещения — это ключевой вызов для государственных регуляторов. Причём простых призывов недостаточно. Призыв «Давайте импортозамещаться» эквивалентен «Давайте построим коммунизм».

* * *

Чтобы реализовать это на практике, нужна система метрик на базе методологии. Тогда будет понятно, какие данные стоит добавить в KPI руководителям разных уровней, чтобы они были заинтересованы в практическом исполнении планов импортозамещения. Ведь управлять можно только тем, что измеримо: анализировать динамику, вовремя выявлять наметившиеся провалы, принимать дополнительные управленческие решения, в том числе по дополнительным инвестициям. Тогда можно чётко понимать, где мы можем сократить технологическую зависимость максимально безболезненно, а где придётся очень постараться.

СРЕДИННЫЙ ПУТЬ ПРОТИВ ВЫСТРЕЛА В НОГУ

«ОПТИМАЛЬНЫЙ ВАРИАНТ — ЧАСТНО-ГОСУДАРСТВЕННОЕ ПАРТНЁРСТВО, А ВОЗМОЖНО, ГОСКОРПОРАЦИЯ»

Относительно доли используемого иностранного ПО и ИТ-оборудования в финансовой отрасли на уровне 85 % банкирам, конечно, виднее, но, думаю, что оценка не совсем верная. Скорее, эта доля достигает 95%. Но что сегодня по-настоящему беспокоит банкиров? Прежде всего, безудержная денежная эмиссия в ответ на пандемию CoVID-19, отключения от SWIFT и ограничения доступа к долгосрочному фондированию и капиталу как результат ужесточения антироссийских санкций, высокая рыночная волатильность, отзыв банковской лицензии, угроза «затопления» объёмами хранимой информации. Ну и проблема импортозамещения. В чём выражается эта проблема?

Представьте себе, что у вас есть заштатная вила на 12 комнат на Лазурном берегу. И вдруг вам говорят, что теперь вы будете жить в ближнем Подмосковье, где вам предоставят шикарную четырёхкомнатную квартиру со всеми удобствами. С одной стороны, хорошо, что качество жилья улучшится. Но с другой — куда девать всю эту мебель и бытовую технику, диваны, пуфы, буфеты и прочая, что составляет комфортный быт? В четыре комнаты то, что стояло в двенадцати, просто не влезет. Так и в нашем случае: как ни ругай зарубежные технологии, но, к сожалению, предложить отечественные аналоги (не похожие, а именно аналоги) пока нет возможности. Не могут пока отечественные средства обеспечить банковские бизнес-процессы с тем же качеством и той же надёжностью, что и зарубежные.

Но банковский сектор очень сильно зависит от качества ИТ-технологий. Любой сбой в транзакциях (а это сегодня, как правило, электронные транзакции) может привести к краху всего бизнеса. Вот поэтому банкиры стараются выбрать то, что надёжно, функционально, недорого и эффективно. И если наши производители смогут предложить что-то, действительно отвечающее этим требованиям, то, скорее всего, проблема импортозамещения решится сама собой.

Стоит иметь в виду, что жизненный цикл любой информационной системы составляет примерно 7–10 лет, а моральное устаревание аппаратной платформы и того меньше — 3–5 лет.

Вот и получается, что любой банк приблизительно каждые пять лет обязательно сталкивается с проблемой модернизации своей информационной системы. И в этот момент для него, по сути, не имеет значения, переходить ли на отечественное оборудование, которое не уступает по качеству и функциональности западному, или на западное. Кстати, по этой же причине оценки огромных затрат на переход на отечественное оборудование, которые делают банки, на мой взгляд, сильно завышены: в любом случае каждый банк закладывает в бюджет регулярную модернизацию информационных систем. Здесь главное, чтобы было на что менять нынешние импортные решения. И это уже проблема российских производителей.

В этой задаче есть несколько критически важных моментов. Во-первых, наши заказчики уже давно прошли тот рыночный этап, когда им предлагали сырой продукт и предлагали «доработать» его непосредственно «под заказчика», так сказать, «кастомизировать». В ситуации, когда на рынке есть продукты, готовые к применению, но западные, и отечественные продукты, требующие «доработки напильником», потребитель всегда отдаст предпочтение тому, что может сразу начать работать.

Во-вторых, разработать отечественное специальное программное обеспечение — можно, но и работать оно должно на отечественном железе, а его нет. Поэтому и начинать надо прежде всего именно с отечественной элементной базы. И такая база должна быть лучше, чем западная, и производиться серийно. Вот тогда и разработка ПО активизируется.

Задача, по-моему, стоит в том, чтобы поощрять тех российских производителей, которые делают не просто «российское ПО», а российское ПО, не уступающее ни по функциональности, ни по надёжности западным аналогам и работающее на отечественной качественной элементной базе. Именно на это должны быть нацелены преференции государства, тогда и банки будут брать такой продукт без всякого сопротивления нажиму государства. Кстати, по этой причине нынешние реестры отечественного оборудования и ПО не могут



Сергей ВИХОРЕВ

советник
генерального
директора компании
«ИТ-экспертиза»

рассматриваться в качестве рабочего механизма импортозамещения.

Сегодня присутствие в реестре говорит только о производстве конкретной продукции на территории нашей страны. А для задачи импортозамещения важно, чтобы продукт выполнял конкретные функции, был надёжен и демонстрировал параметры функционирования на уровне мировых требований. В этом случае банки без сопротивления согласятся на импортозамещение, а до того будут исходить из оценки рисков: если риск пользования импортным продуктом меньше риска потери функциональности или надёжности, перехода на отечественное не будет.

В этом объективно заключается вызов нынешней ситуации: чтобы создать полный аналог зарубежного продукта, нужны деньги, время, производственные мощности.

Ещё со времён Ломоносова известно, что «может собственных Платонов и быстрых разумом Невтонов Российская земля рождать». Да, создать что-то гениальное для наших спецов — не проблема. Проблема в том, что это будет уникальный, можно сказать, эксклюзивный продукт. Придумать можно, а вот наладить серийное производство... Именно здесь мы ещё очень сильно отстаём от Запада и без его технологий вряд ли справимся.

Вспомним историю на примере автопрома. В начале 30-х в России было трудно с автомобилем — купили технологии Ford. После Великой Отечественной войны по репатриации к нам пришли технологии Opel. Позже, в 70-х, купили технологии Fiat. Но тогда можно было купить технологии, а сегодня — нет. Значит, надо приложить максимум усилий и найти, где можно купить. Ещё один вариант — производство на зарубежных производствах под контролем российских заказчиков. Фактически именно таким образом американские вендоры производят свою высокотехнологичную продукцию в Китае. Кто нам мешает действовать так же? Надо найти методы и способы контроля производства элементной базы в тех странах, которые владеют передовыми производственными технологиями и не отключат нас от этих технологий.

Конечно, этот подход не может быть стратегической линией. Но для промежуточной стадии импортозамещения, когда ещё нет нужного отечественного оборудования, паллиативные меры эффективны. Например, создание совместного производственного предприятия с нашим инженерным контролем производства на «той» стороне позволит радикально снизить остроту проблемы «переклейки шильдиков». А создание доверенной среды на базе импортного

оборудования снизит риски информационной безопасности ИТ-инфраструктуры банков.

Но надо понимать, что такой «срединный путь» взамен реального импортозамещения — это типичный путь. Обязательно надо переходить на продукцию отечественных производителей и быть полностью независимыми от западных технологий, поскольку только такая независимость в итоге обеспечивает безопасность страны. Но как промежуточный вариант на переходный период эти действия оправданы и даже необходимы. По мановению волшебной палочки технологии не развиваются, нужно время, а работать банкам надо. Поэтому на это время как раз и нужно вводить режим «срединного пути». Но при этом нельзя забывать о безопасности и с этой целью обеспечить доверие к тем платформам, которые производятся на Западе. Решаемая ли это задача?

Да, решаемая, но требует многогранной комплексной работы. С одной стороны, надо модернизировать систему подтверждения доверия, придать ей определённую гибкость, устранить необоснованные требования, расширить полномочия и ответственность тех, кто проверяет. С другой стороны, надо найти юридические механизмы получения гарантий западных производителей в долгосрочных обязательствах, не подверженных каким-либо санкциям, по поставке и технической поддержке продукции на нашей территории. С третьей стороны, надо разработать специальные средства мониторинга за работой информационных систем на основе западных платформ.

В принципе, здесь нет ничего нового. Это модная в последнее время парадигма «нулевого доверия» — Zero Trust, идея, получившая своё второе дыхание во время пандемии. Считается, что она была придумана в 2010 году аналитиком Forrester, но на самом деле в России парадигма «доверенной среды» появилась лет на 20 раньше (как говорится, нет пророка в своём отечестве). Идея очень проста: никому не доверяем, всех контролируем. Да и средства, способные это сделать, уже есть, пусть немного, но есть. Может быть, это и есть выход? Ну а потом, когда мы сможем контролировать то, что сами пока не производим, будем развивать собственную производственную базу. Вот и решим проблему импортозамещения, не очень напрягая потребителей.

Для комплексного решения поставленной задачи просматривается альянс: государство, банк, производитель, интегратор. Каждому участнику интересно решение этой задачи, но по отдельности ни у кого не хватает денег на её решение. Поэтому оптимальным вариантом в этом случае может стать частно-государственное партнёрство, а возможно, госкорпорация.

ВНУТРЕННИЙ НАРУШИТЕЛЬ ПРОТИВ ВНЕШНЕГО

«В ОЧЕРЕДИ НА ИМПОРТОЗАМЕЩЕНИЕ
БАНКИ БУДУТ ПОСЛЕДНИМИ»



Ренат ЮСУПОВ
старший вице-
президент
компании Kraftway

Что касается банковской ИТ-инфраструктуры, то до тех пор, пока продукция отечественных производителей не станет полностью конкурентоспособной с импортной и по характеристикам, и по ценам, мы ничего не сможем сделать. Потому что менеджеры, принимающие решения в банках, умеют считать деньги. И если есть возможность сэкономить, они сэкономят, то есть купят импортную технику, оставив в стороне все призывы к импортозамещению.

Вопросы информационной безопасности, конечно, имеют значение. Другое дело, что модели угроз, с которыми работает банковский сектор, отличаются от тех, которые есть в информационных системах других ведомств. На первом месте у них сохранность персональных данных. Даже вводится в действие Единая биометрическая система (ЕБС), которая позволяет идентифицировать клиента не только по паролям, логинам и SMS, но дополнительно по биометрическим данным. Важно, что в части персональных данных больше проблем доставляют не внешние нарушители, а внутренние. А в банковских структурах с развитой филиальной сетью внутренний нарушитель — это вообще одна большая головная боль. Крупные утечки данных, которые происходили в крупных банках, происходили как раз через филиалы и через конкретных людей — самое слабое звено в любой системе.

Сегодня внутренний нарушитель — самое страшное в банковской системе, но импортозамещение эту проблему не решает, потому что оно нацелено в основном на внешнего нарушителя: кибервойны, кибератаки и т.д. Конечно, банковская система подвержена им тоже, но в приоритетном списке угроз они стоят, скорее всего, на третьем месте — после рисков утечек персональных данных и угроз ДБО.

Таким образом, на первом месте — проблемы, связанные с клиентами, на втором — с деньгами, и только на третьем — с внутренней ИТ-инфраструктурой. При этом ситуация

с отечественным софтом там выглядит более-менее неплохо. С «железом» ситуация иная — Центральный банк этими вопросами не очень занимался, потому что реальной угрозы там вообще не видел. По сути, только сейчас заговорили об этих угрозах — тех, которые реализуются через компьютерное «железо», и таких «дыр» довольно много.

Поэтому логика банковских ассоциаций, которые просили перенести сроки импортозамещения для банков на 2027–2028 год, понятна. Но с точки зрения государства это вредная практика. По одной причине: не создав внутреннего спроса на импортозамещающие продукты, невозможно достичь нужного результата — получения импортозамещающей продукции, которая будет конкурентоспособной по цене и техническим характеристикам.

Как государству продвигать идею импортозамещения в банковском секторе? С одной стороны, раз все отрасли принуждают к импортозамещению, то почему эту должны обойти вниманием? С другой, если банки сами не ощущают острой необходимости в импортозамещении, то их сопротивление принуждению будет сильнее, чем в других отраслях. Тут и безопасники, которые нередко конфликтуют с айтишниками, займут солидарную позицию: нам нужно потратить деньги на самую актуальную задачу защиты клиентских данных, при чём тут российский процессор?

Поэтому я считаю, что сегодня банковский сектор — это не первоочередной кандидат на успешное импортозамещение. Конечно, банки должны быть в списке импортозамещаемых,

Не создав внутреннего спроса на импортозамещающие продукты, невозможно достичь нужного результата — получения импортозамещающей продукции

но усилия, которые на них придётся затратить, будут гораздо больше, чем в других секторах экономики. В итоге они всё равно впишутся в тему — в тот момент, когда другие отрасли станут переходить на отечественную продукцию, сама эта продукция станет гораздо лучше, технологичнее, дешевле и т.д. К этому моменту и «дыры» в электронной компонентной базе будут закрываться, в операционных системах, то есть весь стек технологий станет более безопасным.

Другое дело, что всё равно это длительный процесс. Помимо ЦОДов и офисного оборудования, есть ещё и банкоматы. А импортозаместить банкоматы — это гораздо более сложная задача, чем создать отечественный ПК. Поэтому отечественные производители не будут усиленно стремиться в этот сегмент, и понадобится довольно длительный период разработки, чтобы там появился национальный лидер.

Кроме того, у многих банков — разветвлённая филиальная сеть. Даже для банка средней руки с сотней филиалов это уже крайне сложная задача — взять и начать менять во всех филиалах аппаратное обеспечение. Это очень дорогостоящее удовольствие и непростой проект, потому что придётся переучивать целые организации, которые занимаются эксплуатацией инфраструктуры.

Впрочем, банки будут вынуждены играть по правилам, которые устанавливаются для КИИ. Вот только сопротивляться этому процессу они будут дольше всех. Будут ещё и ещё раз просить откладывать сроки. Скорее всего, в очередь импортозамещения банки встанут, но будут в ней последними.

Возникает логичный вопрос: можно ли ускорить этот процесс за счёт некоторых типовых протестированных решений, которым банки могут доверять в ходе модернизации ИТ-инфраструктуры? С одной стороны, вроде бы, с точки зрения ИТ, там используются типовые решения. С другой — ИТ-инфраструктура разных банков развивалась хаотично. Предложить переход на современную платформу? Тут тоже всё не так просто.

У них уже есть набор серверного «железа» в ЦОДах, серверного ПО и прикладного ПО на клиентах. У них есть определённые протоколы, по которым они работают. Значит, они сразу потребуют каких-то виртуальных десктопов типа Citrix в стиле «сделайте нам такой же». Пойдут специфические запросы на доработку ПО. И переместить всю инфраструктуру с VDI на новое решение на базе новых производителей — это точно непростая задача. Ведь даже когда банк меняет внутреннюю базу данных, скажем, с SQL переходит на PostgreSQL, он к этому готовится года

полтора-два, потому что это крайне сложная и ответственная задача. А тут задача сложнее на порядок — перевести все клиентские рабочие места на отечественный софт, на десктопах ведь очень часто используются проприетарные протоколы. Особенно этим любит заниматься тот же Citrix, знатный любитель что-нибудь такое проприетарное учудить. Попробуй обеспечить поддержку такого протокола! Не зря ведь мы говорим, по сути, про классическую задачу импортозависимости: если подсел на «иглу» того или иного крупного вендора, сойти с неё крайне трудно.

Поэтому есть большие сомнения в том, что на практике удастся реализовать типовое протестированное решение — вряд ли оно будет сразу применимо для всех. Оно не сможет стать типовым, скорее всего, в силу того, что ИТ-инфраструктура развивалась в разных банках по-разному. Скажем, в ЕБС худо-бедно есть типовой подход, потому что есть требования, которые предъявляют регуляторы ИБ, есть определённая регуляторная база. А в части импортозамещения, по сути, регуляtorики нет. Есть квоты и требование продукции из реестров. Но этот набор никак не тянет на механизм регулирования. Кто может сказать, есть ли вообще в этих реестрах то, что надо банкам для импортозамещения?

Возьмите недавний скандал по поводу СХД на базе отечественного процессора. Регулятор в лице Минпромторга требует, чтобы сегодня под требования импортозамещения попадали только такие. Но таких производителей — раз два и обчёлся. Разве это выбор? А другие российские производители, которые уже присутствовали в реестре, больше не отечественные?

Конечно, как представитель отечественного разработчика и производителя, я не на стороне банков в их истории с торможением импортозамещения. Уже сегодня есть целый ряд отечественных решений по безопасности, которые комплексно закрывают бреши информационной инфраструктуры на уровне аппаратуры, на уровне охраняемых данных и на уровне контроля и разграничения допустимых действий внутренних пользователей. Такие решения позволяют обеспечить надёжное прикрытие от кибератак и внутренних нарушителей. Однако пока они не на слуху, и поэтому ими пользуются в основном специализированные организации. Но, честно говоря, я понимаю сопротивление финансовых организаций процессу «обрусения». Видя те большие трудности, с которыми сегодня сопряжён переход банков на новую продукцию, и понимая лоббистские возможности банкиров, думаю, сроки перехода на отечественные ИТ-решения будут сдвигаться всё дальше и дальше. Тем более что банки,

даже самые крупные, не являются госструктурами, и потому влияние государства в этом секторе будет не самым сильным. И даже принадлежность к объектам КИИ вряд ли изменит ситуацию.

В конце концов импортозамещение всё-таки состоится. Но только когда импортозамещающая продукция будет близка к состоянию зрелости, и зрелость обретёт весь рынок отечественных ИТ-решений, подходящих для импортозамещения. К этому времени появятся успешные кейсы в разных банках, которые можно изучать и примерять к собственной инфраструктуре. А если к этому времени будут решены

задачи защиты клиентских данных и систем ДБО, тогда точно во весь рост встанет вопрос защиты от угроз самой ИТ-инфраструктуры от кибератак. Приоритет этого риска повысится, на эти задачи будут выделены деньги. И тогда ЦБ введёт какое-нибудь жёсткое регулирование: переходите на отечественные ИТ или лишитесь лицензии.

А до того мы будем слышать «убедительные» рассказы о невозможности миграции. Если, конечно, государство не скорректирует своё отношение к регулированию процессов импортозамещения в финансовой сфере.

КАРТА «МИР» ПРОТИВ ЗАПАДНЫХ КОНКУРЕНТОВ

«РЕЗКИЙ ПЕРЕХОД НА ДРУГИХ ВЕНДОРОВ И ПОСТАВЩИКОВ — РИСК САМ ПО СЕБЕ»

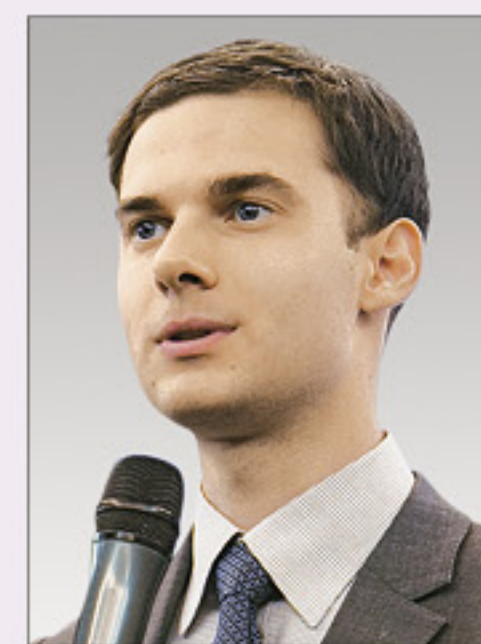
Финансовый сектор сегодня в принципе сильно зависит от информационных технологий. Более того, банки по большому счёту конкурируют именно на уровне технологических решений: качеством интерфейсов, скоростью обработки платежей и т.д. Поэтому конкуренция разработчиков ПО и производителей оборудования не менее важна, чем конкуренция банков. Не будет конкуренции — не будет инноваций. Это видно по кейсам национальных карточных систем. В тех странах, где такие системы являются монополиями, их технологический прогресс ограничен, стимулов к развитию нет. А в России, где карты «Мир» вынуждены конкурировать с иностранными системами, НСПК старается не отставать от конкурентов.

На самом деле, с 2014 года платёжный рынок прошёл очень большой, иногда болезненный, путь локализации. Все карточные операции обрабатываются внутри страны, у нас есть российский аналог SWIFT, есть российская СБП и так далее. Поэтому тезис о критических рисках экономики и системы государственного управления мне кажется несколько преувеличенным.

С чисто операционной точки зрения, резкий переход на других вендоров и поставщиков (вне зависимости от их

национальной принадлежности) — риск сам по себе. Банк — это огромная технологическая машина, которая обрабатывает платежи, управляет рисками, хранит и анализирует клиентские данные, формирует и сдаёт отчётность регуляторам. Сбои и ошибки неизбежно приведут к сбоям в обслуживании клиентов, этот риск вполне материален. К тому же банки связаны между собой: проблемы у одного неизбежно сказываются на других. Не говоря о том, что перестройка связана с внушительными затратами: особенно это актуально для низкомаржинальных банков, бюджеты и людские ресурсы у которых ограничены.

То, что оборудование и программное обеспечение, которое используют финансовые организации, должно работать стабильно, предсказуемо, быть защищено от внешних влияний и исключать риски контрагента — безусловно, правильно. Но оно также должно постоянно эволюционировать, отвечать требованиям банков, которые конкурируют с иностранными финансовыми сервисами. Эти критерии мне представляются первичными. И если отечественные предложения будут, во-первых, этим требованиям отвечать и, во-вторых, будут конкурентоспособны по цене, то финансовые организации сами будут постепенно на них переходить, даже без нормативной обязанности.



Павел ШУСТ
исполнительный директор Ассоциации участников рынка электронных денег и денежных переводов «АЭД»



Светлана АППАЛОНОВА
председатель
Совета Ассоциации
производителей
электронной
аппаратуры
и приборов (АПЭАП)

МИМИКРИЯ ПОД ОТЕЧЕСТВЕННОЕ ПРОТИВ ОТЕЧЕСТВЕННОГО

«ПОЧЕМУ БЫ НАМ НЕ СДЕЛАТЬ ВЕЛИКОЙ
СВОЮ СТРАНУ?»

Когда банки начинают говорить про 5–7 триллионов рублей, которые будут изъяты из объёма кредитования отрасли, то, видимо, подразумевается замена всего «железа» и ПО банков. Напомню также, что несколько лет назад Сбербанк объявил об обеспечении кредитных линий Huawei на уровне 600 млрд долларов, что широко обсуждалось. Но тогда почему-то никто не беспокоился, что эти деньги выводятся из кредитования российской экономики. Тогда почему бы этой же кредитной организации не обеспечивать кредитные линии для российского оборудования? Это вопрос сочетания тактических и стратегических целей.

МИФЫ ПРОТИВ МЕХАНИЗМОВ

В нынешних условиях сама банковская система, её здоровье и работоспособность — это государственный интерес, а вовсе не исключительно коммерческий интерес отдельных банковских организаций. В таком контексте необходимо развенчивание ряда мифов относительно отечественной и зарубежной ИТ-продукции. В частности, миф о дороговизне российских решений. Пример из сферы телекома: даже крупнейшие федеральные операторы жалуются на нынешние высокие цены телеком-оборудования. Причина в том, что, по сути, в телекоме сложилась олигополия 4–5 зарубежных вендоров, которые держат очень высокие цены. Сегодня они действуют в основном через товарные кредиты и продажи законченных решений. А при изменениях курса доллара операторы, которые воспользовались этими привлекательными кредитами, попали в жёсткую долговую зависимость. Так что дорогое отечественное оборудование — это, я бы сказала, экзистенциальный вопрос.

Ещё один миф — риски нарушения работоспособности критически важных ИТ-систем в результате импортозамещения. Для задач модернизации всегда используются тестовые зоны и мероприятия для тестирования качества систем. А совместимость с уже установленным зарубежным оборудованием в ходе постепенного перехода — это вопрос стандартизации. Если мы ведём разработку, следуя стандартам, все подключения будут работать нормально.

МЕТОДОЛОГИЯ ЕСТЬ, НУЖНА СТРАТЕГИЯ

В 2018 г. в рамках «Цифровой экономики» наша ассоциация выполнила исследовательскую работу по теме преимущественного применения отечественного ПО, телекоммуникационного оборудования и вычислительной техники на объектах КИИ. Там всё системно разложено по полочкам: вначале проводится аудит того, что есть, оборудование и ПО разбивается по группам риска. Причём начинать надо с верхнеуровневого ПО и оборудования. А поскольку по верхнему уровню у нас точно не всё есть, то, прежде чем запрещать что-то, надо создать своё. Но если стратегии такой деятельности нет, то, наверное, надо переформатировать госпрограммы.

ПРО ТИПОВЫЕ ТЗ

Ключевым элементом госпрограммы должно стать формирование типовых ТЗ на разработку недостающих ИТ-продуктов и решений. Такое ТЗ должно создаваться совместно банками-заказчиками и экспертами, а дальше выделяется финансирование и объявляется поиск разработчика оборудования с конкретными характеристиками и в указанные сроки. В этом механизме нет ничего особо нового — это так называемый

контракт с отложенными обязательствами: тот, кто подписывается на эти условия, получает впоследствии гарантированную долю рынка. Здесь критически важно развивать внутреннюю конкуренцию ИТ-разработчиков, ведь самым банкам важно наличие по крайней мере двух российских поставщиков, чтобы избежать монополизма единственного вендора. В этом смысле единственный поставщик — ущербное решение, его нужно максимально избегать.

РЫНОК ПРОТИВ МИНПРОМТОРГА

Совсем иной подход к разработке новых решений сегодня использует Минпромторг. По линии департамента радиоэлектронной промышленности Минпромторга РФ идут, например, программы субсидирования отечественного телеком-оборудования, вычислительной техники. Разработчики приходят со своими проектами, их отбирают по определённым критериям. При этом каждый не только описывает, что он намерен разработать, но ещё и обеспечивает такой же объём внебюджетного финансирования, а также обязуется самостоятельно коммерциализовать свою разработку в определённый срок. Фактически самому разработчику предлагается за финансовую субсидию создать рынок сбыта для своей разработки, и это притом, что ни один НПА по формированию рынка для российской хайтек-продукции пока не работает. На каком основании разработчик может обещать гарантированные объёмы продаж на конкурентном рынке, если его вообще никто не поддерживает? Иными словами, если рынок сбыта принудительно не формируется государством, то откуда возьмётся внебюджетное финансирование? И это не новость: абсолютно все страны, которые стали высокотехнологичными лидерами, занимались тем, что формировали рынки под своих разработчиков, как внутри страны, так и вне её.

Наши заказчики — неглупые люди. Если они поймут, что само государство открывает рынок для российских вендоров, они сами к ним придут. В ином случае — то, что мы видим сейчас, — заказчики не хотят вкладываться в проекты миграции на отечественную продукцию, предпочитая заниматься мифотворчеством. Ну а разработчики ищут выходы из создавшейся ситуации, и мы порой видим, что в реестр телекоммуникационного оборудования российского происхождения (ТОРП) приносят по третьему разу один и тот же маршрутизатор...

Нужен принципиально иной подход: вначале — задача, а от неё должны идти деньги, но не на субсидии, а на получение части рынка — он

сразу формируется под тех исполнителей, кто действительно выполняет поставленную задачу. Однако не надо начинать процесс импортозамещения с самого нижнего уровня «железа», и не надо пытаться сразу перевести на российскую продукцию всё.

МИМИКРИЯ ПОД ОТЕЧЕСТВЕННОЕ ПРОТИВ ОТЕЧЕСТВЕННОГО

Не надо также заниматься кампанейщиной в стиле «пятилетку за 4 года» — полностью импортозаместиться в 2024 году. У такой задачи есть только два варианта решения: либо вся ИТ-инфраструктура компаний будет российской, либо весь пар уйдёт в свисток «бумажного» импортозамещения. Поскольку первый вариант недостижим, остаётся второй. И мы сегодня наблюдаем активную работу над корректировками критериев признания оборудования и ПО отечественным, в которой принимают участие самые разные группы лоббистов. А ведь эти критерии действительно нуждаются в корректировке — нужно, в конце концов, положить конец порочной практике «переклейки шильдиков», которая, к сожалению, по-прежнему процветает. В то же время лоббисты status quo, то есть отказа от перехода на отечественные решения — а к ним относятся в первую очередь крупнейшие компании из разных отраслей экономики, в том числе банковского сектора, — стремятся законодательно закрепить в этих критериях сложившуюся практику применения зарубежной продукции под видом «мимикрии» под отечественное.

Так, неурегулированность понятия «продукт ЕАЭС» на внутреннем контуре Союза по-прежнему обеспечивает статус российского продуктам локализации зарубежных дочек американских и китайских вендоров. Подчеркну, что при этом технологии в ЕАЭС не передаются. Но при нынешнем подходе к определению «товар ЕАЭС» можно ожидать повторения ситуации с белорусскими креветками и белорусским пармезаном и в высокотехнологичных областях. Кроме того, все НПА, которые сегодня дают преференции российской продукции, отталкиваются от тезиса про отсутствие аналога российской продукции, произведённой на территории РФ. Такой подход гарантированно ставит страну в положение вечно догоняющих. Нужно вместо аналогов опираться на национальные продукты и национальные стандарты.

ОТ ПРИНУЖДЕНИЯ К СТАНДАРТАМ

Таким образом, сложилась парадоксальная ситуация: на фоне всех призывов к импортозамещению отраслевые заказчики этого просто не

Никакой экспорт в модели локализации не светит, потому что локализуют тебя ровно настолько, насколько это нужно зарубежному вендору из каких-либо, например, логистических соображений

хотят, а российских производителей мало кто об этом спрашивает. Так что заставить банки заняться ИТ-импортозамещением может только государство. И принуждение — это единственный метод. Зато потом те типовые решения, которые будут обкатаны на пилотных банках, станут тиражироваться и перерастать в национальные стандарты.

ОТ РОССИЙСКОЙ ТЕРРИТОРИИ К РОССИЙСКОМУ ПРОИСХОЖДЕНИЮ

Помимо принуждения, конечно, и побудительные стимулы надо использовать. Как минимум КРІ топ-менеджмента банков должны быть связаны с импортозамещением. Правда, реализовать этот механизм нужно очень точно, чтобы не получилось то, что мы видим сегодня вокруг, — вендорозамещение вместо импортозамещения.

Есть отрадный факт: вице-премьер Юрий Борисов дал поручение внести изменения в 488-ФЗ «О промышленной политике» — ввести в регуляторную практику термин «оборудование российского происхождения». Это уже повторная попытка добавить этот термин в дополнение к нынешнему «оборудованию, произведённому на территории РФ». Будем надеяться, что статус вице-премьера позволит ему довести эту задачу до победного завершения.

ПОКУПАЙТЕ РОССИЙСКОЕ!

Идёт настоящая война старого и нового мира. В этой войне участвует много сторон — каждая со своими интересами: кто-то стремится сохранить прежние отношения с западными вендорами, кто-то — показать уверенный рост импортозамещения, не брезгуя «бумажными» цифрами, а кто-то цинично делает на этом бизнес. Очевидно, что в этих условиях никакая деятельная самоорганизация ИТ-отрасли невозможна. Сильные лоббисты формируют её под свои интересы. Это мы, в частности, видим по деятельности тематических консорциумов ИТ-компаний.

Но самое главное, что тормозит все процессы импортозамещения, — это отсутствие идеологии в форме здорового патриотизма. Типа того

закона, который работает в Америке с 1934 (!) года. Он называется очень просто: «Покупай американское!» Давайте к нашим точно так же относиться! Почему бы нам не сделать великой свою страну?

Потому что когда у тебя нет больших задач, которыми ты «болеешь», ты начинаешь в первую очередь думать о своём кармане. Тогда любое хорошее дело превращается в «свечной заводик», который изготавливает, скажем, «переклеенное» оборудование. Вместо «боевых» партнёрств разработчиков, которые вместе создают прорывную отечественную продукцию, работает принцип: умри ты сегодня, а я завтра. А значит, большая задача никак не решается, потому что она требует объединённых усилий больших людских ресурсов.

МЕЖДУ АЛЬТЕРНАТИВ. СРЕДИННЫЙ ПУТЬ

Где же главная болевая точка? Регулятор должен уйти от парадигмы поддержки локализации к поддержке собственной разработки. Это вопрос выбора «срединного пути» между двух крайних альтернатив. Одна — это локализация. Это тупик. В любой момент всё производство может свернуться, и ты останешься ни с чем. И никакой экспорт в модели локализации не светит, потому что локализуют тебя ровно настолько, насколько это нужно зарубежному вендору из каких-либо, например, логистических соображений.

Вторая крайняя альтернатива — запрет всего зарубежного. Это вариант «бумажного» импортозамещения, для которого достаточно обосновать соответствующие критерии для ИТ-продуктов.

* * *

Срединный путь предполагает, что начинать масштабное импортозамещение надо с аудита ИТ-инфраструктур и анализа рисков. Затем составить план перехода и проанализировать эту дорожную карту, с точки зрения функциональности ИТ-систем. Для того, чего не хватает, с учётом всего существующего и оценок рисков госпрограммы переформируются. Разработчики погружаются в разработки. Интеграторы приступают к внедрениям того, что можно устанавливать в организациях. А экспертные советы — их активность в плане импортозамещения вице-премьер Юрий Борисов поручил усилить — занимаются глубокой экспертизой того, что действительно разработано в России, и какие компетенции надо развивать в первую очередь у отечественных разработчиков.

ПАНДЕМИЯ ПРОТИВ ИНЕРЦИИ

«НЕ НУЖНО ДЕЛАТЬ ВИД, ЧТО ВОЗМОЖНОСТЕЙ НЕТ»

Если исключить фактор «сопротивления изменениям», то тут большая проблема с точки зрения банков — замена ПО. Но, как говорится, нет нерешаемых задач! Всегда есть возможность выстроить план постепенного перехода на отечественную продукцию и его реализовывать, а не приводить из года в год одну и ту же аргументацию против. Тем более что срок эксплуатации ИТ-оборудования составляет 3–5 лет, в течение которых можно провести замену этого оборудования на отечественные аналоги, причём без дополнительных затрат. И не нужно будет делать вид, что никто о такой возможности не знает.

Примером «нерешаемых» проблем могла бы стать тема дистанционной работы банковских сотрудников. Но пандемия вынудила пересмотреть и этот вопрос. Многие банки не только изменили нормативные акты и стандарты организации работы, но и модернизировали ИТ-инфраструктуру, в том числе с использованием отечественного оборудования. Такие процессы идут во многих крупных организациях, например в ЦБ и Сбере. Российское оборудование, в том числе и нашего консорциума, стало частью их инфраструктуры.

Как говорится, «дорогу осилит идущий». Любые ИТ-решения не являются статичными, они постоянно развиваются, тестируются, дорабатываются... Зная эту базу, вполне можно спланировать миграцию банков на отечественные продукты и платформы без разработки с нуля. Кроме того, в 2020 г. стартовала тема сквозных проектов. Их суть в том, что именно конечный потребитель определяет спрос и социальный заказ на разрабатываемую радиоэлектронную продукцию. Минпромторг РФ готов поддерживать такие проекты субсидиями.

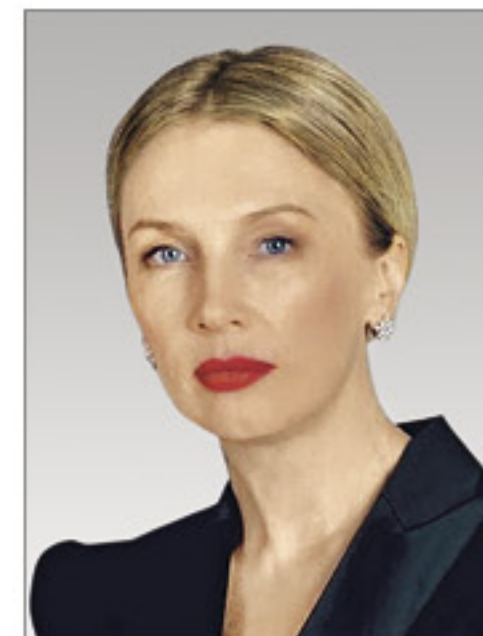
Ещё один аспект системной поддержки стратегии импортозамещения — создание консорциумов поставщиков ИТ-решений. Это актуальный инструмент для развития радиоэлектронной отрасли и реализации политики импортозамещения. В нашем консорциуме на

текущий момент нет отдельной стратегии работы с банками. Однако инициативы консорциума, способствующие увеличению доли рынка российской вычислительной техники, есть результат совместной работы всех его компаний-участников, в том числе обладающих экспертизой в банковском секторе, что позволяет учесть его специфику. Так, консорциум принял активное участие в работе по подготовке Постановления Правительства РФ от 3 декабря 2020 г. № 2013 «О минимальной доле закупок товаров российского происхождения». Нормы квот на закупку отечественной вычислительной техники в наступившем году обязательны для исполнения всеми банками, осуществляющими закупки в соответствии с требованиями 223-ФЗ.

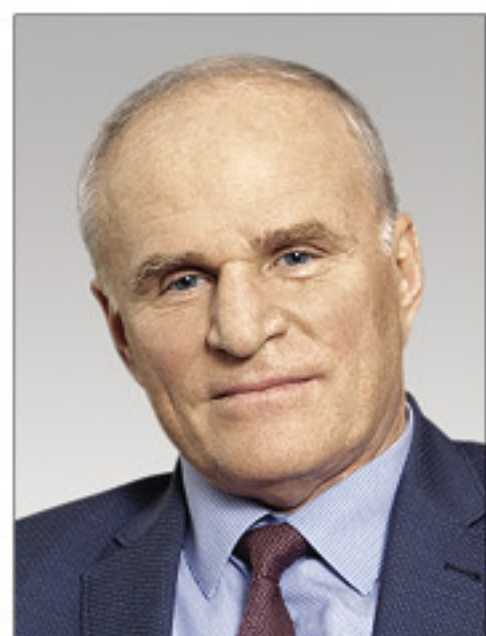
Универсальной стратегии импортозамещения, к сожалению, предложить невозможно. Но что касается банков, то у них уже накоплен богатый опыт внедрений сложных ИТ-продуктов без остановки деятельности. Нет сомнений, что и в случае перехода на отечественные решения можно составить максимально эффективный план этого процесса. Я люблю приводить личный пример. Возглавив консорциум, я стала использовать отечественный компьютер одной из наших компаний. И совершенно ответственно могу сказать: как пользователь не вижу разницы. Даже приобретение российской техники в процессе обновления компьютерного парка для менеджеров банка — это пусть не самый существенный, но уже первый шаг на пути импортозамещения.

* * *

Что касается реальных сроков импортозамещения в той или иной отрасли, то они зависят от всех участников реализации этой политики. От лица отечественных разработчиков вычислительной техники могу сказать, что мы готовы к тестированию и массовым поставкам достаточно широкой номенклатуры продукции.



**Светлана
ЛЕГОСТАЕВА**
генеральный
директор
консорциума
«Вычислительная
техника»



**Григорий
СИЗОНЕНКО**
генеральный
директор группы
компаний ИБК

ПРИМЕРЫ ПРОТИВ СЛОВ

«НЕ СДВИГ СРОКОВ,
А ИНТЕНСИФИКАЦИЯ РАБОТ!»

Сдвигать сроки перехода объектов КИИ на отечественное оборудование и ПО нельзя. Здесь в прямом смысле «промедление смерти подобно». Когда несколько лет назад США и ЕС начали вводить санкции против России, меня удивляла недалёковидность некоторых руководителей, уверенных, что сферы ИТ они не коснутся. Но если несколько лет назад такую недалёковидность можно было списать на отсутствие опыта, то теперь она просто преступна.

Допустим ли такой подход для финансовой сферы? Нет, конечно. Сегодня все внутренние и клиентские сервисы банков построены на цифровых платформах. Если развитием и политикой использования ключевых элементов этих платформ — вычислительной техники и ОС — управляют зарубежные организации, то речи о самостоятельности государственной финансовой системы можно не вести. Разработчики зарубежного ПО и «железа» могут в любой момент отозвать лицензии, запретить доступ к новым версиям продуктов, наложить ограничения на сферы их применения. События с МГТУ им. Н.Э. Баумана — наглядный тому пример.

Вопрос «Что делать?» в этой ситуации, конечно, беспрецедентно запоздал. Начинать действовать надо было годы назад: провести ревизию корпоративных ИТ-ресурсов, составить поэтапный план перехода на российский софт и оборудование, проанализировать и сравнить

предложения российских разработчиков, изучить свойства их продуктов, при необходимости — сформировать технические задания на доработку, составить план поэтапного перехода и приступить к его реализации.

Именно так поступил, например, Сбербанк, следуя распоряжению руководства о миграции на российскую технологическую платформу. ИТ-специалисты банка обратились в ИБК за помощью в разработке системного ПО. Таким образом, у нас появились требования, которые мы выполнили в интересах конкретного заказчика — Сбербанка.

Аналогичным образом построила работу одна из крупнейших энергетических компаний страны. На протяжении двух лет мы совместно реализуем масштабный проект перевода её цифровых ресурсов на российское ПО и отечественные процессоры. Сегодня типовое техническое решение уже сформировано и успешно прошло апробацию на пилотной зоне. Впереди — устранение замечаний и рекомендаций и выход на поэтапное внедрение на всех производственных площадках компании.

В ИБК функционирует демонстрационный стенд, на котором можно увидеть работу всех программных и аппаратных решений «в боевом режиме». Мы готовы оказать поддержку любой организации, которая озаботилась реализацией программы построения технологически независимой цифровой инфраструктуры, программы, которая вносит вклад в обеспечение технологической независимости государства.

Поэтому повторю: сегодня речь должна идти не о сдвиге сроков перевода объектов КИИ на отечественные доверенные программно-аппаратные платформы, а об интенсификации работ в этом направлении.

Когда несколько лет назад США и ЕС начали вводить санкции против России, меня удивляла недалёковидность некоторых руководителей, уверенных, что сферы информационных технологий они не коснутся

ДАВАЙТЕ ВСПОМНИМ ПРО ЕГИПЕТ

«ПРИ РЕАЛИЗАЦИИ ПРОГРАММЫ ГЛАВНЫМ УЧАСТНИКОМ ЯВЛЯЕТСЯ ЗАКАЗЧИК, В ДАННОМ СЛУЧАЕ БАНК»

Модернизация банковской ИТ-инфраструктуры в разрезе импортозамещения, по нашему мнению, должна идти в двух направлениях. Первое — это постепенная замена аппаратной части стандартных серверов, например серверов, используемых для front-end-операций. Такие сервера российского производства широко представлены на рынке, и по своим техническим характеристикам они ничем не отличаются от зарубежных аналогов. Это импортозамещение вполне возможно реализовать в рамках и в сроки текущих программ банков по замене оборудования. То есть при замене оборудования закупить не американское, а отечественное, которое уже оттестировано и отлично зарекомендовало себя в работе front-end-систем.

Второе и самое сложное направление — это замена серьёзных программно-аппаратных комплексов (ПАК), например тех, которые обрабатывают «тяжёлые» базы данных. Тут необходимо тесное взаимодействие ИТ-служб банков, разработчиков и производителей электроники. ИТ-директорам банков нужно выработать технические требования, активно участвовать в процессе разработки, обеспечить боевое тестирование продуктов. Сроки этого этапа, конечно, больше. Разработка и внедрение серьёзного аппаратного комплекса на заказ — это вопрос не одного года. Но уложиться в три года можно вполне.

Иными словами, при реализации программы импортозамещения основной участник — не производитель или разработчик и даже не государство, а заказчик, в данном случае банк. В этом случае у банковских ИТ-служб не будет боязни, что какое-либо отечественное решение «положит» всю банковскую систему. Да и номенклатура российских решений увеличится в разы.

В этой части хорошо работает механизм консорциумов — они призваны увеличить долю российских производителей на отечественном

ИТ-рынке, используя инструменты, которые дали им Минцифры и Минпромторг. Вспомним, что именно при помощи консорциумов производителям аппаратных платформ удалось реализовать и успешно поставлять решения, подходящие под «закон Яровой» в телеком-компаниях. И сегодня консорциумы вычислительной техники и разработчиков и производителей электроники активно участвуют в разработке критериев для отечественной продукции.

Существует миф, что «всё, что отечественное, — либо дорогое, либо некачественно». И это действительно миф. Если говорить о ценах, то, например, серверы, которые мы разрабатываем и производим, гораздо ниже по стоимости аналогичного оборудования ведущих мировых брендов. При этом завод оснащён роботизированным оборудованием, точно таким же, которое стоит на заводах компаний Dell, Lenovo и т.д. Оборудование собирается на линии, где полностью отсутствует ручной труд, что гарантирует качество производимой продукции.

* * *

Остаётся ли при этом место для зарубежной продукции, например, в виде доверенного оборудования? Доверенным считается ИТ-решение, проверенное специальными службами на предмет закладок, удалённого доступа и т.д. Да, возможно. В некритичных сегментах ИТ-среды можно использовать такие решения. Но давайте вспомним ситуацию во время напряжённости в Египте, когда уважаемый международный ИТ-производитель в одну секунду отключил целую страну от внешнего доступа в сеть. ИТ-среда — это не ресторан, где мы доверяем блюду, приготовленному не тобой лично. Если ты не имеешь доступа к документации и не знаешь всех нюансов оборудования, которое используешь в своих системах, то всегда есть риск «отравиться».



Борис ИВАНОВ
вице-президент
по развитию
компания «Рикор»

А ЕСТЬ ЛИ ПРОБЛЕМА?

«СПОСОБЫ СНИЖЕНИЯ РИСКОВ ИБ НЕ ЗАВИСЯТ ОТ ТОГО, ОТЕЧЕСТВЕННОЕ ИЛИ ЗАРУБЕЖНОЕ ОБОРУДОВАНИЕ И ПО ИСПОЛЬЗУЕТСЯ В БАНКЕ»



Сергей НЕЙГЕР
менеджер
по развитию
бизнеса компании
«Перспективный
мониторинг»

Как это часто бывает, многие участники рынка — и вендоры, и пользователи — по вопросу импортозамещения ИТ в банковском секторе разделились на три лагеря. Первые поддерживают позицию «Импортозамещение из принципа! Любой ценой!», вторые отрицают необходимость самого перехода на отечественные ИТ, а третьи стараются оценивать политические, технологические риски и риски безопасности и снижать их уровень. Последний подход видится наиболее взвешенным и учитывающим интересы отрасли.

Существует риск «импортозависимости», который можно описать как «Сможем ли мы приобрести, обновить и обеспечить непрерывность деятельности, если иностранный вендор прекратит поддержку своего продукта?» И здесь кто-то пытается риск снизить путём замены на отечественную продукцию (или дружественных государств), а кто-то принимает эти риски в надежде, что если это произойдёт, то будут придуманы различные «костыли» к функционированию продукта и сложные схемы в цепочках закупки, опять-таки через дружественные государства.

Технологические риски связаны в основном с отсутствием выбора информационных технологий. Такой риск описывается словами «Сможем ли мы найти аналог, и будет ли он выполнять все требуемые функции?» Но и тут есть варианты. Можно приобретать ИТ у более «дружественных» с точки зрения государства зарубежных поставщиков или у отечественных разработчиков. А можно адаптировать решения open source, хотя в последнем случае совокупная стоимость владения может оказаться выше, чем для проприетарных решений. Все эти варианты вызывают экономические риски в виде дополнительных затрат.

Способы снижения рисков информационной безопасности не зависят от того, отечественное или зарубежное оборудование и программное обеспечение используется в финансовой организации. Мы в любом случае рекомендуем проводить поиск недеklarированных возможностей (стоит отметить, что вероятность преднамеренных закладок в отечественном софте всё-таки считается меньшей), анализ защищённости аппаратных и программных решений и тестирование на проникновение. Благодаря такому подходу можно отвязаться от страны происхождения ИТ и минимизировать риски использования конкретных продуктов.

Исследования безопасности помогают предотвратить четыре главные опасности для защищаемой информации предприятия:

- ◆ Ошибки программирования, которые не только препятствуют нормальной работе приложений (зависания, BSOD, потеря данных), но и «приглашают» злоумышленника ими воспользоваться.
- ◆ Расширение функциональных возможностей приложений в ущерб безопасности. Разработчики — неважно, российские или нет — используют наиболее простые (но не безопасные!) приёмы в погоне за сроками и удобством.
- ◆ Встраивание функций, которые делают возможным обход механизмов защиты. Разработчики ПО оставляют такие функции для облегчения тестирования и отладки приложений, но забывают их отключить в финальной версии.
- ◆ Программные закладки, которые умышленно встраиваются в исходный код приложений или в обновления ПО и используются для получения несанкционированного доступа к информации или других вредоносных действий. В исходный код закладки встраивает либо сам разработчик, либо атаковавший его злоумышленник.

ОТ РЕДАКЦИИ

К сожалению, публикацию мнений по разным аспектам импортозамещения на этой неожиданной ноте приходится остановить. Только-только, казалось бы, становится понятным образ слаломиста (на обложке), лавирующего между камней. Но... остановиться всё-таки надо, ведь главную задачу мы выполнили — картина видения профессиональным сообществом данной темы на начало 2021 года зафиксирована.

Ситуация с импортозамещением в банковском секторе, как мы видим, предельно непростая: за одним уровнем открывается другой, ещё более глубокий, и на каждом — свои действующие лица со своими целями, задачами и интересами. И 2021-й год в этом отношении, безусловно, будет гораздо более насыщенным, динамичным и захватывающим, чем 2020-й. Впереди ещё не один крутой поворот.



Твоя сеть. Твои правила.

Гибкая защита — для растущего бизнеса.

Kaspersky Endpoint Security для бизнеса Универсальный защитит виртуальные и физические рабочие места в любом их соотношении и поддержит ваши планы по развитию корпоративной IT-инфраструктуры.



**Kaspersky
Endpoint Security
для бизнеса
Универсальный**

kaspersky

**АКТИВИРУЙ
БУДУЩЕЕ**

© АО «Лаборатория Касперского», 2020.
Зарегистрированные товарные знаки и знаки обслуживания
являются собственностью их правообладателей.

ДиалОгНаука

**СИСТЕМНАЯ ИНТЕГРАЦИЯ В ОБЛАСТИ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

dialognauka.ru

KASPERSKY.RU/BUSINESS



Анатолий АКСАКОВ
председатель Комитета
Государственной думы РФ
по финансовому рынку

ДОБРО ПОЖАЛОВАТЬ В НОВУЮ — ЦИФРОВУЮ — ФИНАНСОВУЮ РЕАЛЬНОСТЬ

ПРИНЯТ ПАКЕТ ФЕДЕРАЛЬНЫХ ЗАКОНОВ, СИСТЕМНО
ОБЕСПЕЧИВАЮЩИХ БЕЗОПАСНУЮ ЦИФРОВИЗАЦИЮ
ФИНАНСОВОГО РЫНКА

В минувшем 2020 году было принято несколько важных федеральных законодательных актов, направленных на цифровизацию финансовой сферы. В том числе о цифровых активах, о маркетплейсе, о расширении возможностей использования биометрических данных. На очереди криптовалюты и цифровой рубль.

ЦИФРОВЫЕ АКТИВЫ И МАРКЕТПЛЕЙС

Прежде всего, был принят базовый для развития цифровой экономики Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31 июля 2020 года № 259-ФЗ. С 1 января 2021 года дан старт работе с новыми цифровыми финансовыми инструментами.

Этого давно ждал весь рынок, многие представители бизнеса, особенно сырьевые компании, обращались с просьбами, чтобы мы побыстрее приняли закон. Наконец создана правовая возможность, чтобы наши организации могли выпускать и продавать цифровые финансовые активы (ЦФА), привлекать инвестиции с помощью этого нового инструмента. Закон даёт основу для правовой защиты таких инвестиций, в том числе в судах.

Поэтому полагаю, что с начала 2021 года в стране начнётся масштабный выпуск ЦФА. Во всяком случае, по моим данным, многие крупные компании уже собираются выпускать свои стейблкоины (криптовалюту, стоимость которой привязана к ценному материалу). При этом закон прямо говорит, что цифровая валюта не может быть использована в качестве средства для оплаты услуг или товаров.

Также принят Федеральный закон «О совершении финансовых сделок с использованием финансовой платформы» от 20 июля 2020 года № 211-ФЗ, то есть о маркетплейсе. Тем самым созданы правовые возможности для граждан получать различные финансовые услуги удалённо с помощью электронных платформ.

Этот закон, кроме того, повышает конкуренцию в финансовом секторе за счёт выравнивания условий для крупных и небольших участников (небольшие финансовые организации смогут с помощью новой инфраструктуры преодолеть технологическое отставание от лидеров рынка).

Необходимо отметить, что недавно в Госдуму РФ внесён законопроект, направленный на дальнейшее совершенствование указанного закона о маркетплейсе. И теперь, опираясь на этот закон, юридические лица, в том числе субъекты малого и среднего бизнеса, а также ИП, также смогут получать соответствующие услуги удалённо.

ЕДИНАЯ БИОМЕТРИЯ

На последней в ушедшем году пленарной неделе Госдума РФ приняла Федеральный закон от 29 декабря 2020 года № 479-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации». Он направлен на расширение возможностей использования Единой биометрической системы (ЕБС) для удалённого оказания финансовых услуг.

Закон крайне важный и актуальный, поскольку развитие дистанционной идентификации для оказания услуг — очевидное требование времени, особенно с учётом продолжающейся пандемии коронавирусной инфекции. Рассмотрение закона растянулось на два года из-за многочисленных



согласований с министерствами и ведомствами, поскольку обеспечение сбора биометрических персональных данных требует уверенности в максимальной защите персональных данных граждан.

Первоначально он касался использования биометрии только при открытии банковского счёта или вклада. Однако во втором чтении было решено распространить это на весь спектр финансовых услуг. Кроме того, биометрические данные теперь можно будет использовать и при оказании государственных и муниципальных услуг.

ЕБС будет теперь иметь статус государственной информационной системы. Количество «пунктов» сбора биометрической информации вырастет за счёт многофункциональных центров (МФЦ). Банк России наделяется правом устанавливать, каковы условия сбора биометрии в ЕБС, в зависимости от видов банковских подразделений (операционные кассы, отделения и т.д.). Банки с базовой лицензией теперь получают право, а не обязанность собирать биометрические данные в ЕБС.

Помимо ЕБС законопроект разрешает использовать и коммерческие биометрические системы. Закон содержит положение об обязанности владельцев коммерческих биометрических систем передавать данные в ЕБС. В целях обеспечения безопасности в законопроекте предусмотрен механизм аккредитации коммерческих биометрических систем.

Что касается контрольно-надзорных полномочий, то их будут осуществлять Банк России, ФСБ России, ФСТЭК России и Роскомнадзор. Закон о биометрии заработает уже в 2021 году. Использование биометрических данных позволит

сделать доступными банковские услуги для людей из удалённых регионов, где выбор ограничен или вовсе отсутствует, а также для маломобильных групп граждан.

БУДУЩЕЕ ЦИФРОВОГО РУБЛЯ

В принципе, Россия готова к цифровому рублю, создана правовая основа для его выпуска. Принят закон о цифровых финансовых активах, кроме того, достигнут довольно высокий уровень развития финансовых технологий и их проникновения.

По данным Банка России, уже в 2019 году доля россиян, для которых дистанционный доступ к банковским счетам для совершения переводов стал обычной практикой, составила около 55 %. В 2020 году в условиях пандемии доля таких переводов тем более возросла.

Кроме того, удельный вес безналичных платежей за товары и услуги в российской розничной торговле, общепите и платных услугах населению за последние три года выросла почти в два раза. Само общество постоянно формирует запрос на повышение скорости, удобства, безопасности транзакций и использование современных технологий. И это делает актуальным вопрос о выпуске цифровой валюты.

В опубликованном прошлой осенью докладе Банка России о цифровом рубле представлен ряд возможных вариантов реализации такого решения, а также функциональные требования. Этот доклад даёт основу для обсуждений с экспертами, финансовым сектором и обществом в целом.

На базе Комитета Госдумы по финансовому рынку проблематика цифровых валют обсуждается уже довольно давно. В частности, 21 декабря 2020 года этот вопрос обсуждался в



Государственной думе РФ на круглом столе «Цифровой рубль. Новые возможности для граждан, бизнеса и государства».

Введение цифрового рубля потребует законодательных изменений. Нам необходимо понять, что нам надо будет поменять в законодательстве для того, чтобы цифровой рубль мог активно войти в нашу жизнь. Вносить изменения придётся прежде всего в Гражданский кодекс РФ — в части включения цифрового рубля в перечень объектов гражданских прав, установления возможности осуществления платежей в цифровой валюте центрального банка, включения цифрового рубля в общие положения о расчётах.

Также потребуются изменения в Федеральном законе «О Центральном банке Российской Федерации (Банке

России)» 10 июля 2002 года № 86-ФЗ — о расширении функций Банка России, определении вопросов выпуска и обращения цифровой валюты. Важно также решить правовые вопросы использования цифровой валюты Банка России, если технологическая и операционная инфраструктура будет создаваться регулятором с включением кредитных организаций и, возможно, иных финансовых посредников.

Здесь особое значение приобретает установление и распределение ответственности за устойчивость и непрерывность деятельности информационной системы, в рамках которой будет осуществляться обращение цифровой валюты Центрального банка.

ТРЕТЬЯ ФОРМА ДЕНЕГ

Цифровой рубль — это третья форма денег: сочетает свойства наличных и безналичных средств. Есть и отличия: например, возможность офлайн-платежей без доступа к сети Интернет на всей территории страны. Но чтобы реализовать офлайн-платежи цифровым рублём, придётся создавать специальные технологии и инфраструктуру.

В отличие от «криптовалют», цифровой рубль — равноценная форма национальной валюты, и её устойчивое функционирование в интересах граждан и бизнеса обеспечивается государством в лице Банка России, их доверием к уже существующей национальной валюте.

Цифровой рубль будет доступен всем субъектам экономики — гражданам, бизнесу, участникам финансового рынка и государству для осуществления платежей и расчётов. Он будет храниться на индивидуальных электронных кошельках, открытых непосредственно в платёжной системе Банка России и являющихся его обязательствами.

Создание цифрового рубля будет способствовать цифровизации финансового рынка и экономики в целом, его внедрение снизит для граждан и бизнеса издержки для расчётов платежей.

Решение о выпуске цифрового рубля ещё не принято, поэтому говорить о тех или иных сроках его внедрения ещё рано. Однако полагаю, что тестирование цифрового рубля в экспериментальном режиме может начаться уже в 2021 году. В частности, считаю, что использование цифрового рубля может быть в пилотном варианте опробовано в Крыму для преодоления санкционных ограничений.

Очевидно, что все понимают неизбежность реализации этой идеи. И важно, чтобы она очень эффективно вошла в нашу жизнь. С моей точки зрения, цифровой рубль — это обязательное будущее нашего денежного обращения, это будущее российской экономики.

ОСОБЕННОСТИ КРИПТОВАЛЮТ

Правительство планирует направить развитие этого рынка в цивилизованное русло, чтобы владельцы таких активов могли защитить свои права и интересы, а создание теневых схем было затруднено.

Сейчас на рассмотрении в Госдуме РФ находится законопроект, вносящий поправки в Налоговый кодекс. В нём предлагается признать цифровую валюту имуществом и распространить на её владельцев соответствующие права и обязанности. В частности, они могут рассчитывать на юридическую защиту в случае каких-либо противоправных действий, а также отстаивать свои имущественные права в суде.

Появление законопроекта связано с тем, что всё больше наших граждан активно используют криптовалюту. Поэтому мы должны, во-первых, закрепить имущественные права. Тогда криптовалюта как некая ценность в случае смерти человека будет переходить к его наследникам. А во-вторых, решить вопрос налогообложения.

Для многих криптовалюта — это высокодоходный бизнес. Поэтому вполне логично будет собирать с неё налоги — так же как с любых других видов предпринимательской деятельности. Однако для этого необходимо легализовать

цифровые деньги и закрепить все необходимые аспекты в законодательстве.

Согласно внесённому законопроекту, все граждане России, иностранцы, постоянно проживающие в стране на основании вида на жительство, а также компании и организации, распоряжающиеся криптовалютой, обязаны будут отчитываться в налоговый орган.

Норма будет касаться всех, на чьих электронных кошельках движение средств за календарный год превышает сумму, эквивалентную 600 тысячам рублей. А для нарушителей установят налоговую ответственность.

Им грозят штрафы в размере 40 % от суммы неуплаченного налога. За недекларирование и подачу неправильных сведений об операциях с криптовалютой предусмотрен штраф в размере 10 % от этих операций.

В законопроекте об изменении Налогового кодекса и законе о цифровых финансовых активах не описано, как, например, доказывать факт покупки криптовалюты. Также не ясно, будут ли действовать налоговые вычеты и норма об освобождении от уплаты налогов при владении криптовалютой более трёх лет. Эти вопросы предстоит решить при подготовке указанного законопроекта ко второму чтению.

БЕЗОПАСНОСТЬ НОВЫХ РЕАЛИЙ

При этом важно отметить, что цифровые технологии несут не только новые возможности, но и новые риски. Риски при внедрении новых технологий есть всегда. Всё новое — это всегда риск безопасности. В финансовой сфере риски особенно чувствительны, поскольку связаны с возможной потерей финансовых средств.

Главное требование в таких случаях — это аккредитация соответствующих организаций и оборудования ФСБ России. Это ведомство обеспечивает нам высокий уровень безопасности. Хочу также напомнить, что у ФНС России, которая в своей работе активно использует цифровые технологии, не было ни одной утечки.

Внедрение ЦФА повышает риски проведения незаконных операций, в том числе с использованием доходов, полученных преступным путём. Специфика рынка ЦФА обуславливает и регуляторные запреты, ведь некоторые участники стараются оставаться анонимными, используя техники отмывания денег.

В 2020 году ФАТФ выпустила доклад «Виртуальные активы — красные флажки для отмывания денег и финансирования терроризма». Он включает рекомендации участникам рынка, которые позволяют избежать правовых рисков при работе с ЦФА (это оценка объёма транзакций и их моделей, проверка профиля отправителя и получателя, географических рисков и т.д.).

Не стоит забывать и о рисках «цифры» для финансового рынка, например, цифровых пирамидах. Справиться с ними поможет соблюдение требований информационной безопасности.



Вадим УВАРОВ
директор Департамента
информационной
безопасности Банка России

ПРИЦЕЛ ОБУЧЕНИЯ — ПРАКТИКА

УНИВЕРСИТЕТ БАНКА РОССИИ НАЧАЛ ПРАКТИКО-ОРИЕНТИРОВАННОЕ ОБУЧЕНИЕ СПЕЦИАЛИСТОВ ИБ

Необходимость обучения информационной безопасности отраслевых специалистов со стороны Банка России возникла в связи с современными реалиями. Сейчас доступ ко многим финансовым услугам имеет любой человек, у которого есть мобильное устройство — гаджет и выход в интернет.

ОРИЕНТАЦИЯ НА ПРАКТИКУ

Процесс цифровизации финансового сектора в России происходит стремительно. Однако у этого позитивного явления есть и обратная сторона: любые новые технологии несут и новые риски.

И Банк России, и правоохранительные органы, и финансовые организации — вообще все, кто так или иначе сталкивается с обеспечением кибербезопасности, — отмечают рост преступности в этой сфере.

Чтобы успешно противостоять злоумышленникам, необходимо, во-первых, поддерживать и актуализировать свои знания в сфере обеспечения кибербезопасности, во-вторых, налаживать межведомственное взаимодействие. Чтобы решить эти две задачи, Банк России запустил масштабное практико-ориентированное обучение.

Отличие от повышения квалификации, проводимого учебными организациями, в том, что Банк России не является образовательной организацией, не имеет образовательной лицензии. Запуская проекты, направленные на повышение профессиональных компетенций специалистов финансового рынка или организаций, чья деятельность связана с ним, мы тем самым способствуем его развитию.

В случае с практико-ориентированным обучением мы преследуем глобальную цель — снизить уровень киберпреступлений через повышение квалификации специалистов по ИБ, а также тех, кто эти преступления предотвращает.

ФОРМАТ КУРСА

Учебный курс состоит из пяти блоков, адаптированных под разные целевые аудитории: работники Банка России, сотрудники правоохранительных органов, преподаватели вузов, специалисты кредитно-финансовой сферы и организаций цифровой экономики. Мы гибко подходим к проектированию программы, внимательно отслеживаем обратную связь, вопросы слушателей, добавляем или корректируем содержание лекций.

Учебный курс продолжительный, составляет почти три месяца. Это долгий срок для общения с целевой аудиторией, и есть возможность максимально удовлетворить потребность в конкретных знаниях.

Формат учебного курса Банка России отличается от программ профильных обучающих организаций. Наш учебный курс — «практико-ориентированное обучение» — в первую очередь реализует стратегию обучения pull («проталкивания»). Сама целевая аудитория осознаёт необходимость определённых знаний и навыков для ежедневного применения в работе.

Программы профильных обучающих организаций, на наш взгляд, более академичны. Кроме того, наше обучение в том числе направлено на налаживание межведомственного взаимодействия, обмен опытом с коллегами, что, мы уверены, будет иметь синергетический эффект по результатам его проведения.

ПРЕПОДАЮТ ПРАКТИКИ

В обучении используются практические примеры, инциденты и меры реагирования на них. Большая часть учебного процесса посвящена разбору конкретных примеров киберпреступлений, в том числе в финансовых организациях. Что важно — лектор не будет просто рассказывать, что и как было, слушатели будут непосредственно вовлечены в разбор конкретных кейсов.



Для нас большое значение имеет коммуникация, так как и преподаватели, и аудитория — это профессионалы, у каждого из них есть свой опыт, свои мысли, которыми, по нашей задумке, они будут делиться, дискутировать друг с другом. В споре рождается истина.

Преподавать приглашаются лучшие профессионалы в сфере обеспечения информационной безопасности. Это как представители частных организаций, работающих в сфере ИБ, в финансовой сфере, так и сотрудники государственных структур.

К ЕЖЕГОДНОЙ РЕГУЛЯРНОСТИ

После проведения всех пяти блоков программы (до конца 2021 года) есть планы перевести курс в ежегодный регулярный формат. Потребность в обучении участников большая, например, сейчас мы охватили почти тысячу сотрудников правоохранительных органов, но уже видим запрос на обучение ещё 1 500 человек. Это явный сигнал для перевода курса в регулярный, полагаем, ежегодный формат.

Лекции проводятся в два потока из-за большого числа слушателей и для обеспечения бесперебойности (с технической точки зрения). После каждой лекции осуществляется обратная связь в форме анкетирования, отражающего оценки по содержанию программы обучения в целом, мотивации участников обучения, организации обучения и работе наших спикеров. Анкеты анализируются, с учётом комментариев мы рассматриваем возможность добавления новых, факультативных тем по запросу слушателей.

Во внутреннем обучении приняли участие 1500 сотрудников Банка России из всех регионов. Обратная связь с участниками осуществлялась по итогам каждой лекции, имеет преимущественно положительный контекст.

Большая часть учебного процесса посвящена разбору конкретных примеров киберпреступлений, в том числе в финансовых организациях

ТЕСТИРОВАНИЕ И СЕРТИФИКАТЫ

Итоговое тестирование предполагается, но носит рекомендательный характер. В большей степени для самопроверки понимания материала слушателями, а также в целях корректировки нами образовательной составляющей. Мы создали базу знаний для всех прошедших обучение в формате видеозаписей, вебинаров и материалов спикеров, участники в любое удобное время могут обратиться к ним.

По итогам тестирования предполагается выдача сертификатов как об успешном прохождении тестирования, так и об участии в практико-ориентированном обучении.

Сертификат Университета Банка России по результатам обучения не является свидетельством о повышении квалификации и не даёт официальный допуск к той или иной деятельности. Обучаем ради получения конкретных знаний, которые можно применять на практике.

Главное и бесспорное преимущество обучения — овладение уникальными знаниями из достоверных, компетентных источников, онлайн-доступ к учебным материалам. В процессе обучения происходит широкий обмен опытом с лучшими специалистами, налаживается межведомственное взаимодействие.



**Екатерина
РАЧКОВА
(КАЛАШНИКОВА)**
эксперт BIS Journal,
заместитель
начальника
Управления
по обеспечению ИБ
Банка ВТБ (ПАО)

ЗАСТАВЬТЕ КЛИЕНТА ПОРАБОТАТЬ

ПЕРЕНОС РИСКОВ ИБ НА КЛИЕНТОВ —
ЛЕНЬ, ХИТРОСТЬ ИЛИ НЕОБХОДИМОСТЬ?

На текущем этапе развития цифровизации общества, информационные технологии стали настолько технически сложными, разнообразными, повсеместными и всепроникающими, их влияние на нашу жизнь и все виды деятельности, наша зависимость от них уже настолько велики, что по аналогии с автомобилями услуги и процессы, использующие такие технологии, уже вполне можно считать средствами повышенной опасности. При этом все мы понимаем, что обходиться без них, как и без транспортных средств, общество уже не может и не готово.

ПО АНАЛОГИИ С АВТОМОБИЛЕМ

Продолжим аналогию с автомобилем. Производители долгое время наращивали уровень надёжности техники (двигателя, коробки передач, подвески, бортовых систем и т.д.), поскольку её сбой в значительном числе случаев становился причиной аварии, и вышли в этой части неантропогенных уязвимостей на некоторое довольно высокое плато, после чего взялись за оставшуюся составляющую факторов риска — антропогенную. Активно стали развиваться системы ограничения скорости, ведения в полосе и, наконец, автопилотирования.

Примерно по такой же схеме шло развитие обеспечения информационной безопасности. Если коротко — были выделены основные направления защиты и задачи по их реализации, которые по максимуму постарались взять на себя поставщики услуг (кредитно-финансовые организации и др.), но абсолютно исключить влияние человека (клиента — потребителя услуг) на результат не удалось. И в текущей концептуальной парадигме обеспечения информационной безопасности вряд ли удастся, поскольку невозможно вывести за скобки вопросы аутентификации.

Невозможно быть уверенным и нести ответственность за результат в среде, над которой нет контроля. А контролировать клиента и его внимательность, осторожность и аккуратность в обращении с факторами аутентификации невозможно.

Можно объяснять, что надо и не надо делать. Нельзя делать паролем легко вычисляемые сочетания, нельзя сообщать пароль или cvv-код карты

приятелю «потому что вот прямо сейчас очень надо успеть купить что-то там на распродаже», нельзя по той же причине непонятно куда и как отсылать фото паспорта, водительских прав и той же карты во всех ракурсах, сохранять «на доверенных» устройствах логины, пароли, настраивать автоматический вход в какой-нибудь банковский личный кабинет, а потом давать это устройство ребёнку в школу, например. Нельзя не смотреть, по какому адресу ссылки осуществляется переход, с какого адреса (а не алиаса) пришло электронное письмо, с какого номера телефона звонят, представляясь работником банка. Происходят такие случаи регулярно, как аргумент приводится «вроде было похоже, вот я и...», а в понимании клиента виноват поставщик услуг (вероятно, в том, что не поместил клиента в металлический шар на дно моря), и каким-то образом он, поставщик, должен вернуть всё как было за его счёт.

А с автомобилем происходит совсем не так. Клиент в данном случае — водитель. И за то, что он проехал под запрещающий знак или пересёк двойную сплошную, оштрафуют или лишат прав управления транспортным средством именно его, а не автодилера или производителя автомобиля (даже если водитель использовал автопилот). И это нормально, никто такой практике не удивляется. Возможно, здесь играет роль больший накопленный опыт законотворчества и судебной практики в автотранспортной отрасли. А может быть, и тот факт, что допуск к управлению автомобилем (да ещё и определённой категории) осуществляется после нескольких месяцев обучения правилам и практике его эксплуатации, после сдачи экзамена.

Интересно было бы представить допуск к взятию кредита или подключению к онлайн-банку после курса информационной безопасности и тестирования, а также «полевых» испытаний?

Вряд ли мы в обозримом будущем, конечно, такое увидим в обязательном порядке, но на добровольной основе — почему не предоставить возможность тем, у кого в этом есть потребность, прослушать курс онлайн-лекций и пройти тест, поучаствовать в вебинаре с возможностью задать вопросы хотя бы в ограниченном количестве, а не прочитать сухую памятку о безопасности на

сайте, зачастую сложную для понимания без обратной связи для человека неподготовленного. Чем это не забота о клиентах, не инвестиция в их лояльность и, хоть и в отдалённой перспективе, в уменьшение числа инцидентов, повлёкших за собой финансовые потери, которые (в зависимости от того, чью сторону примет суд), ещё неизвестно, какой стороне придётся возмещать.

А что лучше всего стимулирует человека к более ответственному поведению, обращению с чувствительной информацией, соблюдению установленных правил, как не прямое и явное указание на то, что при доказанном несоблюдении правил клиентом поставщик услуг ответственность за результат не несёт? Смирилось же общество с такими «правилами игры» на рынке страхования, и продукты данного рынка от этого менее востребованными не стали. Скорее даже наоборот, понимание открытости в таких вопросах поставщика услуг перед клиентом, прозрачность картины рисков, желание представить реальную ситуацию (в которой всегда есть плюсы и минусы), а не приукрасить её (ради того, чтобы навязать продукт), может найти у клиента положительный отклик, повысить репутацию поставщика как благонадёжного и честного. Подобная оценка вообще характерна для общества, в котором изобилует информация, а наибольшую ценность представляет информация достоверная.

Конечно же, не предлагается сделать спасение утопающих делом рук самих утопающих. Только открыто сообщать и акцентировать внимание клиентов на том, в каких границах лежит их роль и ответственность в процессах обеспечения информационной безопасности и какими последствиями им может грозить пренебрежение этой ответственностью. При необходимости давать возможность научиться нести эту ответственность, повысить техническую грамотность.

ЭТО ВСЁ «ЛИРИКА». А СОВЕТЫ БУДУТ?

Советов будет даже два.

Первый: сделайте клиента — дилетанта в области обеспечения информационной безопасности — полноценным участником сложной и дорогостоящей деятельности по защите информации и чётко выделите зону его единоличной персональной ответственности. Энтузиазм, обусловленный осознанием цены собственной небрежности в отношении своих чувствительных данных и денежных средств, в какой-то мере нивелирует недостаток опыта и каких-то специфических знаний.

Второй: чтобы получить лояльность клиента, убедите его поработать на безопасность его собственных данных и средств. Ничто так не

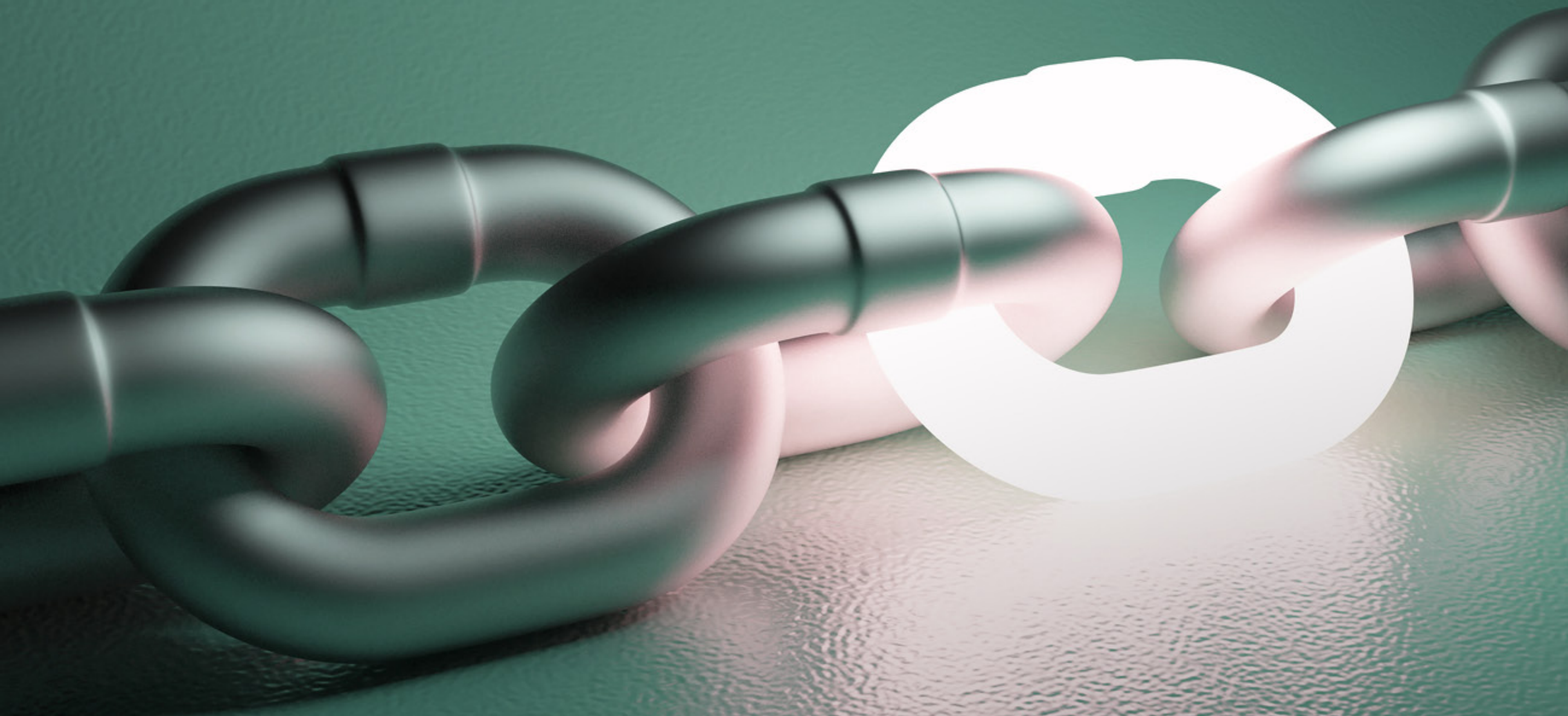
добавляет ценности продукту в глазах человека, как вложенные в этот продукт его собственные усилия. Кроме того, вынужденно вникнув хотя бы на общем уровне в те меры, которые принимаются для защиты данных, клиент в более полной мере сможет оценить качество и надёжность предоставляемой ему услуги.

А РЕГУЛЯТОР ДОПУСКАЕТ ПОДОБНУЮ СТРАТЕГИЮ?

Конечно, даже более жёсткую. Вспомним пункт 2.10.5 уходящего от нас Положения Банка России от 9 июня 2012 года № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств», в котором, говоря простым языком, если оператор по переводу денежных средств не может или не хочет переписывать своё ПО или клиент не может или не хочет использовать два устройства для формирования и подтверждения перевода денежных средств, то клиенту просто предлагается по своему усмотрению определить, какие суммы он согласен переводить без таких мер предосторожности на свой страх и риск, и зафиксировать это в договоре.

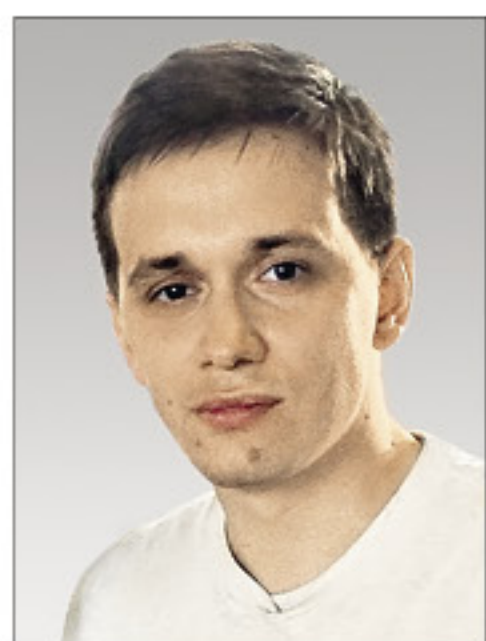
* * *

Использование дистанционных финансовых сервисов в настоящее время можно сравнить с вождением автомобиля. Как известно, снизить риски, связанные с ДТП, можно не только совершенствуя пассивную и активную безопасность с последующим увеличением стоимости или вводя неудобные для пользователя ограничения по мощности двигателя, скорости, ремни безопасности и пр., но и уделяя время обучению водителей. Вложение в просвещение пользователей может быть также (или более) эффективно для снижения рисков, как и вложение в средства безопасности, контроля действий пользователей, и поможет расширить область допустимого использования информационных технологий. В частности, одна из причин недостаточной безопасности сервисов — непонимание клиентами рисков, связанных с их использованием. Очень часто клиенты выбирают низкую стоимость и удобство в ущерб безопасности. А поставщики финансовых услуг идут у них на поводу — сокращают офисы, упрощают аутентификацию, отказываются от дополнительного подтверждения подозрительных операций.



БЕЗ ШВОВ

КАК РЕШИТЬ ГЛАВНУЮ ПРОБЛЕМУ ДЛЯ КОРПОРАТИВНЫХ БЛОКЧЕЙН-РЕШЕНИЙ



Илья ДРУЖИНИН
аналитик-исследователь
в Ассоциации
ФинТех, руководитель
рабочей группы № 5
«Взаимодействие
систем
распределённого
реестра» в ТК 159

Технология распределённого реестра (ТРР), или блокчейн, находится на стадии перехода от НИОКР к промышленному внедрению в корпорациях из различных отраслей. Только в России, по данным Mindsmith, более 40 российских организаций публично заявили о внедрении блокчейна в свой бизнес. Этот процесс крайне неоднороден: отличаются подходы к внедрению, используемые платформы, сферы применения. Пока корпоративные системы с использованием ТРР чаще всего замкнуты внутри одной компании.

В то же время наибольший потенциал технологии кроется как раз в возможности создания среды для обмена информацией между разными участниками. И в будущем главным вызовом для ТРР станет обеспечение

функциональной совместимости, или интероперабельности, систем, построенных на разных блокчейн-платформах.

Потребность в интероперабельности будет возрастать с увеличением количества корпоративных блокчейн-сетей. В этом году, со вступлением в силу закона о цифровых финансовых активах (ЦФА), появятся несколько новых информационных систем на базе распределённого реестра, и рынку потребуется обеспечить безопасное и бесшовное взаимодействие платформ для передачи ЦФА между этими информационными системами и сетями. И подготовка стандартизированных подходов к интероперабельности — необходимый шаг для передачи ЦФА между гетерогенными платформами, например «Мастерчейн» и Hyperledger Fabric.

Сложность «бесшовного» объединения корпоративных информационных систем на основе распределённых реестров состоит в разнородности платформ, которые выступают базой для реализации корпоративных информационных систем. Различные блокчейн-платформы привыкли «общаться» по своим правилам, и разработчикам предстоит научить свои платформы «разговаривать» на одном языке и при этом сохранить технологические особенности, ради которых эти платформы были выбраны. Для этого нужен общий протокол, который бы помог организовать взаимодействие платформ для отправки и получения ценной информации из одной сети в другую.

Сегодня в мире разрабатывается ряд проектов по интероперабельности. Работу над ними ведут как крупные блокчейн-консорциумы и альянсы, так и отдельные криптоэнтузиасты. Однако такой подход может быть эффективен, если количество участников, которым нужно интегрировать блокчейн-системы, невелико и у них есть возможность выбрать единый механизм. Но что, если участников много, они используют целый зоопарк блокчейн-решений и не могут договориться о способе взаимодействия? Ключевым моментом реализации интероперабельности блокчейн-платформ является даже не техническая, а

организационная составляющая. Разным корпорациям очень сложно договориться о том, по каким правилам учить свои системы «общаться». Помимо этого, существуют и технологические проблемы — при разработке популярных блокчейн-платформ не учитывалось их последующее взаимодействие.

Подход, который решает сразу и технологические, и организационные вопросы, — это стандартизация. Разработка стандартов позволяет найти оптимальное технологическое решение за счёт привлечения широкого круга экспертов и снимает будущие разногласия организационного характера за счёт установления единых правил игры. В сфере стандартизации интероперабельности блокчейн-платформ можно выделить тематическую рабочую группу в ISO TC 307 SG 7. В России не так давно открылась рабочая группа (РГ № 5) в Техническом комитете по стандартизации «Программно-аппаратные средства технологий распределённого реестра и блокчейн» (далее — ТК 159). В неё входят основные представители российского рынка корпоративных распределённых реестров. Это площадка для диалога по технологическим вопросам, связанным с блокчейном, и эксперты ключевых российских компаний принимают активное участие в развитии способов

АССОЦИАЦИЯ ФИНТЕХ. НОВЫЕ ПРОЕКТЫ В 2021 ГОДУ

Наблюдательный совет Ассоциации ФинТех (АФТ) утвердил план деятельности ассоциации на 2021 год. Члены совета высоко оценили результаты работы АФТ в 2020 году. Среди наиболее значимых — перевод в промышленную эксплуатацию сервиса «Цифровые банковские гарантии» и разработка прототипа сервиса для выпуска цифровых финансовых активов на блокчейн-платформе «Мастерчейн», проведение пилота проекта «Цифровой профиль» физического лица. Участники Ассоциации ФинТех пропилотировали новые сервисы Системы быстрых платежей: выплаты от компаний в пользу физических лиц, оплата покупок в интернете по ссылке и другие. Банк России утвердил стандарты открытых API, разработанные совместно с участниками рынка на площадке АФТ.

В 2021 году АФТ совместно с участниками проработает вопросы создания механизма обмена данными юридического лица из государственных информационных систем

(«Цифровой профиль»), продолжит проекты по цифровизации в финансовой отрасли, в том числе: цифровая ипотека, торговое финансирование, включая построение платформы для цифрового факторинга и выпуска ЦФА.

В рамках развития Системы быстрых платежей продолжится разработка новых сервисов и обсуждение ряда инициатив участников, в том числе сервиса B2B-платежей.

Важным направлением в 2021 году станет работа над проектами и инициативами, способствующими повышению уровня цифровизации страхового бизнеса. Кроме того, в следующем году АФТ приступит к созданию профессионального стандарта «Инженер в области блокчейн-технологий» и разработает образовательные программы в областях технологии распределённого реестра и открытых API.

Также на площадке Ассоциации планируется обсуждение подходов к регулированию экосистем и оборота данных на финансовом рынке.

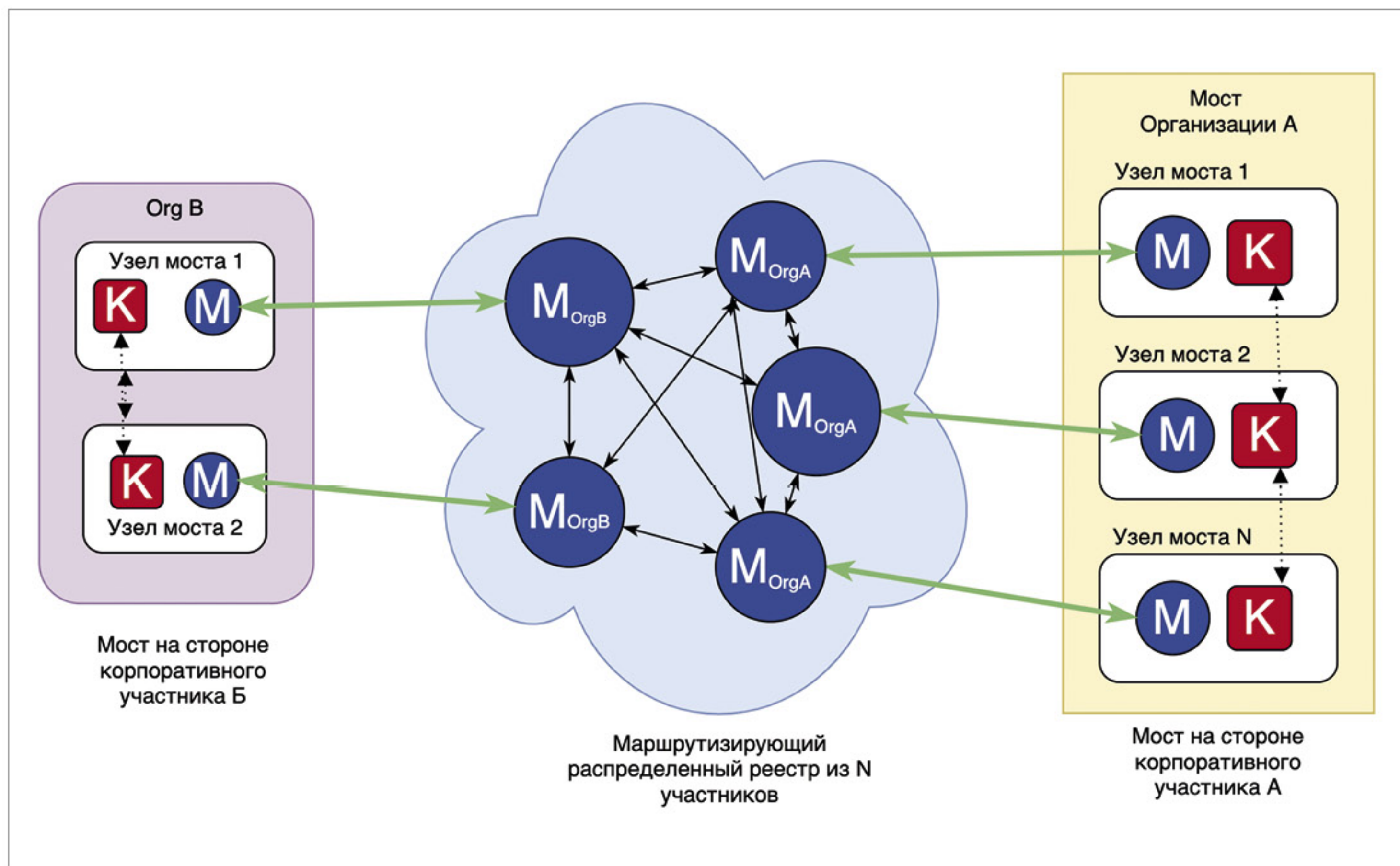


Рисунок 1. Сетевая архитектура консорциумной блокчейн сети. К — корпоративная блокчейн-сеть, М — маршрутизирующая блокчейн-сеть

интероперабельности распределённых реестров. Принять участие в работе групп Технического комитета 159 может любой заинтересованный.

Результатом работы российских экспертов стала публикация в конце 2020 года методических рекомендаций по созданию «моста» между распределёнными реестрами МР 159.5.001–2020 «Протокол обмена сообщениями между распределёнными реестрами с децентрализованным подтверждением пересылаемых сообщений». В первой опубликованной версии описываются принципы реализации функциональной совместимости распределённых реестров для разнородных платформ.

В общем случае описываемый в Методических рекомендациях протокол взаимодействия позволяет создать консорциумную сеть из множества отдельных корпоративных блокчейнов, которые связаны между собой общим маршрутизирующим блокчейном. Если новый корпоративный участник хочет присоединиться к консорциумной сети, ему необходимо поставить в своей инфраструктуре узел маршрутизирующей сети и разработать (или воспользоваться уже разработанным) программное обеспечение, известное в экспертных кругах как «мост», чтобы обеспечить взаимодействие корпоративной и маршрутизирующей сетей.

Методические рекомендации призваны помочь участникам рынка разрабатывать свои системы (на базе распределённых реестров) с учётом возможности организации взаимодействия с системами других компаний. В плане на 2021 год стоит создание формальной спецификации на протокол взаимодействия, описание подходов к информбезопасности и публичное обсуждение с экспертами российского блокчейн-рынка.

* * *

Стандартизация — важный этап на пути создания зрелого блокчейн-рынка. Стандарты упростят жизнь его участникам при реализации корпоративных систем на базе распределённого реестра, снизив затраты на исследования и разработку. Сейчас, когда мы видим новости о том, что компании А и Б наладили интероперабельность своих блокчейн-платформ, то, скорее всего, речь идёт о разовых испытаниях, которые сложно масштабировать и сложно тиражировать на других участников рынка. Развитие методических рекомендаций на базе ТК 159 даёт равные возможности всем игрокам, что позволит динамичнее развиваться всему рынку распределённых реестров в России.

НОВЫЕ ИНСТРУМЕНТЫ

ДЛЯ РАЗВИТИЯ КИБЕРБЕЗОПАСНОСТИ ЭКОСИСТЕМЫ СБЕРА

ВЫЗОВЫ ЭКОСИСТЕМЫ

Сбер сегодня — это не просто финансовая организация, а технологическая компания, которая предоставляет своему клиенту разнообразные банковские и небанковские сервисы и продукты, удовлетворяя потребности физических и юридических лиц. Сбер создал и развивает экосистему, состоящую из дочерних обществ (ДО), а также компаний-партнёров, взаимодействующих друг с другом по ключевым вопросам технологий, маркетинга и бизнеса.

Под экосистемой понимается совокупность компаний и их продуктов и сервисов с принципами, устанавливаемыми банком в сфере его технологических платформ, и взаимодействующих друг с другом для формирования лучших сервисов и продуктов для клиентов. В основе экосистемы находится собственная технологическая платформа, позволяющая в режиме реального времени за счет открытых интерфейсов и кода, машинного обучения, облачных технологий и анализа больших данных с заданным уровнем безопасности, формировать лучшее предложение для клиента как из собственных товаров и услуг, так и за счёт подключения внешних провайдеров.

Один из главных вызовов — обеспечение бесперебойной работы и защищённости продуктов экосистемы Сбера. На текущий момент в её состав входят более 60 ДО с различной

спецификой и масштабом деятельности, ИТ-инфраструктурой, регуляторными требованиями, уровнем зрелости кибербезопасности. Каждый элемент экосистемы не только разделяет её риски кибербезопасности, но и влияет на них. Инцидент в любом из ДО может негативно сказаться на работоспособности всей экосистемы, нанести материальный и репутационный ущерб всем её участникам. К примеру, информация о случившемся инциденте кибербезопасности с утечкой данных в ДО, в наименовании которого упоминается слово «Сбер», быстро распространяется в медиа и социальных сетях, что влечёт негативное отношение пользователей, клиентов и партнёров к банку и ко всей экосистеме. Поэтому для обеспечения непрерывности бизнес-процессов всей экосистемы Сбер решает задачу управления кибербезопасностью и повышения уровня зрелости каждого ДО.



Кристина ЛАВРЕНТЬЕВА
менеджер
Управления
методологии
кибербезопасности
Сбербанка

МЕТОДИЧЕСКИЕ ИНСТРУМЕНТЫ ПОВЫШЕНИЯ УРОВНЯ ЗРЕЛОСТИ КБ ДО

Для мониторинга и контроля состояния кибербезопасности (КБ) ДО экосистемы (рис. 1) банк разработал ряд методических инструментов:

- И1. Профилирование кибербезопасности;
- И2. Оценка текущего уровня зрелости КБ;
- И3. План развития КБ;
- И4. КПЭ «Индекс КБ».

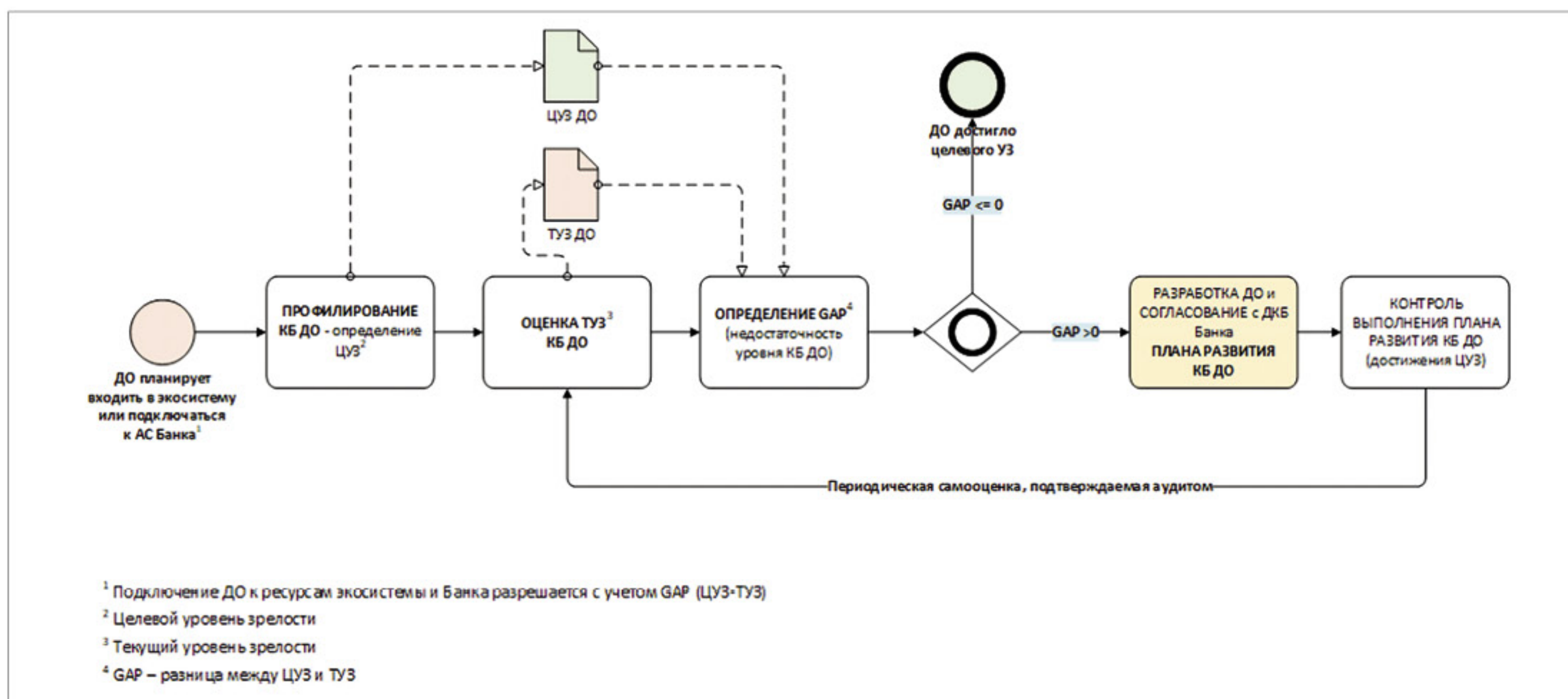


Рисунок 1. Процесс использования методических инструментов

И1. ПРОФИЛИРОВАНИЕ КИБЕРБЕЗОПАСНОСТИ

Для определения точных требований и рекомендаций по кибербезопасности осуществляется профилирование компании с учётом специфики её бизнеса и применимых регуляторных требований. Формирование профиля происходит при вхождении компании в экосистему, профиль определяет целевой уровень зрелости КБ и требования, необходимые для его достижения.

Согласно методике профилирования (и рассматриваемой далее методике оценки зрелости) ДО оценивается по шести доменам КБ (таблица 1).

Каждый домен состоит из направлений (всего 26). Общий целевой уровень зрелости ДО — среднее арифметическое целевого уровня по каждому из 26 направлений КБ.

И2. ОЦЕНКА ТЕКУЩЕГО УРОВНЯ ЗРЕЛОСТИ КИБЕРБЕЗОПАСНОСТИ

Для определения направления дальнейшего развития КБ оценивается также текущий уровень зрелости кибербезопасности ДО. Для его оценки банк применяет собственную методику, в основу которой положена методология СММІ с оценкой процессов КБ по одному из пяти уровней зрелости: начальный (1), управляемый (2), определённый (3), измеримый (4), оптимизируемый (5). Также дополнительно введён уровень 0 — для случаев, когда в оцениваемой компании работы по направлению не ведутся.

Каждый домен подразделяется по направлениям (наименование радиальных осей на рис. 2).

Процесс оценки происходит по трём этапам:

Наименование домена	Описание домена
Управление отношениями	Оценивает эффективность управления кибербезопасностью в ДО
Защита продуктов	Оценивает уровень безопасности сервисов, разрабатываемых и предоставляемых ДО
Защита инфраструктуры	Оценивает функциональные и административные меры обеспечения комплексной защиты инфраструктуры ДО
Проактивное противодействие угрозам	Оценивает эффективность мероприятий по повышению уровня защищённости ДО
Взаимодействие с государственными органами и внешними организациями	Оценивает уровень комплаенса ДО по отношению к законодательству и регуляторам РФ
Процессы и организационная модель	Оценивает уровень программы непрерывности бизнеса, директивные меры ДО и организационную структуру

Таблица 1. Шесть доменов кибербезопасности

Расчёт уровня зрелости по каждому направлению КБ:

$$CS = \sum_1^U \frac{\sum_1^L S}{L},$$

где CS — оценка зрелости направления КБ,

U — количество уровней,

S — количество характеристик на уровне, присущих ДО,

L — количество характеристик на уровне.

Расчёт уровня зрелости по каждому домену КБ. Для этого необходимо рассчитать среднее арифметическое оценок по направлениям, входящим в этот домен:

$$CS_d = \frac{\sum_{i=1}^N \min(CS_i; ЦУЗ(CS_i))}{N},$$

где CS_d — оценка зрелости по домену КБ,

CS_i — актуальная оценка по направлению КБ,

$ЦУЗ(CS_i)$ — целевой уровень зрелости по соответствующему направлению КБ,

N — количество направлений в домене.

Превышения целевого уровня зрелости по зрелым направлениям отбрасываются ($\min$) и не учитываются в расчёте во избежание необоснованного завышения общего уровня зрелости компании.

Расчёт общей оценки уровня зрелости. Для этого необходимо рассчитать среднее арифметическое по всем доменам:

$$CS = \frac{\sum_{d=1}^N CS_d}{N},$$

где CS — оценка уровня зрелости КБ,

CS_d — оценка зрелости домена КБ,

N — количество доменов КБ.

Разница между целевым и текущим уровнем зрелости образует GAP — показатель набора несоответствий, для уменьшения которого каждое ДО экосистемы формирует стратегический план развития КБ, в котором описаны мероприятия для достижения целевого уровня зрелости (рис. 2).

ИЗ. ПЛАН РАЗВИТИЯ КИБЕР- БЕЗОПАСНОСТИ ДО (ПЛАН ДОСТИЖЕНИЯ ЦЕЛЕВОГО УРОВНЯ ЗРЕЛОСТИ)

Последовательная реализация мероприятий «Плана развития» обеспечивает оптимальный путь достижения дочерними обществами целевого уровня зрелости и ликвидацию GAP по каждому из 26 направлений КБ.

Для каждого из этих направлений подбираются мероприятия (кадровые, разработка нормативной документации, внедрение средств защиты) с учётом рекомендаций из отчёта оценки зрелости. Для каждого мероприятия в плане

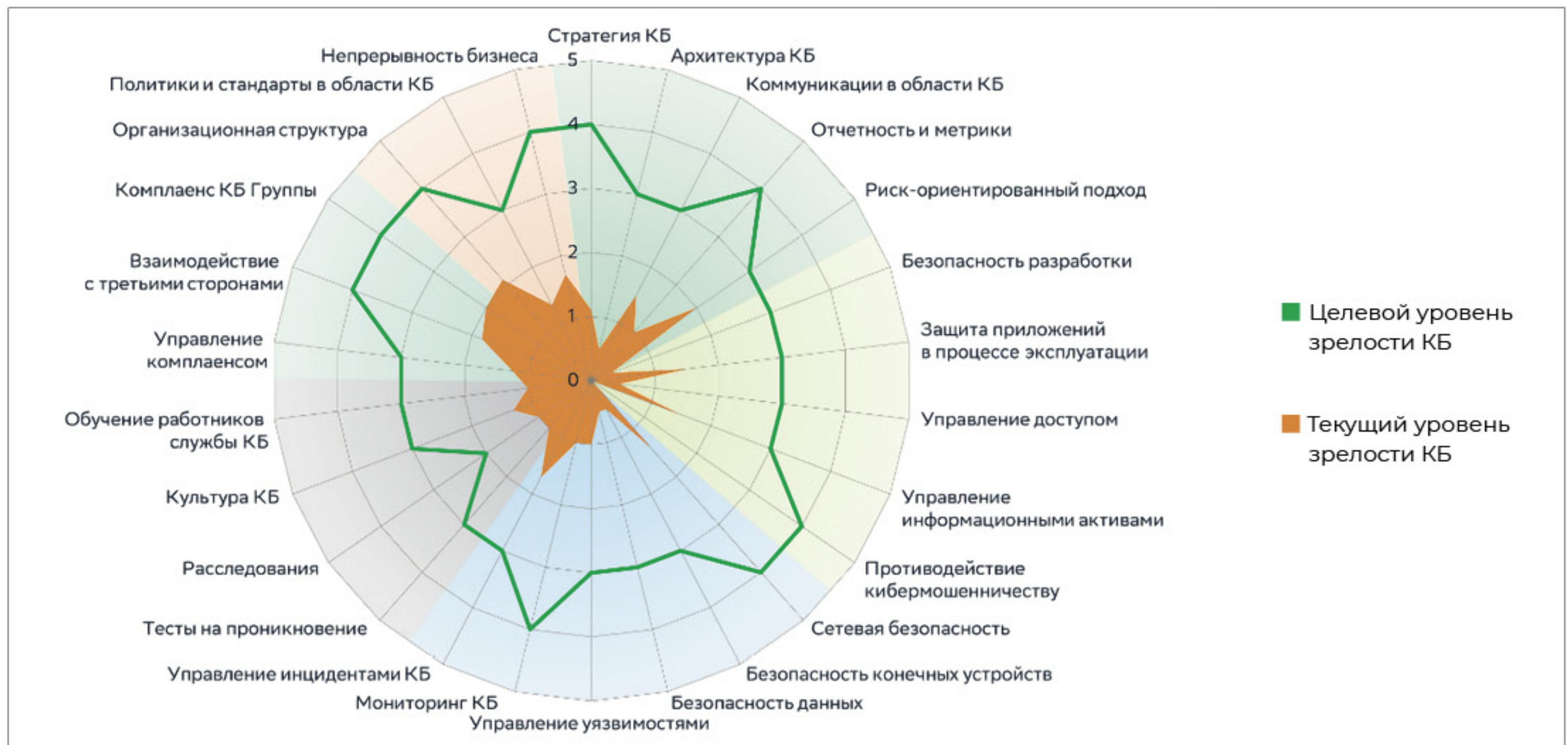


Рисунок 2. Пример визуализации оценки зрелости

задаются приоритет, сроки исполнения и ответственный за его реализацию со стороны ДО.

На регулярной основе ДО экосистемы информируют банк о статусе реализации своего плана развития КБ, а также о возникающих проблемах. Специалисты банка, в свою очередь, помогают в реализации плана и достижении целевого уровня зрелости КБ. Являясь носителями экспертизы, они консультируют ДО, делятся опытом и рекомендациями использования средств защиты информации (СЗИ), поддерживают при закупках.

И4. КПЭ «ИНДЕКС КБ»

КПЭ «Индекс КБ» — показатель эффективности, который оценивает качество управления КБ ДО в рамках общей системы управления, а также входит в состав ключевых показателей эффективности каждого ДО экосистемы и встроен в качестве одного из модулей в общую систему оценки деятельности ДО.

ДО принимает «Индекс КБ» на совете директоров, без его принятия ДО ограничено в возможности доступа к данным участников экосистемы.

Расчёт оценки КПЭ «Индекс КБ» осуществляется на базе сложной табличной функции, которая может гибко настраиваться банком под конкретные стандарты КБ (включая регуляторные) и учитывает в том числе такие параметры:

- ♦ соблюдение сроков разработки и выполнения планов по направлению КБ;
- ♦ согласование с банком ключевых решений в области КБ (назначение руководителей подразделений КБ ДО, открытие проектов в области

КБ, закупка/внедрение СЗИ, предоставление информации по ИТ-проектам ДО);

- ♦ своевременность предоставления в банк полной информации о критичных инцидентах КБ, ходе и результатах расследований;
- ♦ своевременность предоставления отчётности по кибербезопасности, включая статус выполнения применимых регуляторных требований.

КПЭ «Индекс КБ» стимулирует руководителей ДО к регулярному контролю состояния КБ компании, выделению необходимых ресурсов и является одним из важнейших инструментов повышения качества менеджмента КБ компаний экосистемы.

ЗАКЛЮЧЕНИЕ

Быстро меняющаяся бизнес-среда требует новых подходов к управлению кибербезопасностью компаний экосистемы. Сбер разрабатывает и применяет новые инструменты для контроля и мониторинга уровня зрелости кибербезопасности ДО и вовлекает топ-менеджмент компаний в работу по развитию КБ ДО в рамках системы управления КБ Группы Сбербанк.

Банк не только контролирует, но и помогает компаниям в развитии кибербезопасности, определяя для каждого ДО целевой уровень зрелости процессов КБ с учётом специфики его бизнеса (специфичных факторов риска КБ). Также Сбер помогает ДО разработать стратегический план развития КБ для достижения целевого уровня зрелости и организует работу по контролю его статуса. В результате формируется эволюционное улучшение защищённости экосистемы при оптимальном расходовании ресурсов.



КИБЕРБЕЗОПАСНОСТЬ ПРОМЫШЛЕННОСТИ

К ЧЕМУ ГОТОВИТЬСЯ И КАК ЗАЩИТИТЬСЯ В 2021 ГОДУ

Проблемы информационной безопасности выходят на первый план во многих отраслях, и промышленность не исключение, так как после «удивительного» 2020 года и массового перехода на удалёнку некогда популярный тезис «мы не боимся кибератак, поскольку отключены от интернета», больше не работает.

Из публичных историй конца 2020 можно привести в качестве приме-

ра остановку производства крупного мебельного производителя Steelcase по вине вымогательского ПО. Если говорить про Россию, то в октябре 2020 года злоумышленникам удалось взять под управление одно из предприятий в Рязани, относящееся к значимым объектам КИИ. Примечательным здесь стал финал: виновника допущенной ошибки нашли внутри предприятия и наказали сотрудника согласно КоАП.

Законодательство в области безопасности КИИ призывает руководителей промышленных компаний к обеспечению безопасности. Однако если изучить статистику привлечения к ответственности по профильной статье 274.1 УК РФ за всё время её действия, то большинство случаев наказания виновных связано с неправомерным доступом к детализации или иным сведениям операторов связи. И всего лишь несколько судебных дел, связанных с

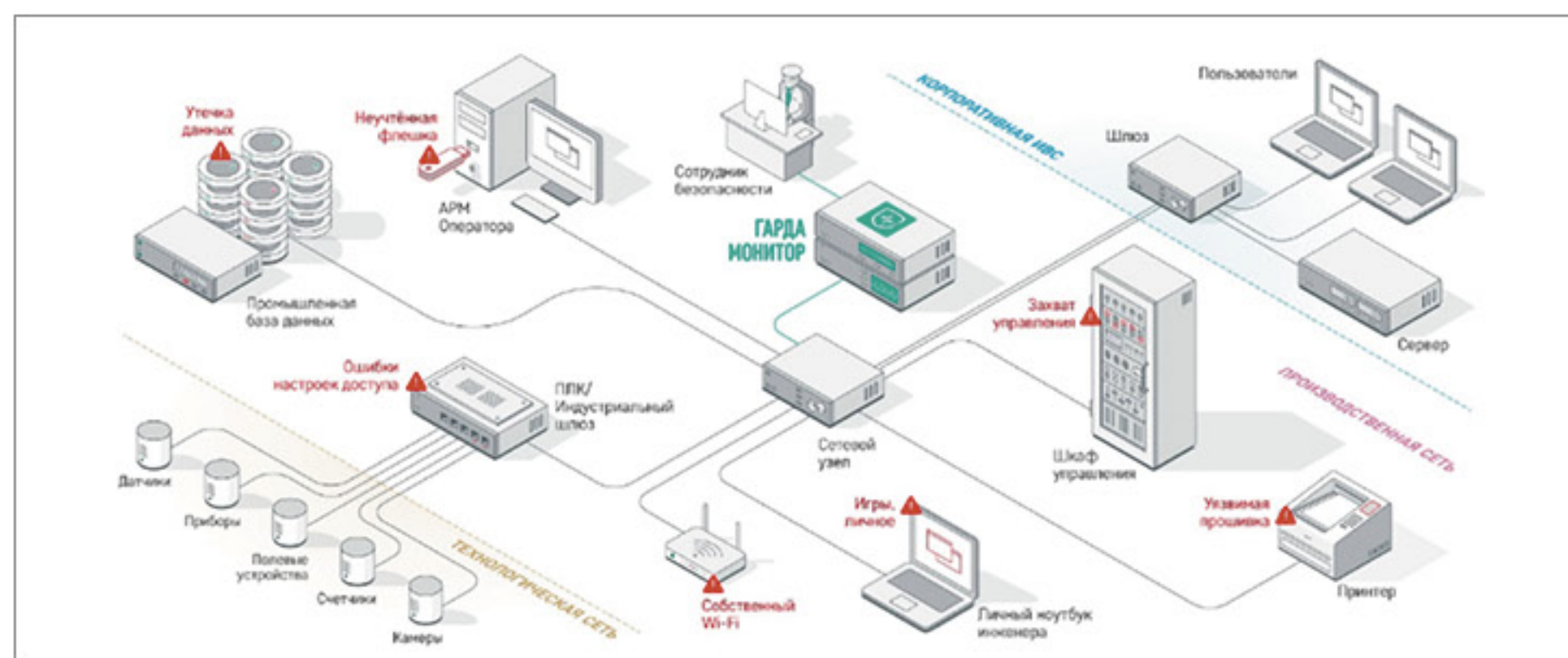


Рисунок 1. Риски безопасности для производственной сети

Технологии» поддерживает такой практический подход и с помощью технологий собственной разработки помогает производственным предприятиям и другим компаниям решать «боевые» задачи безопасности.

ЧТО ПРОИСХОДИТ В ПРОИЗВОДСТВЕННОЙ СЕТИ?

Уверены, что знаете всё о происходящем не только в корпоративной, но и в производственной сети? Согласно данным исследования SANS 2020 года, меньше 30 % специалистов по безопасности отвечают утвердительно на подобный вопрос, при этом почти 60 % уверены, что недостаточная прозрачность сетей несёт высокие риски их безопасности (рис. 1).

Самое важное в работе современного специалиста по безопасности — суметь обнаружить угрозу инцидента до его наступления. Не получится защититься от всего сразу, потому важно обращать внимания на индикаторы, с высокой долей вероятности сигнализирующие о проблемах в ИБ. Если говорить о мониторинге промышленной сети, то к таким можно отнести:

- ♦ ошибки разграничения доступа;
- ♦ появление новых неучтённых устройств;
- ♦ появление нетипичного трафика и возникновение аномалий;
- ♦ непроизводственная активность на подключённых в сеть устройствах.

Всё это может привести к опасным последствиям, например:

- ♦ заражению устройств и захвату управления;
- ♦ нарушению технологических процессов;

- ♦ несанкционированной передаче данных вовне;

- ♦ проникновению в другие сегменты сети.

Решать указанные задачи и пресечь кибератаки помогает система обнаружения и расследования сетевых инцидентов «Гарда Монитор». Приведём несколько примеров.

Один из механизмов, который мы часто применяем на практике, — контроль сетевых соединений на периметре технологического сегмента за счёт глубокого разбора содержимого пакетов и сигнатурного анализа трафика. «Гарда Монитор» позволяет обнаружить (рис. 2):

- ♦ возникновение нелегитимного трафика (игровой, YouTube, BitTorrent и т.п.);
- ♦ подключение к SCADA-серверу из внешнего сегмента и изменение параметров работы технологического оборудования;
- ♦ сканирование хостов технологического сегмента сети;
- ♦ эксплуатацию уязвимостей в ПО устройств;
- ♦ ошибки в настройках межсетевых экранов и маршрутизаторов.

«Гарда Монитор» способна разбирать популярные промышленные протоколы до уровня команд, что позволяет максимально точно учитывать специфику технологических сетей при детектировании киберинцидентов.

Другой пример — контроль сетевых соединений внутри технологического сегмента. Используя «Гарда Монитор», служба безопасности осуществляет:

- ♦ инвентаризацию устройств и служб (по используемым протоколам);
- ♦ автоматическое выявление новых устройств и служб;

кибератаками, доведены до привлечения виновных к ответственности (хотя именно это соответствует изначальному смыслу ФЗ-187 от 26.07.2017) или вымогательство с подтверждённым финансовым ущербом.

Самое интересное, что в документах регуляторов (приказах ФСТЭК и ФСБ) заложен процессный подход к построению системы защиты объектов КИИ, к числу которых относится множество промышленных предприятий. Таким образом, от выполнения формальных требований фокус должен смещаться к предотвращению неправомерного воздействия на информацию, защите от реальных атак (приводящих к ущербу), обнаружению, реагированию и расследованию инцидентов. «Гарда

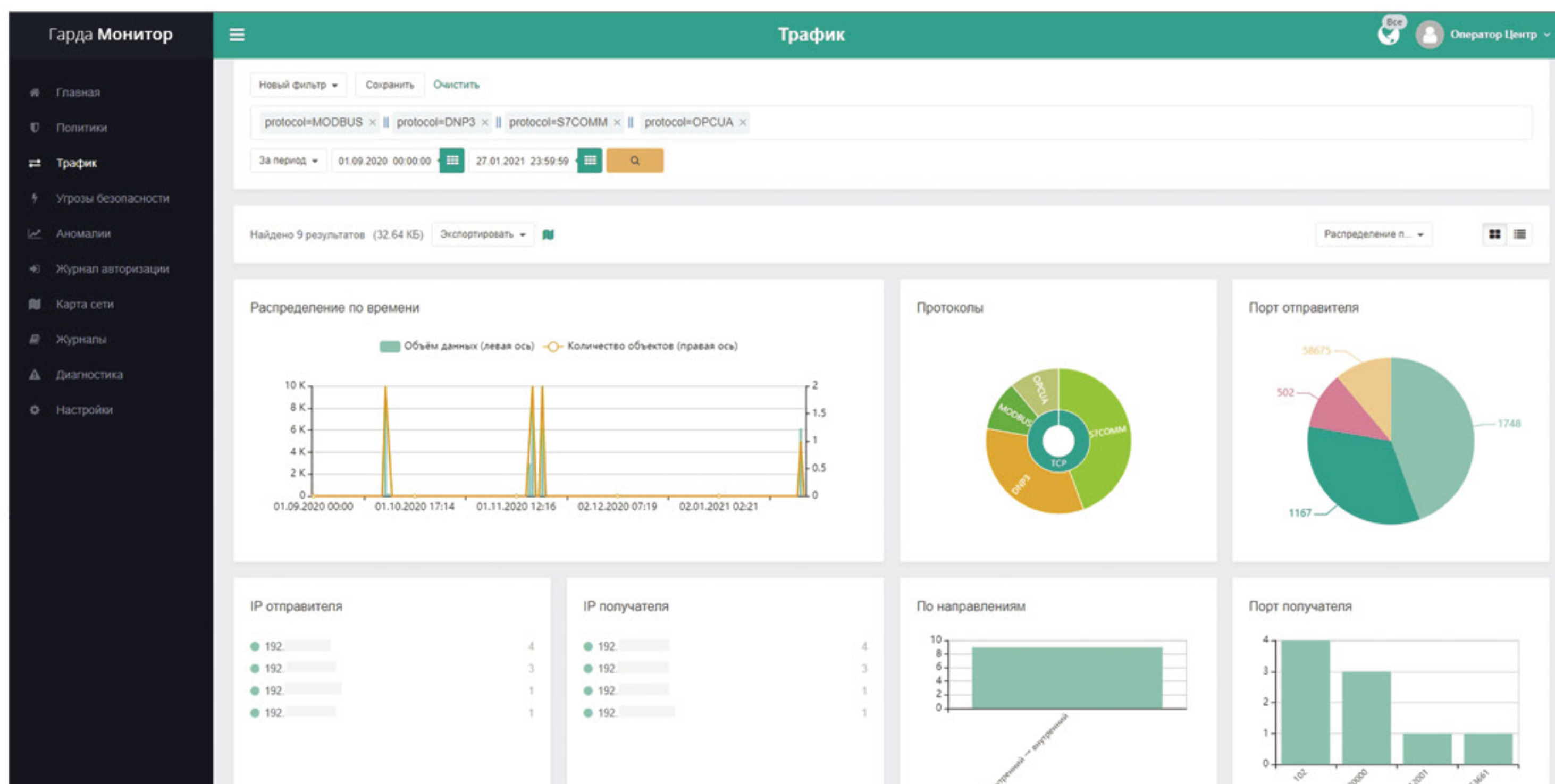


Рисунок 2. Промышленный трафик — отображение в интерфейсе «Гарда Монитор»

♦ прозрачное понимание команд, передаваемых внутри промышленных протоколов;

♦ выявление вредоносной активности или действий злоумышленников с помощью автоматического обнаружения аномального поведения устройств;

♦ автоматизированное уведомление о нарушениях в сети.

Наконец, стоит упомянуть о важном мероприятии, про которое нередко забывают. Но ровно до тех пор, пока не столкнутся с отсутствием или недостоверностью имеющихся данных. Речь про расследование инцидентов, фиксацию фактов и восстановление хронологии событий. «Гарда Монитор» независимо от сетевого оборудования, промышленных систем и других средств защиты фиксирует всю сетевую активность, а не только точечные «сработки». Эти сведения помогают проанализировать ход атаки или последовательность злоумышленных действий, чтобы сделать необходимые выводы, а также могут быть отправлены по запросу в компетентные органы.

КАК ОБЕСПЕЧИТЬ БЕЗОПАСНОСТЬ ПРОИЗВОДСТВЕННЫХ БД

Сердце любой информационной системы — базы данных, иначе она просто

лишена смысла. Производственные системы, системы проектирования, моделирования, учёта не исключение. Если посмотреть на самые громкие киберинциденты 2020 года, то они направлены либо на кражу данных, либо блокировку доступа к ним с целью шантажа. Самый эффективный способ контроля того, что происходит с критичными данными, — мониторинг баз данных «в непосредственной близости» от них. К подобного рода инструментам (системы DAM/DBF — Data access management — управление доступом к данным/ Database firewall — межсетевой экран баз данных) относится система защиты баз данных и веб-приложений «Гарда БД» (рис. 3). На промышленных предприятиях и объектах КИИ она позволяет:

♦ проводить полный аудит действий сетевых- и БД-администраторов промышленных баз;

♦ защищать критичные и особо важные БД;

♦ выявлять теневые, нелегитимные и неконтролируемые БД на промышленных объектах;

♦ детектировать специфичные инциденты с учётом специфики конкретного производственного объекта;

♦ своевременно обнаруживать критичные уязвимости и неверно сконфи-

гурированные СУБД (в том числе на базе старого ПО);

♦ фиксировать и проводить независимое расследование инцидентов, связанных с базами данных.

Приведём несколько сценариев использования «Гарда БД» для защиты баз данных на промышленных предприятиях, где применение любых других механизмов защиты либо неэффективно, либо не защитит от инцидента.

1) Появление баз данных, доступных вне защищённого контура. При переходе на «удалёнку» службам ИТ, в том числе производственных предприятий, пришлось срочно обеспечивать доступ к служебным ресурсам фактически откуда угодно (из дома, кафе или коворкинга). При этом вопросы безопасной организации такого доступа не всегда решаются в приоритетном порядке. «Гарда БД» способна в онлайн-режиме контролировать работу в базах, выявлять и сигнализировать о нарушении правил доступа, уязвимых или неверно настроенных СУБД, блокировать нелегитимные запросы и т.п. Это позволяет службе безопасности своевременно пресекать нарушения и минимизировать риски серьёзных последствий утечек данных, атак на СУБД и т.п.

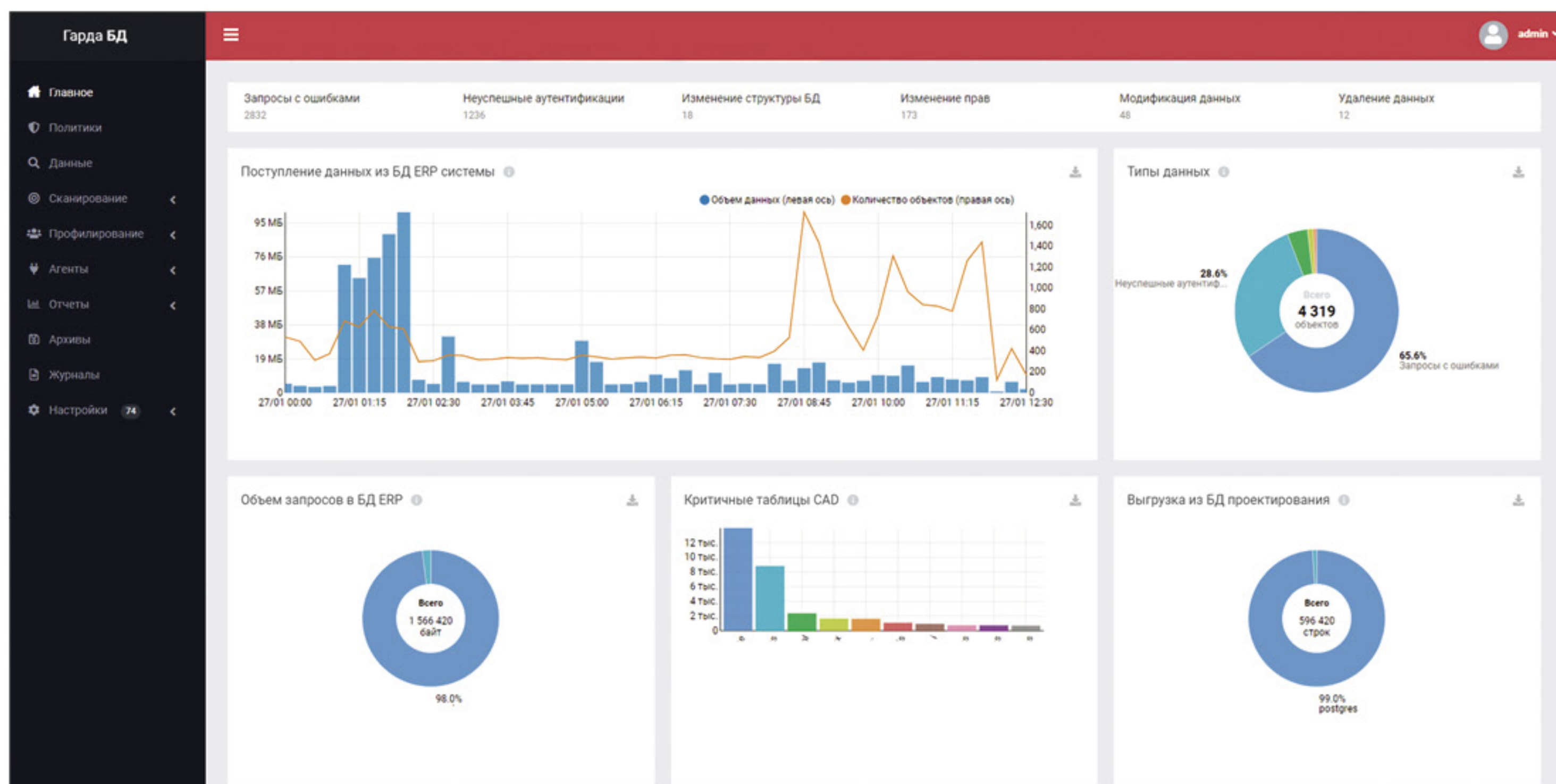


Рисунок 3. Непрерывный мониторинг баз данных в системе «Гарда БД»

2) **Выявление нелегитимных манипуляций с промышленными базами данных с помощью нештатных средств.** Чтобы получить нелегальный доступ или нарушить целостность производственной, конструкторской или любой другой системы, злоумышленники нередко действуют в обход штатных процедур работы, например, через веб-интерфейс или клиентское ПО. Для полноценного выявления такого рода инцидентов недостаточно использовать только лишь системы специализированных средств защиты на конечных устройствах. «Гарда БД» контролирует и фиксирует все обращения непосредственно в базах данных, на которых работают указанные выше системы, не оставляя «белых пятен» для службы ИБ, и позволяет обнаружить и заблокировать:

- ♦ большие единовременные выгрузки из баз данных;
- ♦ выгрузки из баз данных небольшими частями в течение определённого времени;
- ♦ попытки злоумышленника воспользоваться ИТ-инструментами, отладочными программами;
- ♦ попытки администраторов выгрузить данные, напрямую подключившись к СУБД.

3) **Аттестация информационных систем промышленного предприятия**

в случае применения несертифицированных СУБД.

«Гарда БД» помогает выполнить нормативные требования регуляторов, в частности, отдельные положения следующих групп мер приказа ФСТЭК № 239:

- ♦ ИАФ (идентификация и аутентификация);
- ♦ УПД (управление доступом);
- ♦ АУД (аудит безопасности);
- ♦ ЗИС (защита информационной системы);
- ♦ ИНЦ (обнаружение вторжений).

«Гарда БД» имеет сертификат ФСТЭК России по требованиям безопасности информации.

ОСНОВНЫЕ ТРЕНДЫ ПРОМЫШЛЕННОЙ КИБЕРБЕЗОПАСНОСТИ В 2021 ГОДУ

Все сценарии применения современных технологий для защиты от актуальных угроз в промышленности в рамках одной статьи разобрать невозможно. Ещё более неблагоприятное занятие — прогнозирование. Однако попробуем наметить несколько важных трендов.

Во-первых, киберпреступники в 2020 году хорошо «почувствовали вкус наживы». Суммы выплат мошенникам

за остановку атаки или восстановление доступа к данным со стороны компаний исчисляются миллионами долларов. Поэтому кибератаки на промышленные объекты будут всё больше сфокусированы на получение выкупа.

Во-вторых, количество доступных в интернете сервисов производственных предприятий будет расти, следовательно, случайные или целенаправленные сканирования, подборы паролей, DDOS-атаки и тому подобное не потеряют актуальности.

В-третьих, цифровизация будет проникать на производства, а это значит, что вариативность традиционных для корпоративных инфраструктур инцидентов ИБ станет обыденной и для промышленных сегментов. Речь о злоупотреблениях или халатности сотрудников, атаках через классические сетевые службы и протоколы, обычные вирусы для ПК. Наконец, никуда не уходят геополитический фактор, промышленный шпионаж и конкурентная борьба.

В современных реалиях connected world (англ. «взаимосвязанного мира») не защищаться от вышеупомянутых рисков кибербезопасности может означать моментальный проигрыш и снижение темпов развития бизнеса на долгие годы вперёд.



Марина СОРОКИНА
руководитель направления
отдела развития продуктов
компании «ИнфоТеКС»

«МЫ ПОМОГАЕМ ЦИФРОВОМУ ПРЕДПРИЯТИЮ СТАТЬ РЕАЛЬНОСТЬЮ»

ПРОДУКТЫ ИНФОТЕКС ПОЗВОЛЯЮТ ДЕЛАТЬ БЕЗОПАСНЫМИ ЛЮБЫЕ СЦЕНАРИИ ЭКСПЛУАТАЦИИ И ОБСЛУЖИВАНИЯ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

На вопросы BIS Journal отвечает руководитель направления отдела развития продуктов «ИнфоТеКС» Марина Сорокина.

— Марина, мы бы хотели задать вам несколько вопросов о защите АСУ ТП. Что сегодня предлагает ИнфоТеКС в части обеспечения кибербезопасности?

— В продуктовом портфеле ИнфоТеКС есть две специализированные линейки для защиты АСУ ТП: наложенные средства защиты и встраиваемые.

— Расскажите, пожалуйста, про наложенные средства защиты. Как с их помощью можно защитить промышленные системы?

— Прежде всего, речь идёт об индустриальных шлюзах безопасности ViPNet Coordinator IG, предназначенных для установки на всех уровнях АСУ и АСУ ТП и позволяющих построить эффективную систему информационной безопасности предприятия.

Технология ViPNet VPN, использующаяся в шлюзах, обеспечивает безопасную передачу данных, а функция межсетевого экрана защищает объекты от несанкционированного доступа.

Индустриальный дизайн ViPNet Coordinator IG позволяет устанавливать его рядом с промышленным оборудованием и эксплуатировать в сложных климатических условиях.

Важную роль играет то, что шлюзы безопасности могут работать как с проводными (Ethernet), так и с беспроводными (Wi-Fi, 3G/LTE) каналами связи. Кроме этого, в них поддерживается работа с последовательными (RS-485/232) интерфейсами.

Отдельно хочу подчеркнуть, что ViPNet Coordinator IG полностью совместим с другими продуктами ViPNet VPN: шлюзами безопасности, используемыми для защиты ИТ-инфраструктуры разного масштаба (от маленьких офисов до ЦОДов) и программными VPN-клиентами, предназначенными для компьютеров и мобильных устройств, работающих на всех распространённых ОС. Также возможно централизованное управление ключами и политиками безопасности.

— Получается, что вы предлагаете сквозную безопасность целиком для промышленного предприятия, а не только для части АСУ?

— Да, именно так. Продукты позволяют делать безопасными практически любые сценарии эксплуатации и обслуживания промышленных предприятий. Все технологии, которые предлагает так называемая четвёртая промышленная революция (Industry 4.0) и которые невозможно было использовать ранее из-за отсутствия инструментов по защите информации, становятся доступными.

Не побоюсь сказать, что мы помогаем цифровому предприятию стать реальностью в соответствии с жёсткими требованиями наших ИБ-регуляторов. Например, в проектах «цифровой монтер или обходчик» информация с датчиков, расположенных на касках персонала, попадает в планшет и позволяет отслеживать состояние их здоровья или обслуживаемого ими оборудования. Используя планшет, персонал может подключаться к контроллерам для просмотра журнала событий. Так как эти данные носят конфиденциальный характер, встают вопросы информационной безопасности. Функционал наших продуктов позволяет их решить.

— Интересно. Есть уже проекты, реализованные в этом ключе?

— Пока не буду раскрывать все карты, но есть ряд очень интересных проектов, в том числе и «цифровые монтеры», о которых я упоминала ранее. Есть проект по безопасному управлению беспилотным транспортом, где тоже используется ViPNet Coordinator IG.

Сейчас мы работаем над расширением сценариев и предлагаем защищать каналы до самих устройств автоматизации. Для этого в 2020 году было разработано и сертифицировано ПО ViPNet Client 4U, который может работать в том числе на контроллерах с архитектурой ARMv5, ARMv7, ARMv8, MIPS под ОС Linux.

— Мы обсудили наложенные средства защиты, давайте теперь перейдём к встраиваемым. Что вы предлагаете в этой области?

— Мы часто слышим о том, как важно прийти к реализации концепции *secure by design*, но мало кто представляет, как это сделать. В нашем продуктовом портфеле есть уникальное решение — единственный в России сертифицированный криптомодуль ViPNet SIES Core, предназначенный для защиты устройств нижнего уровня АСУ, межмашинного взаимодействия (M2M) и промышленного интернета вещей (IIoT): ПЛК, терминалов, интеллектуальных устройств и пр.

Криptomодуль встраивается в различные защищаемые устройства независимо от их производительности, архитектуры и операционной системы, по сути, речь идёт о криптографическом сервисе для устройства. Идея в том, что все криптографические преобразования, а также хранение ключей шифрования выполняются внутри ViPNet SIES Core, который интегрируется с защищаемыми устройствами через межплатные интерфейсы. Защищаемые устройства запрашивают у встроенного криптомодуля выполнение криптографических операций с данными, а потом используют результат для построения собственной защиты. Например, для безопасной передачи данных, а также для доверенного обновления или доверенной загрузки.

ViPNet SIES Core — часть решения ViPNet SIES (Security for Industrial and Embedded Solutions), объединяющего криптографические средства защиты информации в АСУ и M2M-системах для всех уровней. Кроме криптомодуля, в него также входят программный комплекс ViPNet SIES Unit, обеспечивающий защиту устройств уровня оперативно-диспетчерского управления АСУ, и центр управления жизненным циклом компонентов решения ViPNet SIES — программно-аппаратный комплекс ViPNet SIES MC.

— В каком случае рекомендуется использовать наложенные средства, а в каком лучше подходят встраиваемые? Когда эффективней комплексный подход?

— Сложно сказать, что лучше, — всё зависит от задачи. Иногда эффективней использовать встраиваемые средства, иногда наложенные. Одно другого не исключает. Например, каналы защищаются наложенными средствами, так как это проще, а доверенная загрузка или обновление контроллеров обеспечивается встроенными средствами. Бывает так, что каналы нельзя защитить наложенными средствами, так как сеть не TCP/IP или даже не Ethernet, тогда для защиты остаётся один вариант — ViPNet SIES.

Я, например, поддерживаю рекомендации, сформулированные в Приказе № 239 ФСТЭК России от 25.12.2017, где приоритет отдаётся встраиваемым средствам защиты информации. Те механизмы ИБ, что привнесли сами разработчики средств автоматизации, более инвазивны по отношению к АСУ из-за глубокого понимания технологического процесса. Вендоры, разрабатывающие средства защиты информации, не так погружены в АСУ. Другое дело, что на стороне разработчиков устройств автоматизации пока не хватает специалистов ИБ, поэтому таких решений крайне мало. Наш ViPNet SIES Core был создан как раз для того, чтобы помочь разработчикам средств автоматизации делать их безопасными.

— **Задам провокационный вопрос...** Считается, что в АСУ вмешиваться нежелательно — можно прервать технологические процессы, поэтому в основном все говорят про мониторинг и обнаружение вторжений, почему вы развиваете проактивные продукты?

— По моему мнению, тема с инвазивностью для АСУ преувеличена. Во-первых, на момент становления рынка кибербезопасности средства ИБ, особенно некорректно внедрённые и настроенные, действительно могли оказывать негативное влияние на техпроцесс. Эти времена ушли в далёкое прошлое, а миф остался.

Во-вторых, если разбираться, страхи связаны не с влиянием средств защиты информации, а с надёжностью системы после их внедрения. Вопросы надёжности и отказоустойчивости в АСУ позволяют решить механизмы резервирования. В ответственных

АСУ резервируется всё — начиная от каналов связи и заканчивая самими устройствами. И мы учитываем это, разрабатывая свои продукты. Так, промышленный шлюз ViPNet Coordinator IG может работать в режиме кластера, поддерживает резервирование каналов, может переключать проводной канал на беспроводной, если первый перестаёт работать. В решении ViPNet SIES мы поддерживаем работу устройств автоматики, имеющих резервирование.

Говоря про надёжность, хочу подчеркнуть, что мы проектируем решения с учётом наработки на отказ и подбираем соответствующую элементную базу.

И, в-третьих, проактивные средства ИБ уже давно применяются внутри АСУ. Просто раньше они назывались иначе и не учитывали требования российской нормативной базы. Например, в промышленных маршрутизаторах давно есть функции межсетевого экранирования и VPN.

— **Вы говорили ранее, что подбираете компоненты для платформ своих продуктов. Вы сами проектируете и производите «железо»?**

— Да, все аппаратные платформы для промышленного направления мы проектируем сами и являемся владельцами конструкторской документации. Изготавливает их контрактное производство, расположенное в России.

Это позволило нам в прошлом году включить все исполнения ПАК ViPNet Coordinator IG в реестр телекоммуникационного оборудования российского происхождения (ТОРП), являющего частью реестра российского радиоэлектронного оборудования (РЭП). ViPNet Coordinator IG официально стал первым российским промышленным шлюзом безопасности, так как ранее он был включён и в единый реестр российского ПО.

— **Как вы смотрите на будущее развития кибербезопасности в разрезе защиты АСУ ТП?**

— На будущее смотрим с оптимизмом: рынок кибербезопасности очень активно развивается. Конечно, всех серьёзно стимулирует законодательство по КИИ и импортозамещение. Интересное время — много изменений. Приходится постоянно быть в тонусе и подстраиваться, проявляя гибкость.



Сергей КУЗНЕЦОВ
региональный директор Thales
по решениям для управления
доступом и защиты данных

В БУДУЩЕЕ — БЕЗ ПАРОЛЕЙ!

О НЕПРЕРЫВНОМ БЕСПАРОЛЬНОМ ЕДИНОМ ВХОДЕ

Традиционная, основанная на пользовательских паролях, аутентификация безнадежно устарела. Усиление пароля с помощью многофакторной аутентификации в современных гибридных корпоративных информационных средах имеет свои недостатки. Самой перспективной представляется идея непрерывного беспарольного единого входа, реализованная в продуктах компании Thales.

ЧЕМ ПЛОХИ ПАРОЛИ?

Пользовательские пароли хорошо подходили для первого поколения вычислительных систем. Но уже в эпоху клиент-серверных архитектур проявились их неудобства, которые сглаживались с помощью сетевых служб каталогов и механизма однократного входа. В современных же корпоративных вычислительных средах такой подход уже неадекватен. Нам приходится запоминать десятки паролей, мы устаем от них, и 10% пользователей используют хотя бы один из 25 наихудших паролей. А все попытки навязать пользователям жесткие политики длины, сложности и повторяемости паролей приводят к тому, что всё чаще стали использовать один и тот же пароль на разных ресурсах, причём свыше 70%

людей используют те же самые пароли для рабочих и личных учётных записей. Ну и нарушения правил хранения паролей никуда не исчезли. Как следствие, пароли остаются главной мишенью для атак злоумышленников (рис. 1).

Поэтому использование многофакторной аутентификации стало хорошим тоном. Современные нормативы безопасности явно или неявно требуют её использования. Из релевантных для банковской сферы — PCI DSS и новая директива Евросоюза PSD 2. Разумеется, нужно вспомнить и про отечественный стандарт ГОСТ Р 57580 и ссылающиеся на него положения Банка России.

По-прежнему самыми популярными технологиями для многофакторной аутентификации для усиления пользовательских паролей остаются токены PKI (в виде смарт-карт и USB-ключей), SMS и одноразовые пароли, но у каждой из них есть ограничения. PKI неудобен для использования в публичных облачных средах. SMS считаются довольно уязвимыми, особенно для социальной инженерии. Одноразовые пароли на базе отдельных устройств или пуш-уведомлений в мобильном приложении пока остаются самым удобным решением, хотя и не обещают абсолютной

стойкости. К сожалению, идея усилить пароль дополнительным фактором не устраняет присущих паролям неудобств, а из-за дополнительного фактора жизнь пользователей становится ещё сложнее, так что нужен какой-то выход.

Ещё одна область проблем — это управление доступом. Опять же корни существовавшего долгое время подхода тянутся из прошлого века. Предприятия могли контролировать среду пользователя внутри периметра, в которой фактора знания пароля было достаточно, ну а если требовался доступ из-за его пределов, то можно было включить дополнительные методы аутентификации и (или) ограничить уровень доступа. В девяностые и нулевые годы все только так и работали, миллионы сотрудников привыкли к VPN и устройствам-токенам. Но, как известно, периметр «умер», и такой подход больше не работает, он живёт только в привычках и нормативах.

БЕСПАРОЛЬНАЯ АУТЕНТИФИКАЦИЯ

Как следует из названия, беспарольная аутентификация использует для подтверждения учётных данных вместо пароля иные надёжные и простые в использовании методы. Такой способ аутентификации представляется перспективным, так как он исключает присущие текстовым паролям недостатки и благодаря этому значительно упрощает вход в систему для пользователей. Есть несколько моделей беспарольной аутентификации.

При ноль-факторной аутентификации вообще не используется ни один из привычных факторов, а для подтверждения личности пользователя используются только косвенные признаки,



Рисунок 1. Ситуация с пользовательскими паролями

например контрольные вопросы или «отпечаток» пользователя (идентификаторы его устройств, местоположение, время суток). К сожалению, пока невозможно уверенно положиться на чистую ноль-факторную аутентификацию, и поэтому такое решение подойдёт только для не слишком ответственных приложений или же в сочетании с другими факторами.

При однофакторной беспарольной аутентификации вместо пароля используется более удобный и (или) более стойкий фактор. Один из самых популярных — это PIN-код, привязанный к устройству и использующий его защищённое хранилище. Далее — это биометрия. Также применяются дополнительные устройства аутентификации, но использующие стандарты, ориентированные на публичные облачные среды и веб-приложения (в первую очередь это семейство FIDO).

Наконец, многофакторная аутентификация, при которой два или более перечисленных выше фактора используются совместно. При этом такая схема может быть даже удобнее одиночного пароля при несоизмеримо более высоком уровне безопасности.

А когда беспарольная аутентификация комбинируется с единым входом, мы получаем беспарольный единый вход. Он позволяет сохранить удобство беспарольной аутентификации при доступе к нескольким приложениям, но с ростом их числа растёт его уязвимость. Подход «проверили и забыли» здесь не подходит, так как необходимо соразмерять уровень доступа (и связанный с ним риск) с удобством для пользователя. Для доступа к критически важным ресурсам может потребоваться эскалация, повышение строгости, и от пользователя может потребоваться, например, повторить аутентификацию или задействовать ещё один фактор. И сюда очень хорошо вписывается тот самый нулевой фактор, который будет обеспечивать контекстно-зависимую аутентификацию (рис. 2). И тут мы приходим к идее непрерывного беспарольного единого входа.

НЕПРЕРЫВНЫЙ БЕСПАРОЛЬНЫЙ ЕДИНЫЙ ВХОД

Непрерывная аутентификация позволяет убедиться в подлинности пользо-



Рисунок 2. Модели беспарольной аутентификации

вателя в течение времени, даже если пользователь меняет свой контекст, то есть переходит от устройства к устройству, переключается между сетями и обращается к разным приложениям. Служба управления доступом будет подтверждать личность пользователя непрерывно и незаметно, требуя от пользователя пройти дополнительную аутентификацию только тогда, когда сработает какая-нибудь политика или будет обнаружена аномалия в его поведении. Благодаря прозрачной аутентификации пользователю больше не нужно явным образом аутентифицироваться во всех ситуациях, так как решение адаптивно и учитывает контекст пользователя. Стойкость и удобство можно повысить с помощью мобильного устройства, которое служит хорошим датчиком поведения пользователя. Прозрачная аутентификация даёт возможность детализировать доступ к приложениям и данным путём установки пороговых значений: действия пользователя в приложении непрерывно оцениваются, и при достижении какого-то порогового значения потребуется дополнительная аутентификация. Например, если пользователь начинает скачивать через приложение большой объём данных, сработает правило, которое потребует от пользователя подтвердить свою личность с помощью дополнительного фактора.

Красота этих схем заключается в том, что они дают возможность поддерживать очень высокий уровень защиты, при этом существенно уменьшая неудобства пользователей при входе. Они также обеспечивают гибкость использования разных методов аутентификации в разных сценариях в зависимости от критичности приложений и данных, профиля пользователя

и других условий. Представляется, что непрерывный беспарольный единый вход отлично подходит именно для финансовых организаций, которые привыкли принимать решения на основе оценки рисков. Ведь сама идея непрерывной аутентификации заключается в поддержке определённого уровня риска, которому соответствует определённый уровень доверия и который, в свою очередь, диктует строгость аутентификации.

Ожидается, что в течение нескольких лет большинство организаций перейдут к беспарольной аутентификации. Эти организации могут начать с внедрения единого входа к нескольким наиболее часто используемым приложениям и данным. Со временем они смогут оценивать критичность приложений и связанный с ними риск и затем установить подходящий уровень строгости аутентификации для каждого набора данных. И исходя из этого можно будет назначить политики доступа в рамках беспарольного единого входа так, чтобы обеспечить баланс между надёжностью защиты и удобством пользователей.

* * *

Компания Thales предлагает передовые решения, которые помогают защитить доступ к ИТ-инфраструктуре предприятия и облачным приложениям. SafeNet Trusted Access — это облачная служба Thales для управления доступом и аутентификацией, которая позволяет реализовать непрерывный беспарольный единый вход. Она предотвращает утечки данных, помогает организациям соблюдать нормативные требования и делает переход в облако простым и безопасным.



Олег ИВАНОВ
генеральный директор
ГК «ЦИБИТ»



Евгения КОЛОДИНА
директор по развитию
ГК «ЦИБИТ»

ОТ ПРОБЛЕМЫ К ТОЧКЕ РОСТА

ОПЫТ ГК «ЦИБИТ» ПО ПЕРЕВОДУ КОМПАНИИ НА УДАЛЁННУЮ РАБОТУ

ГК «ЦИБИТ» на своём опыте убедилась, что переход на «удалёнку» позволяет бизнесу не только не падать в основных показателях, но даже расти. На вопросы BIS Journal отвечают генеральный директор ГК «ЦИБИТ» Олег Вячеславович Иванов и директор по развитию Евгения Викторовна Колодина.

— Была ли компания готова к переводу сотрудников на удалённую работу? Имелся ли у вас подобный опыт?

О. В. Иванов. За 11 лет существования компании «ЦИБИТ» нам ни разу не приходилось прибегать к такой мере. Однако некоторые процессы изначально строятся исключительно на дистанционных технологиях, например обучение слушателей в Учебном центре. В данном случае трансформация не потребовалась.

Е. В. Колодина. Когда я работала в других компаниях, мне доводилось создавать структуры в регионах и, конечно, поддерживать с ними удалённую

связь. В «ЦИБИТ» я развивала этот опыт в предыдущие три года, уходя на дистанционную работу один раз в неделю. Это позволяло сконцентрироваться, сделать все дела, на которые не хватало времени в офисе, поставить задачи сотрудникам и проверить их выполнение.

— Как руководство ГК «ЦИБИТ» восприняло необходимость выстраивания нового формата? Какие были настроения в коллективе?

О. В. Иванов. Переход на «удалёнку» руководством был воспринят как должное. И как способ развития в том числе. Правильное настроение в коллективе мы поддерживаем постоянным общением руководства с сотрудниками в разных форматах. Это правило сохранилось и при переходе на жёсткий карантин.

Е. В. Колодина. Мы стараемся поддерживать комфортную атмосферу в коллективе различными способами, в том числе устраиваем различные

конкурсы. Например, каждый месяц мы определяем лучшего сотрудника — того, кто совершил какое-либо преодоление, проявил инициативу, добился роста своих достижений, и, конечно, награждаем его. В первые дни перехода на дистанционную работу мы с сотрудниками обменивались фотографиями домашних рабочих мест, делились видео своих физических тренировок, ведь домашний режим поначалу приводил к дефициту движения.

Всё это поддерживало, укрепляло дух и формировало тёплые дружеские отношения. Позже от Медиа Группы «Авангард» нам поступило предложение создать видеоролик на тему безопасного использования платёжных карт для конкурса «#БЕЗОПАСКИ». Мы оперативно написали сценарий, и я пригласила всех сотрудников принять участие в этом проекте. Каждый записал свой эпизод на телефон, и я объединила их в один клип. В результате получилось ещё одно командообразующее, объединяющее мероприятие. Ведь в этом ролике мы были все вместе!

— Каким образом организовали переход на новый формат? Сколько времени потребовалось на перестраивание процессов?

О. В. Иванов. В начале карантина особое внимание мы уделили бизнес-

Правильное настроение в коллективе мы поддерживаем постоянным общением руководства с сотрудниками в разных форматах. Это правило сохранилось и при переходе на жёсткий карантин

процессам и их формальному описанию. Именно на этом этапе открыли для себя много нового.

Также мы сконцентрировались на оформлении договорных отношений с клиентом на предоставление всех наших услуг. В этой части мы добились очень хороших результатов.

Для этого пришлось ввести несколько типов внутренних документов, которые теперь позволяют оптимизировать работу и делать исполнение процесса более надёжным, а работу — более прозрачной.

Е. В. Колодина. В середине марта мы разработали план организации удалённой работы сотрудников, который включал в себя:

- ◆ описание структуры компании;
- ◆ условия, при которых сотрудник допускается к дистанционному режиму работы;
- ◆ график и схемы коллективных коммуникаций;
- ◆ регламент взаимодействия сотрудников внутри каждого подразделения;
- ◆ регламент взаимодействия между подразделениями;
- ◆ тайминг;
- ◆ наглядные схемы бизнес-процессов и т.п.

Перестраивание процессов было проведено быстро и «по-военному» чётко. Далее что-то корректировали, но в целом благодаря дисциплине и по минутам расписанным графикам, а также благодаря самоотверженному труду и энтузиазму команды удалось не только устоять в новых условиях, но и существенно продвинуться вперёд в направлении развития бизнеса.

Помимо разработанного плана, для организации более эффективной работы компания взяла на себя оборудование комфортных домашних рабочих мест сотрудников, которым это потребовалась: была предоставлена необходимая оргтехника, дополнительные средства связи и даже удобная офисная мебель.

— Как была организована коммуникация внутри компании?

О. В. Иванов. Мы полностью сохранили график проведения плановых совещаний. Кроме того, добавили новые, например «утреннее построение». Это

Если раньше нахождение сотрудника на рабочем месте уже оценивалось как показатель результативности, то теперь неважно, где находится сотрудник. Единственным критерием качества работы является эффективность и то, какого результата мы достигаем и за какое время

короткое совещание, в котором принимают участие все сотрудники без исключения, а также озвучивается план проведения совещаний на день и в случае необходимости доводятся срочные сообщения или отмечаются знаменательные события, например день рождения сотрудника или годовщина его выхода на работу в компанию.

Е. В. Колодина. Для организации коммуникации мы используем современные средства связи: конференц-колы, webinar, Google Meet, Zoom, различные мессенджеры, CRM.

Нужно отметить, каждый день в компании проходят не только совещания руководства с тем или иным подразделением по графику, но и онлайн-встречи подразделений. Так, четыре раза в неделю проводятся тренинги по каждой из наших услуг для отдела продаж, на которых разбираются вопросы каналов продвижения, оттачиваются знания продуктов и услуг компании, рассматриваются конкретные кейсы и рождаются новые идеи.

— Каковы результаты компании по итогам перехода на удалённую работу?

О. В. Иванов. То, как компания представляется своим клиентам и партнёрам, является отражением организации в самом коллективе. Если внутри нет порядка, то ничем не добиться предоставления услуг высокого качества.

Нашим ответом первой волне пандемии было ужесточение требований к качеству наших услуг, к сокращению сроков их предоставления. И думаю, что клиент это почувствовал.

Генеральному директору пришлось изменить отношение к оценке качества работы сотрудников. Если раньше нахождение сотрудника на рабочем месте

уже оценивалось как показатель результативности, то теперь неважно, где находится сотрудник. Единственным критерием качества работы является эффективность и то, какого результата мы достигаем и за какое время.

Е. В. Колодина. Нам удалось добиться интенсификации и более чёткой структуризации всех процессов. В результате:

- ◆ повысилось качество предоставляемых услуг (оно и раньше было высоким, но сейчас мы его отточили до совершенства);
- ◆ мы разработали много инновационных решений, автоматизировали некоторые процессы, внедрили новые для нас инструменты и методы работы;
- ◆ повысили спрос на наши услуги;
- ◆ результатом стал рост компании — не только качественный, но и количественный: за период пандемии наш коллектив увеличился, практически каждое подразделение пополнилось новыми сотрудниками;
- ◆ мы вступили в дополнительные партнёрские программы, что позволило предоставлять нашим клиентам более широкий спектр услуг;
- ◆ особой популярностью стали пользоваться бесплатные тематические вебинары, которые наш учебный центр внедрил совместно с подразделениями и экспертами.

Кроме того, мы шире вышли в онлайн. Это повысило потребительскую лояльность наших клиентов, так как теперь один-два раза в месяц мы выступаем перед ними, даём полезные советы, делимся опытом и экспертными знаниями.

Я обратила внимание, что у меня изменилось восприятие. Общаясь дистанционно с клиентами, партнёрами, сотрудниками, я стала лучше

«слышать» то, что происходит вокруг. Многие лишнее ушло на второй план. При общении глаза не отвлекаются на внешнее, и я словно внутренним взглядом вижу суть событий, чувствую малейшие изменения в речи, голосе собеседников. Мозг концентрируется на главном, реагирует на всё мгновенно, и это действительно позволяет работать эффективнее.

— **Какие минусы «удалёнки» можно отметить по сравнению с привычным форматом работы?**

Е. В. Колодина. Нам пришлось чаще пользоваться сторонними курьерами, качество работы которых оставляло желать лучшего. Однако и в этом нашёлся положительный момент — мы перешли на электронный документооборот, что существенно интенсифицирует процессы взаимодействия с клиентами.

Что касается меня лично, я всегда и во всём вижу только плюсы. Я уверена, благодаря новому удалённому формату мы добились той степени концентрации на рабочих процессах, которой не имели никогда.

Возможно, минус в том, что теперь мы постоянно «находимся» на работе... Проснулись — и уже на работе. Рабочий день закончился — а мы всё ещё на работе. Ведь и дом стал работой.

Очень многие сотрудники компаний, перешедших на дистанционный режим, отмечают тот факт, что они стали работать в 2–3 раза больше. Думаю, тут может помочь дисциплина. Необходимо уметь отделять «домашнее» от «рабочего» и, конечно, делать перерывы.

— **Какие новые возможности открыла для себя компания, сотрудники, руководители?**

О. В. Иванов. Одним из положительных факторов перехода на «удалёнку» является расширение горизонтов кадрового рынка. И это стало очевидным не только по работе нашего кадрового агентства, предоставляющего услуги подбора персонала и трудоустройства, но и по собственному опыту привлечения сотрудников в коллектив группы компаний. Если раньше мы искали специалистов, проживающих

в определённом радиусе от офиса, то теперь география расположения коллектива перестала иметь такое значение. Таким образом, к нам в компанию пришли высококлассные специалисты из других городов.

Е. В. Колодина. Добавлю, что география настолько расширилась, что к вебинарам нашего учебного центра теперь присоединяются не только жители нашей страны — мы фиксируем заходы из зарубежья.

Интересный случай: один из наших экспертов выехал в другое государство буквально перед пандемией. Позже границы были надолго закрыты, и он довольно успешно работал из-за рубежа. Подхват клиентов происходил «бесшовно», так как они даже не заметили, что специалист находится не в России. Не так давно ему удалось вернуться в Москву.

— **Как сегодня работает компания?**

О. В. Иванов. Сегодня в нашей компании более чёткая слаженная работа, жёсткие регламенты проведения мероприятий, увеличение номенклатуры и повышение качества предоставляемых услуг, что позволяет добиваться более значимых результатов.

Нашим девизом стало: «Предъявляя более жёсткие требования к себе, мы помогаем соответствовать требованиям другим!»

Е. В. Колодина. Несмотря на пандемию, мы активно работаем, расширяемся, стремимся и достигаем новых вершин. Учимся новому!

Кстати, удалённый режим позволяет нам посещать дополнительные курсы по разным направлениям, чтобы повышать свой профессиональный уровень.

— **Какие наработки этого интересного опыта компания возьмёт с собой в будущее, когда необходимости в дистанционной работе уже не будет?**

О. В. Иванов. Мир изменился настолько, что возврат в предыдущее состояние практически невозможен. Поэтому для нас будущее уже наступило. А мы будем готовиться к новым вызовам и стараться адекватно на них реагировать.

Е. В. Колодина. В качестве резюме мы составили несколько простых рекомендаций, как работать с дистанционными сотрудниками или даже целыми удалёнными командами (см. врезку).

РЕКОМЕНДАЦИИ ГК «ЦИБИТ» ПО РАБОТЕ С ДИСТАНЦИОННЫМИ СОТРУДНИКАМИ



1. Внутренние коммуникации. Чётко сформулируйте, каким образом, по каким каналам и в каком объёме вы будете общаться. Как будет выстраиваться взаимодействие между всеми звеньями сотрудников организации.

2. Обозначьте общее видение и ценности компании. Все сотрудники должны одинаково понимать, для чего и для кого они работают, какие задачи стоят перед всей командой и перед каждым специалистом в частности.

3. Создайте понятную и подробную документацию для всех сотрудников. В непредвиденной ситуации человек, работающий удалённо, всегда сможет обратиться к прописанным правилам.

4. Не стесняйтесь хвалить сотрудников. Психологи отмечают: все сообщения в почте/мессенджере каждый человек читает своим «внутренним» голосом. Зачастую негатив чувствуется сильнее, а позитив может быть неверно истолкован. Поэтому не стоит стесняться хвалить сотрудников, если они этого заслужили.

USERGATE. ОТ ПАРТИТУРЫ К БОЖЕСТВЕННОМУ ЗВУЧАНИЮ

ОТЕЧЕСТВЕННАЯ ПЛАТФОРМА ДЛЯ МАСШТАБИРУЕМОЙ
ЗАЩИТЫ КИИ ОТ СЕТЕВЫХ УГРОЗ

Компания «Юзергейт» начала разрабатывать комплексные решения для защиты КИИ от сетевых угроз около 10 лет назад, уже имея к тому времени 10-летний опыт по созданию продуктов для защиты от интернет-угроз пользовательских устройств на платформе Windows.

ЗОЛОТАЯ РЫБКА В ОТЕЧЕСТВЕННЫХ СЕТЯХ

За 20 лет «Юзергейт» прошла путь от создания решений для обеспечения безопасной работы в Интернете пользовательских устройств на основе платформы UserGate Proxy&Firewall до поставщика комплексных систем защиты корпоративных сетей на основе устройств UserGate (модели UserGate C, D, D+, E, E+, F, X1), реализующих концепцию межсетевого экрана нового поколения (NGFW), анализаторов событий и инцидентов UserGate LogAn (UserGate Log Analyzer, модели E6; E14; F25) и систем управления UserGate Management Center (модели C; E), позволяющих из единого центра управлять большим количеством устройств NGFW UserGate.

Системы на основе платформы UserGate обеспечивают комплексную безопасность корпоративных сетей разного масштаба.

В нашей стране решения UserGate эксплуатируются в КИИ десятков крупных предприятий, среди которых ФосАгро, Транснефть, Газпром Межрегионгаз, Ростовская АЭС; на множестве предприятий СМБ; в госучреждениях регионального и федерального масштаба

(РГБ, Пенсионный Фонд РФ, МЧС, налоговые инспекции); в вузах.

Для решения задач по защите от сетевых угроз компанией предлагается широкая номенклатура программно-аппаратных комплексов (ПАК), работающих под управлением специально созданной и поддерживаемой компанией операционной системы UGOS.

Решения UserGate могут быть развёрнуты и на виртуальной инфраструктуре заказчика. Поддерживается работа с такими гипервизорами, как VMware, Hyper-V, Xen, KVM, OpenStack, VirtualBox. Функциональность виртуальных решений полностью эквивалентна той, что предоставляется аппаратными комплексами UserGate.

Тесная работа «Юзергейт» со ФСТЭК по сертификации своей продукции позволяет с помощью оборудования компании строить системы защиты КИИ, соответствующие не только действующим требованиям ФСБ и ФСТЭК, но и нормативным документам в сфере ИБ отраслевых регуляторов в финансовой сфере, здравоохранении, на предприятиях ТЭК, в «оборонке».

Сегодня компанией успешно пройдена сертификация ФСТЭК по требованиям к межсетевым экранам (4-й класс, профили А и Б) и по требованиям к системам обнаружения вторжений (4-й класс) для программно-аппаратных и виртуальных платформ UserGate.

Авторитет компании, базирующийся на её инженерных компетенциях и успешном ведении бизнеса (эффективность продаж и оперативная

техподдержка), лежит в основе её партнёрства с общественными объединениями и регуляторами в сфере ИБ, позволяя оперативно реагировать на требования «комплаенса», обеспечивая своим заказчикам возможность «ездить с пашечками» не только сегодня, но и в перспективе.

НЕ МОГЁМ, А МОЖЕМ!

На основе NGFW UserGate клиентами компании развёрнуты системы для управления «контентом» (интернет-фильтрация и безопасность электронной почты), для выявления и реагирования на угрозы сети и для контроля работы приложений, для управления доступом в сеть (рис.1).

Технологии обеспечения сетевой безопасности, реализованные в NGFW UserGate, соответствуют современной концепции SOAR (Security Automation, Orchestration and Response), позволяя анализировать поведение различных процессов, выявлять риски и автоматически обеспечивать на основе этого анализа адекватную реакцию, предоставляя защиту от угрозы или просто от аномального поведения на самой ранней стадии.

UserGate поддерживает аутентификацию пользователей и применение к пользователям правил межсетевого экранирования, контентной фильтрации, контроля приложений с поддержкой таких средств и протоколов аутентификации, как Active Directory, Kerberos, RADIUS, LDAP, Captive Portal, TACACS+, 2FA. Администраторы могут применить определённые политики



Рисунок 1. Решения, реализуемые на платформе UserGate

безопасности к любому пользователю, группе пользователей или, например, ко всем неизвестным пользователям.

Отказоустойчивость программно-аппаратных комплексов UserGate обеспечивается их работой в режиме высокой доступности (High Availability) за счёт резервирования и возможность кластеризации ПАК. Режим High Availability позволяет снизить риски, которые могут возникать в связи со сбоями в работе аппаратного обеспечения: при необходимости система устанавливается на парных узлах и обеспечивается автоматическое переключение нагрузки между ними в случае сбоев.

УДОБНЕЕ МАСШТАБИРОВАТЬ, АНАЛИЗИРОВАТЬ, ХРАНИТЬ

Решения UserGate конкурируют по своим функциональным возможностям с теми, что предлагают Check Point, Cisco, Dell SonicWALL, Fortinet, Juniper Networks, McAfee, Sophos, WatchGuard, Barracuda Networks, Palo Alto Networks, StoneSoft.

При этом сертификация по текущим требованиям регулятора (сертификат ФСТЭК России № 3905) и развивающиеся работы по сертификации на соответствие требованиям грядущим

(когда к обязательным новым требованиям ФСТЭК добавятся и требования МинПромТорга) — это серьёзная и обоснованная заявка на замещение решениями UserGate зарубежного ИБ-оборудования на отечественных объектах КИИ.

Сертификация ФСТЭК позволяет использовать решения на основе платформы UserGate в составе автоматизированных систем до класса защищённости 1Г, в информационных системах персональных данных (ИСПДн) и государственных информационных системах (ГИС) до 1-го класса (уровня) защищённости включительно.

Однако «шашечки» — это не повод пренебрежения удобством эксплуатации.

Для средних и крупных предприятий функциональность серверного решения NGFW UserGate эффективно дополняют возможности анализаторов UserGate Log Analyzer — специализированных серверов, которые предназначены для сбора и агрегации данных с ряда межсетевых экранов NGFW UserGate (рис. 2). При настройке NGFW UserGate администратор может указать, какие типы событий пересылаются для анализа в UserGate Log Analyzer. Опции для

выбора включают журнал событий, журнал системы обнаружения вторжений, журналы трафика, событий АСУ ТП, а также события из журнала веб-доступа.

UserGate Log Analyzer развёртывается в виде самостоятельного сервера (ПАК) либо на виртуальной инфраструктуре заказчика под управлением гипервизоров VMware, Hyper-V, Xen, KVM, OpensStack, VirtualBox.

На основании полученных данных UserGate Log Analyzer осуществляет в полуавтоматическом режиме глубокий анализ произошедших событий безопасности, определяет и отслеживает подозрительные активности отдельных пользователей или хостов, что в том числе необходимо для соответствия современной концепции SOAR (Security Automation, Orchestration and Response).

Использование UserGate Log Analyzer позволяет сопоставить результаты отчётов с установленными параметрами и обеспечить соответствие сетевой инфраструктуры требованиям корпоративной политики безопасности.

Сформированные отчёты могут автоматически отправляться по электронной почте администратору и другим уполномоченным лицам по

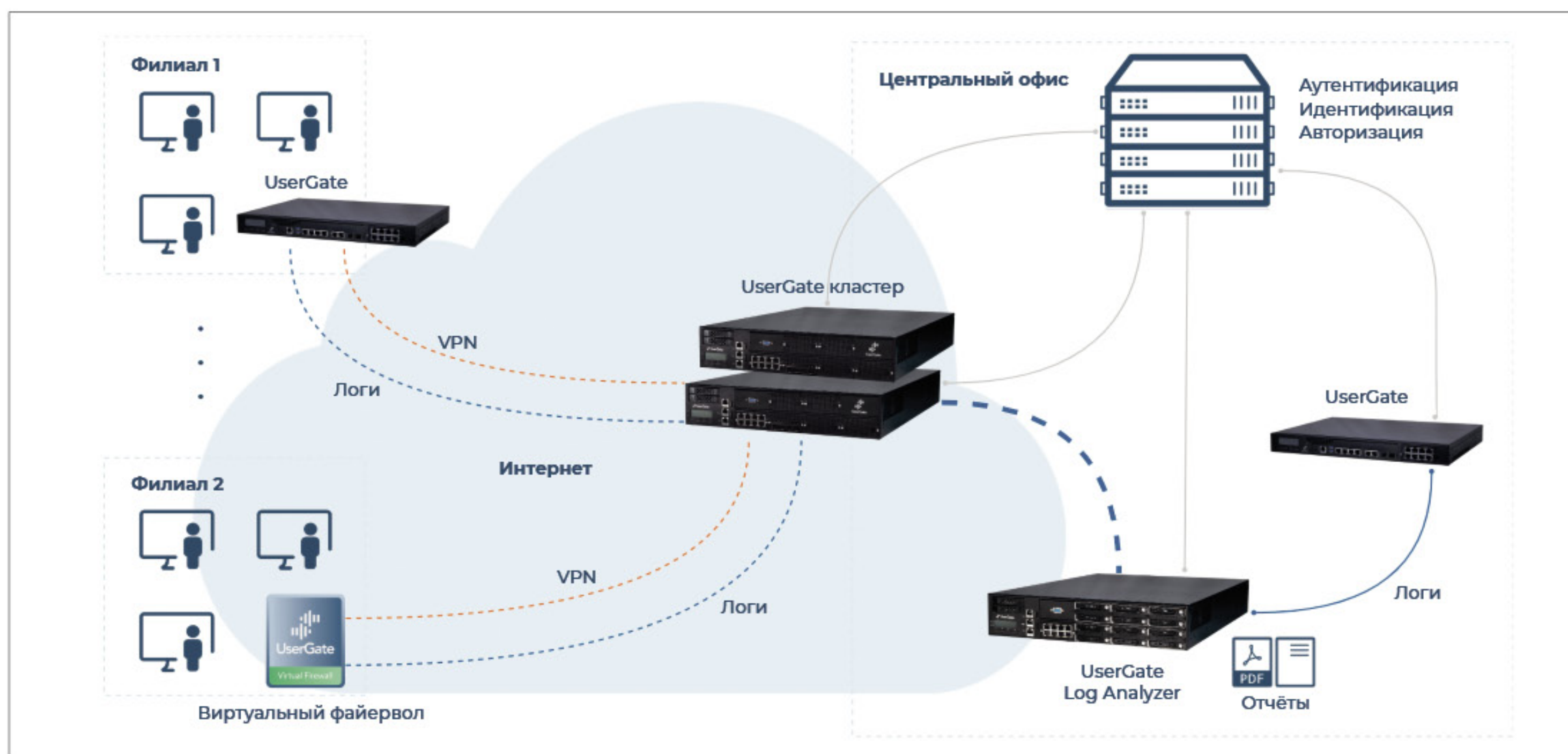


Рисунок 2. Принцип использования UserGate Log Analyzer

расписанию, в требуемое время и в указанный день недели.

В зависимости от масштаба организации (от 3 до 10 тыс. сотрудников) можно выбрать модель ПАК UserGate Log Analyzer с объёмом хранилища в 6, 14 или 25 ТБ и с производительностью от 130 000 до 530 000 записей в секунду.

Уместно заметить, что сервера UserGate Log Analyzer могут собирать данные не только с оборудования UserGate, но и со сторонних устройств, поддерживающих передачу данных по протоколам SNMP.

ПРОЩЕ УПРАВЛЯТЬ

Упростить управление большим количеством устройств NGFW UserGate позволяет программно-аппаратная консоль UserGate Management Center (UGMC) (реализованная по традиции компании ещё и в виде виртуальной платформы), которая объединяет управление устройствами в единой точке (рис. 3).

UGMC обеспечивает возможность централизованной настройки параметров работы межсетевых экранов UserGate. Это сетевые настройки, правила межсетевого экранирования, контентной фильтрации, системы обнаружения вторжений и другие настройки. Систематизировать подход к составлению настроек позволяет применение шаблонов.

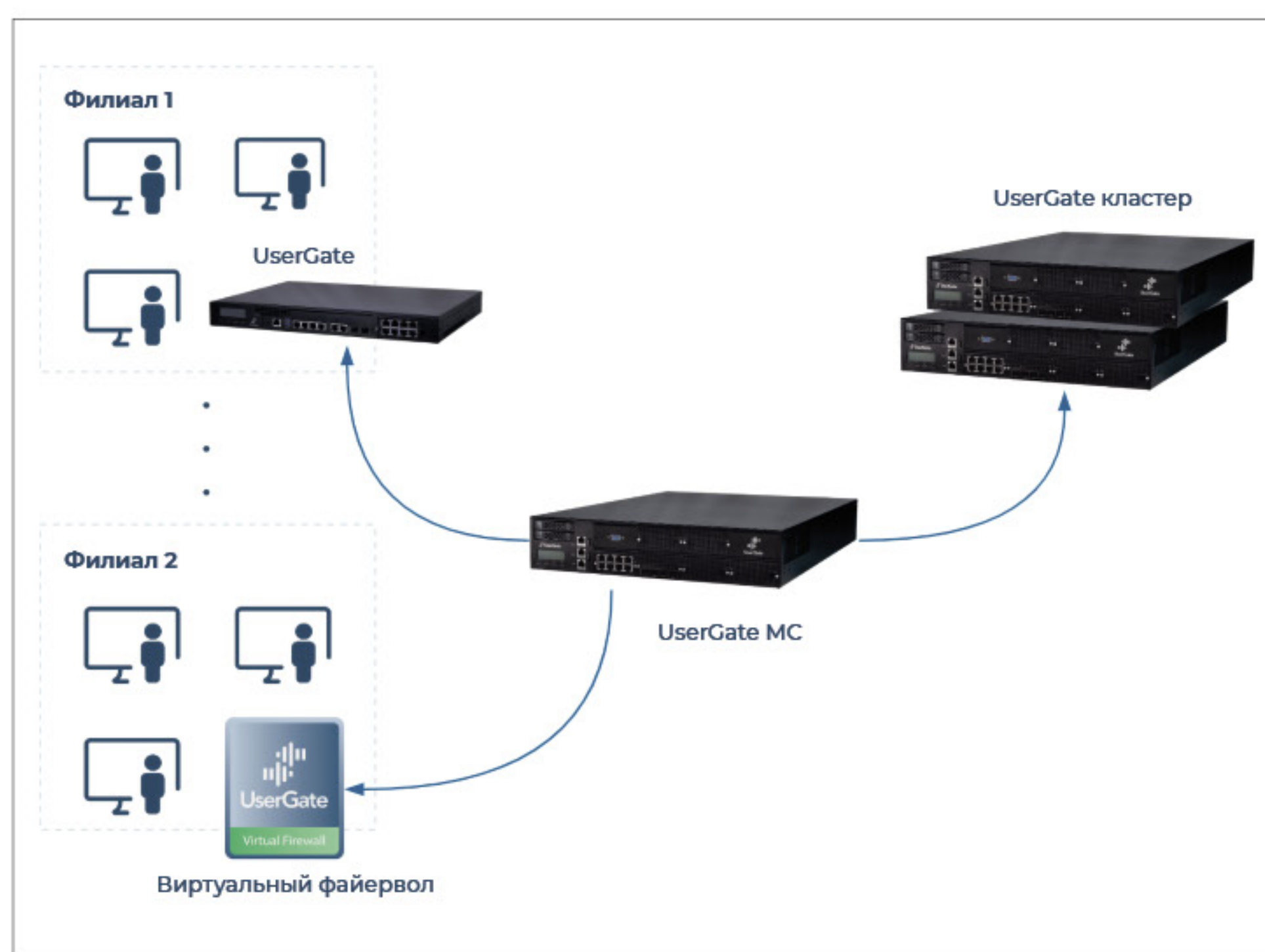


Рисунок 3. Принцип использования UserGate Management Center

ЗАБРОСИЛ СТАРИК СЕТЬ... ИЛИ КАК НЕ ОСТАТЬСЯ У РАЗБИТОГО КОРЫТА

Мировая практика (включающая и отечественный опыт) указывает на то, что должный (то есть заданный, требуемый) уровень метрик систем безопасности, в том числе и информационной, проще всего обеспечить на основе комплекта оборудования, взаимоувязанная

работа которого заложена производителем (вендором) ещё на этапе проектирования. А общая языковая среда разработчика и заказчика и географическая общность их деятельности — это своеобразный финальный аккорд в гармонии сотрудничества вендора и так называемого конечного пользователя. Начальным же является сверка «партитуры» с регулятором.



Сергей НЕЙГЕР
менеджер по развитию
бизнеса компании
«Перспективный мониторинг»

КИБЕРУЧЕНИЯ ДЛЯ ОБУЧЕНИЯ

ПЛАТФОРМА AMPIRE ПОМОГАЕТ ВЫПОЛНЯТЬ ТРЕБОВАНИЯ БАНКА РОССИИ

В настоящее время все финансовые организации живут по новому стандарту информационной безопасности — ГОСТ Р 57580.1 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер». Стандарт объёмный и сложный, содержащий более четырёхсот требований по защите информации. И основная сложность в выполнении стандарта даже не в том, что он сам по себе содержит много требований, а в том, как выстроить последовательный и непрерывный процесс обеспечения соответствия. Сотрудники кредитных организаций уже более 10 лет работают в соответствии с установленными Банком России требованиями по защите информации, хотя и для них многие требования ГОСТ Р 57580.1 в новинку; сотрудники же некредитных финансовых организаций столкнулись с такими требованиями по большому счёту в первый раз, и для них, как показывает практика консалтинга «Перспективного мониторинга» (ПМ), выполнение ГОСТ Р 57580.1 связано с большими затруднениями.

ЧИТАЯ ГОСТ Р 57580.1

ГОСТ Р 57580.1 определяет не только базовый состав мер защиты инфор-

мации для восьми процессов защиты, но и требования по управлению защитой информации. Концепция управления защитой информации по ГОСТ Р 57580.1 устанавливает необходимость подготовки и регулярного повышения квалификации специалистов по защите информации применительно к каждой области защиты информации — мера РЗИ.15 «Обучение, практическая подготовка (переподготовка) работников финансовой организации, ответственных за применение мер защиты информации в рамках процесса защиты информации». Факт обучения / повышения квалификации подтверждается наличием свидетельств, подтверждающих прохождение различных курсов и практических семинаров по соответствующим тематическим направлениям.

Компания «Перспективный мониторинг» разработала курс обучения и повышения квалификации по реагированию на инциденты для работников службы ИБ, ИТ-подразделений финансовой организации с применением учебно-тренировочной платформы Ampire. Прохождение такого курса в ПМ полностью закрывает требования по обучению и повышению квалификации для Процесса 6 «Управление инцидентами защиты информации» и Процесса 3 «Контроль целостности и защищённости информационной

инфраструктуры» ГОСТ Р 57580.1, так как специалисты, прошедшие курс, осваивают или улучшают свои навыки мониторинга событий и управления инцидентами ЗИ (процесс 6) и научатся контролировать уязвимости информационных систем (процесс 3).

АКЦЕНТ НА ПРАКТИКУ

Ampire — это целая экосистема программных технологий, которая позволяет обучать пользователей методам обнаружения признаков компьютерных атак, анализировать причины их возникновения и в конечном счёте внедрять необходимые защитные меры для противодействия им.

Основная задача, которую мы для себя ставили при разработке Ampire, — это повышение практических навыков специалистов в противодействии компьютерным атакам. И в ходе курса для сотрудников финансовых организаций акцент делается именно на практику. Они получают опыт работы с различными средствами обнаружения атак, навыки анализа логов прикладных сервисов (веб-сервера, базы данных, удалённых средств управления и т.д.), отрабатывают навыки устранения уязвимостей с помощью настройки сервисов, изменений на уровне сети абстрактной виртуальной или модели конкретной организации, внедрения межсетевых экранов, корректировки

исходного кода и т.п. Особое внимание мы уделяем отработке навыков совместной работы при расследовании инцидентов. Это выражается в жёстких требованиях по проведению анализа, включая заполнение развёрнутых форм отчётности по инцидентам в собственной IRP киберполигона Ampire.

Опыт проведённых мероприятий на нашем комплексе позволяет говорить, что занятия на нём интересны как для начинающих специалистов, так и для опытных сотрудников, желающих «прокачать» отдельные технические моменты.

ШАГ ЗА ШАГОМ

Процесс киберучений выполнен единообразно для всех шаблонов информационных систем и сценариев киберучений, поставляемых вместе с комплексом. Основные шаги следующие (см. рисунок):

1. Преподаватель создаёт тренировку на базе имеющегося шаблона, выбирая подходящий сценарий, моделирующий действия виртуального нарушителя.

2. После создания тренировки преподаватель активирует учебную компьютерную атаку на виртуальную инфраструктуру.

3. Действия виртуального нарушителя регистрируются различными системами обнаружения вторжений на уровне сети и на уровне конечных узлов.

4. Участники группы мониторинга проводят анализ зафиксированных событий при помощи СОВ и заводят карточки инцидентов ИБ.

5. Участники группы реагирования анализируют полученные карточки инцидентов ИБ, подключаются к отдельным узлам информационной системы тренировки и устраняют имеющиеся в них уязвимости.

Тренировка заканчивается, когда устранены все уязвимости в составе активной учебной компьютерной атаки, отрабатываемой в рамках тренировки, или время тренировки вышло.

Все действия атакующего автоматизированы в рамках сценария, поэтому для проведения полноценных киберучений нет необходимости привлекать «живую» атакующую команду.

При прохождении командами сценария преподаватель самостоятельно

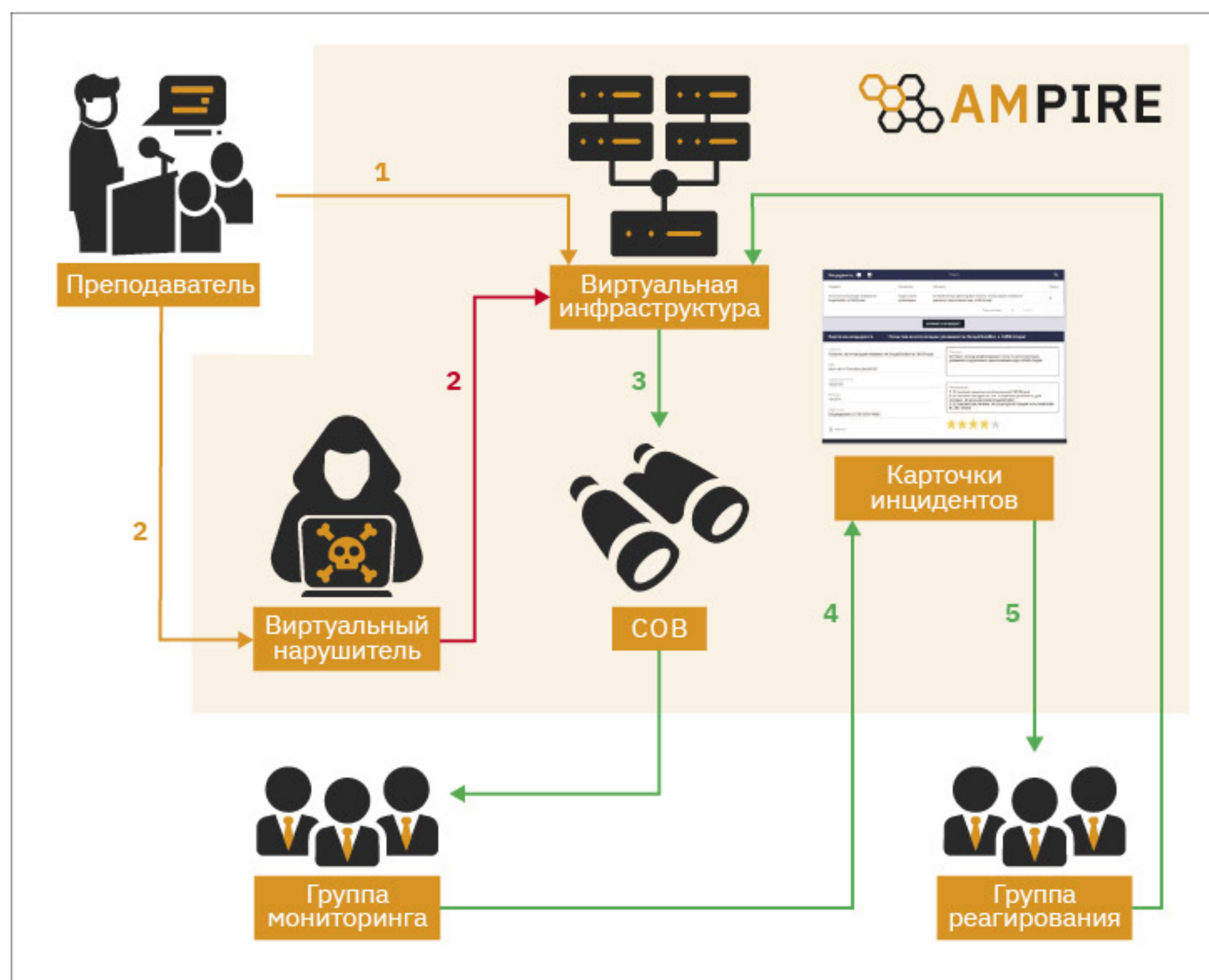


Рисунок 1. Основные шаги в процессе киберучений

управляет виртуальными нарушителями: активирует их, останавливает, даёт задание на выполнение отдельных шагов.

ШАБЛОН СИСТЕМЫ

Шаблон информационной системы в Ampire — это набор виртуальных машин (сервера, рабочие станции, сетевое оборудование и т.д.), которые моделируют работу типовой сети организации (например, офис, банк, предприятие). Состав шаблонов в комплексе определяется на момент поставки, но может быть расширен по требованиям заказчика. Эта потребность возникает в основном из-за желания проводить обучение на макетах информационных систем, максимально близких к уже существующим у заказчика. Шаблон можно дополнить специфическими для конкретного заказчика сервисами, оборудованием и средствами защиты информации (учитывая возможность работы в виртуальной среде и лицензионные ограничения).

И ОНЛАЙН, И В КЛАССЕ

Занятия на платформе Ampire можно проводить и онлайн, и в очном формате. При очном формате киберучений

группы участников работают непосредственно в классе одного из учебных заведений, оборудованных комплексом Ampire или имеющих подключение к облачной версии комплекса. С командами на месте работают один-два преподавателя, помогая отрабатывать запланированные сценарии. Преподаватели оценивают полноту и корректность заполнения форм отчётности по выявленным инцидентам, отвечают на вопросы, дают советы по процессам мониторинга, реагирования и взаимодействия команд. В онлайн-киберучениях члены команд подключаются к комплексу удалённо по VPN-каналу со своих рабочих мест.

* * *

Действенность участия в киберучениях для повышения квалификации специалистов подтверждается положительными отзывами о платформе Ampire, полученными в рамках SOC-Форума и Уральского форума «Информационная безопасность банков» от сотрудников финансовых организаций, организаций из иных отраслей деятельности.



Екатерина СТЕПАНОВА
ведущий консультант отдела
аудита и консалтинга ДИБ
АМТ-ГРУП, к.т.н.

УПРАВЛЕНИЕ РИСКАМИ?

ДАВАЙТЕ ЭТО АВТОМАТИЗИРУЕМ!

РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД

Во многих кредитных организациях уже давно сложилась практика управления рисками информационной безопасности (далее — ИБ; рисками, связанными с угрозами ИБ)¹, основанная на определении актуальных угроз ИБ и планировании мероприятий по их нейтрализации. В ходе выполняемого анализа определяются негативные факторы, в результате наступления которых возможны:

- ♦ нарушение и (или) прекращение функционирования объектов информационной инфраструктуры кредитной организации;
- ♦ несанкционированное изменение, удаление или хищение информации конфиденциального характера и нарушение режима доступа к таким данным как с использованием объектов информационной инфраструктуры, так и без использования таковых;
- ♦ случаи и попытки осуществления финансовых операций без согласия клиента;
- ♦ хищение денежных средств кредитной организации или попытка их хищения;
- ♦ эксплуатация уязвимостей информационных систем, обусловленных ошибками и недостатками процессов обеспечения ИБ организации;
- ♦ и другие последствия.

¹ Риск нарушения ИБ — риск, связанный с угрозой ИБ; РС БР ИББС-2.2-2009 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности».

Такой подход позволяет организациям обеспечивать баланс затрат на построение системы защиты информации и потенциальных потерь в результате реализации идентифицированных рисков ИБ.

Кроме того, Банк России определяет необходимость управления рисками ИБ, рассматриваемыми как часть операционных рисков² кредитной организации:

- ♦ ГОСТ 57580.1-2017³;
- ♦ 716-П⁴;
- ♦ 3624-У.

РАЗНЫЕ ЗАДАЧИ — РАЗНЫЕ МЕТОДИКИ

Необходимость учёта рисков ИБ в составе операционных рисков порождает ряд вопросов:

- ♦ Какую методику использовать для оценки рисков ИБ с целью учёта их в величине операционных рисков? Нормативные документы Банка России не предлагают методику оценки.

² Операционные риски — прямые и косвенные потери в результате несовершенства или ошибочных внутренних процессов организации, действий персонала и иных лиц, сбоев и недостатков информационных, технологических и иных систем, а также в результате реализации внешних событий; Указание Банка России от 15.04.2015 № 3624-У «О требованиях к системе управления рисками и капиталом кредитной организации и банковской группы».

³ ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер».

⁴ Положение Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе».

- ♦ Можно ли использовать значения, полученные в соответствии с имеющейся методикой оценки рисков ИБ?

Как показывает наша практика, методики оценки рисков должны быть разными.

Объясняется это, во-первых, разным пониманием термина «риск информационной безопасности». Длительное время для оценки рисков ИБ используется классический подход, основанный на определении актуальных угроз ИБ, и сейчас уже более-менее понятна последовательность действий:

- ♦ определение активов кредитной организации, для которых реализация угроз ИБ может приводить к нанесению ущерба;
- ♦ определение способов реализации угроз ИБ и уязвимых мест, за счёт эксплуатации которых возможна реализация рассматриваемого способа;
- ♦ оценка потенциального ущерба бизнесу в результате реализации угрозы;
- ♦ оценка вероятности реализации угрозы ИБ;
- ♦ вычисление значения риска ИБ.

В контексте же операционных рисков учитываются только риски ИБ, связанные с потерями кредитной организации в результате наступления определённого события. А для наступления этого события зачастую необходимы дополнительные факторы.

Например, финансовая организация может оценить риски ИБ, связанные с хищением денежных средств у клиентов в результате отсутствия механизма обеспечения безопасности. С точки зрения операционных рисков необходимо учитывать не только вероятность таких

хищений, но и вероятность обращений клиентов в финансовую организацию в целях компенсации. Таким образом, оценки не совпадут.

Во-вторых, в соответствии с 716-П не все риски ИБ необходимо оценивать количественно. Так, риски с типом потерь «качественные» допускается оценивать с использованием экспертного мнения. К таким рискам относятся потери в случаях утечки, утраты или искажения защищаемой информации.

В то же время такого рода риски чаще всего оцениваются кредитными организациями количественно — для обоснования необходимости внедрения соответствующих мер и средств защиты информации.

Таким образом, применение имеющейся в кредитной организации методики оценки рисков ИБ, основанной на анализе угроз ИБ, затруднительно: требуется адаптация используемого подхода к определению вероятности и величины ущерба или разработка отдельной методики, учитывающей специфику операционных рисков.

ВОЗМОЖНОСТИ АВТОМАТИЗАЦИИ ОЦЕНКИ РИСКОВ

Руководитель структурного подразделения, ответственного за обеспечение информационной безопасности, осознавая количество необходимых оценок рисков ИБ, часто принимает решение о необходимости автоматизации этого процесса — в настоящее время на рынке представлено множество программных продуктов, позволяющих это сделать.

Как правило, выбор падает на решения класса SGRC (Security Governance, Risk Management and Compliance). Системы позволяют проводить оценку рисков с помощью предустановленных методик (так называемые методики «из коробки»), а также дают возможность реализации пользовательской методики практически любой сложности.

Соблазнительной выглядит идея использования SGRC-систем для оценки рисков ИБ, рассматриваемой в процессах управления операционными рисками. Однако прежде чем искать возможности автоматизации, в первую очередь необходимо формализовать методику оценки рисков ИБ.

Требуется адаптация используемого подхода к определению вероятности и величины ущерба или разработка отдельной методики, учитывающей специфику операционных рисков

Также целесообразно использовать возможности систем автоматизации для подсчёта ключевых индикаторов риска (далее — КИР) и контрольных показателей уровня риска информационной безопасности (далее — КУРИБ), необходимость оценки которых определена в 716-П.

КИР И КУРИБ

КИР — количественный показатель, направленный на измерение и контроль уровня операционного риска в определённый момент времени, должен определяться таким образом, чтобы обеспечить своевременное выявление и реагирование на тенденции, свидетельствующие о возможности наступления риска.

Для того чтобы КИР действительно «работали» для обеспечения ИБ кредитной организации, а не использовались для формального «закрытия требований регулятора», необходимо максимально полно идентифицировать риски информационной безопасности, проанализировать возможные сценарии реализации угрозы ИБ и определить «слабые места», которыми могут воспользоваться злоумышленники.

К примеру, для риска ИБ, связанного с хищением денежных средств кредитной организации вследствие несанкционированного доступа к каналам ДБО банков-корреспондентов, в качестве КИР можно предложить:

- ♦ количество «сработавших» индикаторов компрометации применительно к определённому перечню хостов, на которых осуществляется подготовка или выполнение платёжного поручения;
- ♦ интегральная оценка, учитывающая совокупность и специфику выявленных индикаторов компрометации на системах, смежных с критичными хостами.

Расчёт предложенных КИР целесообразно проводить на постоянной

основе, в качестве источника исходных данных можно использовать системы класса SIEM (Security information and event management). Для обеспечения возможности агрегации исходных данных от разных систем и средств защиты информации оценку КИР можно реализовать с использованием решений класса Business Intelligence или Security Intelligence.

Автоматизация оценки количественных КУРИБ, приведённых в 716-П, также возможна с использованием решений класса IRP (Incident Response Platforms). Для этого необходимо обеспечить необходимые интеграции, настройку в IRP форм карточек инцидентов с учётом предложенной в Положении системы классификации и ведение базы событий рисков ИБ в системе.

* * *

В 716-П впервые так подробно регулятор определил процедуры, которые должны реализовать кредитные организации в отношении рисков информационной безопасности. Система управления операционным риском кредитной организации должна быть приведена в соответствие с требованиями данного документа до 1 января 2022 года, при этом с большой долей вероятности может потребоваться адаптация действующих процессов и используемых подходов, а для обеспечения своевременного выполнения регулярных оценок — автоматизация. Достаточно сжатые сроки и нетривиальность решаемых задач могут стать проблемой для кредитной организации, поэтому уже сейчас многие наши заказчики обращаются за экспертизой для формализации и автоматизации проводимых оценок.



Валерий ФИЛИН
технический директор
CITUM



Павел СТЕБЛЯНКО
генеральный директор
CITUM



Владимир СОЛОВЬЕВ
старший специалист отдела технических
решений АО «ДиалогНаука»

АВТОМАТИЗАЦИЯ ПЕНТЕСТА — МИРОВОЙ ТРЕНД

ФАКТЫ О КИБЕРУГРОЗАХ И ВЫЗОВЫ

КИБЕРУГРОЗЫ СТАНОВЯТСЯ СЛОЖНЕЕ С КАЖДЫМ ГОДОМ

Угрозы ИТ-инфраструктуре организаций непрерывно усложняются и множатся. В своём отчёте по киберугрозам¹ от сентября 2020 года компания Microsoft отмечает, что за прошедший год злоумышленники серьёзно усилили свой инструментарий, всё чаще используя легитимное программное обеспечение (PsExec, netcat, powershell и т.д.) и применяя всё более сложные техники, препятствующие обнаружению угроз и в то же время позволяющие атаковать самые защищённые цели. («Threat actors have rapidly increased in sophistication over the past year, using techniques that make them harder to spot and that threaten even the savviest targets».)

УЩЕРБ ОТ КИБЕРАТАК РАСТЁТ С КАЖДЫМ ГОДОМ

По оценкам Accenture & Ponemon Institute², в 2018 году средний годовой ущерб от кибератак в финансовом секторе составил 13 млн долларов США в расчёте на одну организацию.

Потери российской экономики в 2019 году от действий кибермошенников составили около 2,5 трлн руб. Возможный

ущерб от кибератак в 2020 году оценивается в 3,5–3,6 трлн руб.³

Средний ущерб от одного инцидента, связанного с критичными данными, оценивается в 3,86 млн долларов США⁴.

ПЕРЕВОД СОТРУДНИКОВ НА УДАЛЁНКУ ПОРОЖДАЕТ ДОПОЛНИТЕЛЬНЫЕ КИБЕРРИСКИ

Вынужденный перевод сотрудников на удалённую работу в связи с пандемией привёл к существенным изменениям в инфраструктуре и правах доступа в большинстве организаций финансового сектора. Увеличение доли удалённых сотрудников закономерно приводит к повышению рисков ИБ: домашние компьютеры, используемые в качестве удалённых рабочих мест, хуже защищены и не подконтрольны организации. В то же время оценить дополнительные риски, связанные с предоставлением удалённого доступа, без пошагового моделирования сценариев атаки, сложно.

НЕХВАТКА КВАЛИФИЦИРОВАННЫХ КАДРОВ В ОБЛАСТИ ИБ

В соответствии с отчётом (ISC)² «Cybersecurity Workforce Study, 2020» количество незаполненных вакансий в области кибербезопасности в

мире впервые в истории снизилось в 2020 году с отметки 4 млн, но всё ещё составляет непостижимые 3,1 млн⁵.

АВТОМАТИЗАЦИЯ И ПРИОРИТИЗАЦИЯ ЗАДАЧ ИБ — ОТВЕТ НА ВЫЗОВЫ СЕГОДНЯШНЕГО ДНЯ

В условиях ограниченных ресурсов важно грамотно выстраивать приоритеты по задачам ИБ. Gartner подчёркивает необходимость фокусного анализа уязвимостей за счёт оценки их практической эксплуатируемости: «Don't try to patch everything; focus on vulnerabilities that are actually exploitable». Риск-ориентированное управление уязвимостями и автоматизация анализа рисков безопасности внесены аналитиками Gartner в топ-10 проектов ИБ на 2020–2021 годы⁶.

Для реализации фокусного подхода организации требуется выполнять регулярную практическую проверку защищённости. Золотым стандартом такой проверки является тестирование на проникновение (или пентест).

НЕПРЕРЫВНЫЙ ПЕНТЕСТ

Пентест — это трудоёмкая задача, поэтому традиционно выполняется 1–2 раза в год и зачастую в ограниченном

¹ <https://blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats/>

² https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf

³ <https://www.kommersant.ru/doc/4226302>

⁴ <https://www.ibm.com/security/data-breach>

⁵ <https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx>

⁶ <https://www.gartner.com/smarterwithgartner/gartner-top-security-projects-for-2020-2021/>

масштабе. Сети современных организаций меняются существенно динамичнее, поэтому окно уязвимости между двумя последовательными пентестами является недопустимо долгим. Современный ландшафт угроз требует нового подхода — постоянное или непрерывное тестирование защищённости (рис. 1).

Можно выполнять непрерывный пентест вручную с помощью инструментов NPTT = Network Penetration Testing Tools (классификация Gartner). Однако найти высококвалифицированных пентестеров непросто, с учётом дефицита кадров на рынке. Ставка для таких сотрудников достаточно высока: не каждый позволит себе нанять в штат команду узкоспециализированных тестировщиков. И даже если в штате организации работает группа профессионалов-пентестеров, она не может гарантированно охватить всю ИТ-инфраструктуру для оценки возможных массовых векторов атак в полном масштабе и на регулярной основе. Злоумышленнику достаточно найти всего один рабочий вектор атаки, в то время как команде защитников важно обнаружить и ликвидировать все возможные векторы.

АВТОМАТИЗАЦИЯ ПЕНТЕСТА

Наиболее ценный результат даёт решение по автоматическому пентесту. Выполняя тестирование на проникновение с решением автоматизации, можно быть уверенными в том, что система найдёт все заложенные в неё векторы атак, с полным охватом «в ширину» и «в глубину», не испытывая влияния «человеческого фактора» — ничего не забывая и не упуская. При этом тестирование можно выполнять на регулярной основе: ежемесячно, еженедельно или ежедневно, — и в произвольном масштабе. Для выполнения автоматизированного теста на проникновение не требуется обладать квалификацией профессионального пентестера, что делает системы автоматизации доступными для широкого круга организаций.

Автоматизация пентеста даёт существенные преимущества:

- ◆ высокая скорость работы;
- ◆ снижение трудозатрат на оценку защищённости сети;
- ◆ снижение трудозатрат на оптимизацию защищённости сети;



Рисунок 1. Изменение уровня риска в зависимости от периодичности пентеста

- ◆ получение более быстрого результата и наглядного представления об уровне защищённости инфраструктуры по сравнению с ручным пентестом;

- ◆ быстрое и наглядное представление результатов от реализованных проектов ИБ, прозрачное обоснование для новых проектов;

- ◆ произвольный масштаб проверки за меньшее, чем при ручном пентесте, время;

- ◆ надёжный результат, не зависящий от человеческого фактора;

- ◆ анализ эффективности новых инструментов ИБ перед покупкой;

- ◆ экономия ресурсов за счёт мощной приоритизации уязвимостей и задач ИБ;

- ◆ обнаружение уязвимостей, действительно опасных для конкретной сети;

- ◆ возможность оперативного получения информации о новых векторах атак при любом изменении в ИТ-инфраструктуре;

- ◆ возможность инкрементального повышения защищённости за счёт внедрения исправлений или контрмер и мгновенной проверки результата, не дожидаясь очередного пентеста;

- ◆ возможность безопасной проверки эффективности внедрённых средств защиты, не дожидаясь реального инцидента;

- ◆ возможность регулярного тестирования эффективности процессов реагирования на инциденты, не дожидаясь реального инцидента;

- ◆ анализ защищённости без разглашения информации третьей стороне.

Всё это позволяет команде ИБ «держать руку на пульсе» рисков ИБ

организации и оперативно реагировать в случае отклонений от приемлемого уровня. Автоматизация процесса анализа защищённости позволяет экономить значительные ресурсы ИТ/ИБ за счёт фокуса на обоснованно важных задачах ИБ и оптимизации уже внедрённых инструментов ИБ вместо внедрения новых.

PCYSYS PENTERA — УНИКАЛЬНОЕ РЕШЕНИЕ НА РЫНКЕ АВТОМАТИЗАЦИИ ПЕНТЕСТА

В настоящий момент единственным продуктом для автоматизации инфраструктурного пентеста является Pcysys PenTera. В подтверждение этой мысли Gartner включил Pcysys в отчёт Cool Vendors за 2020 год в категории Security Operations and Threat Intelligence. Цитата из отчёта: «Pcysys provides an automated penetration testing solution, which is still unique in the security technology space. Pcysys' solution, PenTera, can be thought of as a human penetration tester offered as a technology. It is ideal for internal teams that are looking to replace manual penetration testing and increase the frequency of security testing». Запросить отчёт Gartner можно на сайте PCYSYS⁷.

С 2019 года в России решение Pcysys PenTera широко применяется в проектах ведущими системными интеграторами и консультантами в сфере ИБ. Успешные проекты по автоматизации пентеста уже были реализованы в организациях различных размеров и отраслей экономики.

⁷ <https://go.pcysys.com/pcysys-named-2020-cool-vendor-in-security-operations-and-threat-intelligence>



Анастасия ХАРЫБИНА
директор по развитию
AKTIV CONSULTING



Павел СЕМЁНОВ
консультант по информационной
безопасности AKTIV CONSULTING

СОМНЕНИЯ ПРОЧЬ!

ПЯТЬ ШАГОВ К ЭФФЕКТИВНОМУ АУДИТУ

Вопрос проведения аудита на соответствие требованиям ГОСТ Р 57580.1 продолжает оставаться для финансовых организаций чрезвычайно актуальным. Однако большинство компаний, подлежащих обязательной оценке соответствия, нередко опасаются аудита. Одна из причин — весьма приблизительное представление о специфике его проведения и нежелание допускать внешнего аудитора к внутренним процессам организации.

Тем не менее Банк России обозначил чёткий срок надлежащей готовности

продемонстрировать третий уровень соответствия: с 1 января 2021 года для кредитных организаций и с 1 января 2022 года для некредитных, а ИТ-инфраструктура для работы с Единой биометрической системой (ЕБС) должна пройти проверку к моменту подключения.

Ниже приведена сводная таблица требований нормативно-правовых актов по срокам прохождения проверок состояния информационной безопасности организаций (таблица 1).

Как известно, на рынке консалтинга по информационной безопасности

существуют как услуги по внедрению требований ГОСТ и разработке внутренней документации, так и услуги по сертифицированному аудиту, результаты которого принимаются Банком России. Именно о таком сертифицированном аудите и пойдёт речь в этой статье. Мы представим процесс подготовки финансовой организации как последовательность пяти конкретных шагов, а также дадим необходимые рекомендации.

ШАГ 1: ПРЕДВАРИТЕЛЬНАЯ ПОДГОТОВКА

Безусловно, оценка соответствия ГОСТ Р 57580.1 начинается с предварительной подготовки к ней, так как это позволит заранее осознанно определить все узкие места и устранить их.

Определение направлений оценки соответствия. Для начала следует чётко определиться с направлениями оценки. Формально их может быть несколько:

- ♦ инфраструктура для работы с ЕБС;
- ♦ инфраструктура для работы с платёжной системой Банка России;
- ♦ инфраструктура, обеспечивающая проведение денежных переводов;
- ♦ все ИТ-активы, обеспечивающие проведение финансовых операций.

Мы рекомендуем включать в спектр проверки сразу все упомянутые части инфраструктуры компании и проводить единый аудит. Не стоит рассчитывать на экономию, проводя несколько «небольших» оценок: практика показывает, что «скупой платит дважды», и в результате суммарно проверка потребует

Кредитные организации

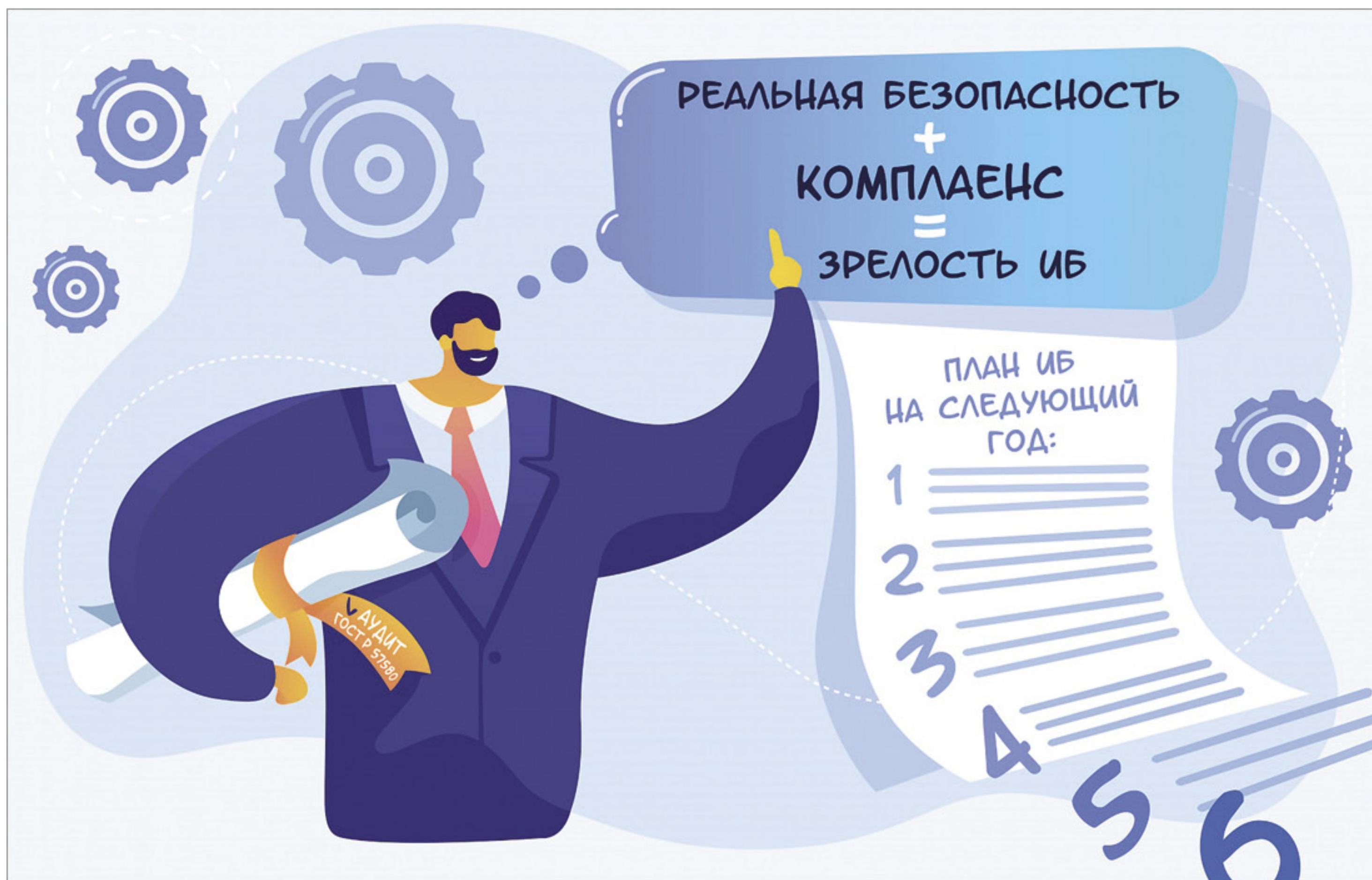
НПА	Вступление в действие в части ГОСТ Р 57580	Периодичность оценки соответствия	Дата первой оценки соответствия	Дата второй оценки соответствия
672-П	01.07.2021	1 раз в 2 года	01.01.2023 (4 уровень)	01.01.2025 (4 уровень)
683-П	01.01.2021	1 раз в 2 года	01.01.2021 (3 уровень)	01.01.2023 (4 уровень)
719-П	01.01.2022	1 раз в 2 года	01.01.2022 (4 уровень)	01.01.2024 (4 уровень)
Приказ №321	25.06.2018	ежегодно	при подключении к ЕБС	через 1 год после подключения к ЕБС

Некредитные организации

НПА	Уровень защиты	Вступление в действие в части ГОСТ Р 57580	Периодичность оценки соответствия	Дата первой оценки соответствия	Дата второй оценки соответствия
684-П	стандартный	01.01.2021	1 раз в 3 года	01.01.2022 (3 уровень)	01.07.2023 (4 уровень)*
	усиленный		ежегодно		

* для НФО с усиленным уровнем защиты информации дата второй оценки не должна быть позже 1 года с момента первой оценки

Таблица 1. Сроки прохождения проверок состояния ИБ организаций



большого объёма собственных ресурсов. Дополнительно мы рекомендуем распространять требования ГОСТ Р 57580.1 на всю инфраструктуру целиком, что позволит упростить задачу с определением контуров безопасности и избежать защиты межконтурного взаимодействия. Крупные компании, у которых значительная часть инфраструктуры поддерживает деятельность, не связанную с финансовыми операциями, могут и не следовать такой рекомендации, но даже им будет полезно выполнять требования ГОСТ для всей инфраструктуры.

Проведение самооценки. После определения направлений оценки необходимо своими силами провести самооценку. Её цель — определить примерный уровень соответствия в разрезе процессов ГОСТ на текущий момент, поэтому совершенно нет необходимости собирать свидетельства и соблюдать высокую точность оценки. Обычно такая процедура занимает 2–3 дня.

Распространённые пробелы. По завершении самооценки станут наглядно видны основные пробелы в реализации

Устраняя недостатки в преддверии проведения сертифицированного аудита, важно обратить внимание на общее количество требуемых доработок

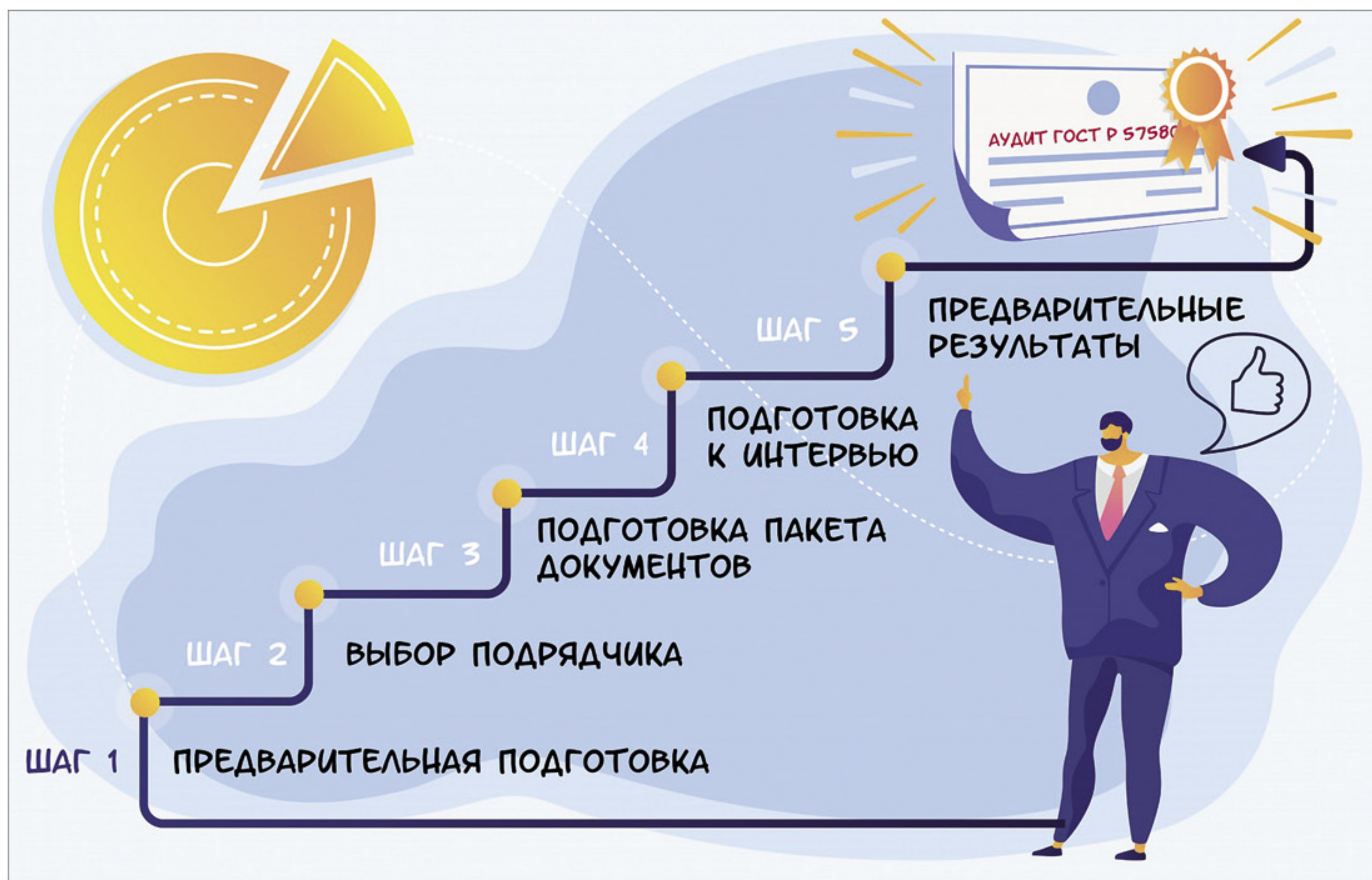
требований ГОСТ. Исходя из нашего опыта, можно выделить ряд типичных недостатков.

Во-первых, это слабая регламентация процессов обеспечения информационной безопасности и общая декларативность внутренних нормативно-правовых актов (НПА). Зачастую такие акты содержат описания требований без малейшего намёка на то, как именно эти требования нужно выполнять в реальности. Во-вторых, нерегулярность в проведении контрольных проверок службами информационной безопасности, отсутствие подробной фиксации результатов подобных проверок в соответствии с требованиями Раздела 8 ГОСТ Р 57580.1–2017.

Устранение недостатков. Устраняя недостатки в преддверии проведения сертифицированного аудита, важно

обратить внимание на общее количество требуемых доработок. Если их немного и они понятны, то целесообразно выполнить улучшения самостоятельно. Если доработок много или имеется непонимание требований ГОСТ, стоит обратиться к консультантам, дабы избежать временных и финансовых затрат и неопределённого результата.

Подготовка технического задания. В случае если итоги повторной самооценки будут удовлетворительными, следующим этапом станет подготовка технического задания на проведение внешнего аудита. Важно не упустить момент и подготовить задание ещё до начала рассылки запросов коммерческих предложений аудиторским компаниям, так как это даст возможность корректно оценить стоимость проекта при соблюдении всех необходимых условий.



Мы бы рекомендовали включать в техническое задание на аудит описание области оценки соответствия, а также отразить собственные ожидания от результатов аудита в части глубины консалтинговых услуг. Это позволит потенциальному аудитору понять, сколько ресурсов следует выделить для обеспечения надлежащего качества работ, и сформировать адекватное коммерческое предложение. Иначе в процессе реализации проекта может выясниться, что область проверки намного больше или что заказчик ожидал не общие рекомендации по улучшению, а подробные по каждому требованию. Качество планирования работ напрямую зависит от детализации технического задания.

Дополнительно в техзадание можно включить описание порядка обмена конфиденциальной информацией и урегулирования спорных ситуаций, что впоследствии также поможет сэкономить ресурсы и повысит эффективность.

ШАГ 2: ВЫБОР ПОДРЯДЧИКА

Формально при выборе подрядчика на выполнение аудита кибербезопасности

финансовых организаций есть только одно ограничение: наличие лицензии ФСТЭК на техническую защиту конфиденциальной информации, включающей подпункты Б, Д или Е. Таких компаний сегодня насчитывается более 2500, при этом их подавляющее большинство никогда не работали с финансовыми организациями и не знакомы с отраслевой спецификой. Поэтому очень важно при рассмотрении потенциального исполнителя убедиться в наличии у аудитора значительного опыта работы с финансовыми организациями. Обязательно познакомьтесь с потенциальной аудиторской компанией, задайте профильные вопросы аудиторам, а также воспользуйтесь рекомендациями коллег по цеху, обладающих практическим опытом подобного сотрудничества.

Что касается выделяемого на проведение аудита кибербезопасности бюджета, тут важно учесть, что при минимальных затратах ряд задач в рамках проверки финансовой организации придется делегировать собственным сотрудникам, что противоречит самой

идее внешнего аудита. К тому же существует весомый риск получения неадекватно высокой оценки состояния кибербезопасности, что впоследствии приведет к неизбежным предписаниям со стороны Банка России во время надзорных мероприятий.

ШАГ 3: ПОДГОТОВКА ПАКЕТА ДОКУМЕНТОВ

После того как подрядчик выбран, договор заключен и установочная встреча проведена, необходимо предоставить аудитору пакет документов для анализа. Правильная подготовка этого пакета — один из важнейших этапов всей оценки соответствия, так как позволяет аудитору быстро войти в курс дел в проверяемой организации и сразу оценить выполнение большей части требований, что значительно экономит ресурсы на проект. Как же подготовить его правильно?

Обычно аудитор помогает это сделать, высылая опросники или списки документов, также он описывает удобный для себя формат этого пакета. Например, просит сгруппировать

документы в разрезе процессов ГОСТ, так как это значительно экономит время при анализе.

Также в пакет нужно включить не только действующие документы, но и проекты нормативно-правовых актов, так как за время аудита они могут перейти в статус официальных и стать свидетельствами выполнения требований ГОСТ. Очень удобно в пакете видеть и планы мероприятий по ИБ, например планы проверок на год и отчёты об этих проверках. Кроме контрольных мероприятий, желательно включить информацию о проектах по внедрению тех или иных мер защиты информации, это также станет свидетельством.

Для снижения количества вопросов по документации желательно сразу включить в пакет списки и краткие описания ИТ-активов, попадающих в область оценки соответствия, а также логические схемы корпоративной сети. В этом случае аудитор сможет самостоятельно понять большую часть взаимосвязей объектов и не задавать лишних вопросов.

Заочный диалог. В процессе анализа собранного пакета документов аудитор неизбежно запрашивает дополнительную информацию, но, как правило, вынужден долго ждать ответа или переносить вопросы на этап интервью, что в итоге увеличивает длительность проекта. Чтобы этого избежать, мы рекомендуем всегда быть на связи и оперативно давать комментарии. Не нужно бояться привлекать к этому смежные подразделения, которые являются держателями процессов или владельцами систем, так как они могут помочь предоставить недостающую информацию.

ШАГ 4: ПОДГОТОВКА К ИНТЕРВЬЮ

Следующий важный этап — подготовка к интервью, которое будет проводить аудитор непосредственно на площадках компании. Ответственному за проект по оценке соответствия необходимо провести внутреннее согласование плана интервью для того, чтобы оно прошло быстро и гладко. Для этого мы рекомендуем запросить примерный список вопросов для раскрытия и назначить по нему ответственных сотрудников. Затем нужно зафиксировать

Аудитор может выявить несоответствия или какие-то нарушения требований ИБ, но непредоставление информации для корректной оценки одного требования ведёт к отсутствию важных свидетельств выполнения других требований ГОСТ

даты и длительность интервью и согласовать получившийся план со всеми участниками процесса.

Участниками интервью будут не только представители ИБ- и ИТ-служб, но и сотрудники бизнес-подразделений, об их осведомлённости мы уже говорили выше. Для комфортного диалога с аудитором желательно предупредить всех участников, что во время интервью он будет собирать свидетельства и наблюдать за процессами, находящимися в области оценки соответствия. В целом основная цель приезда аудитора — сбор свидетельств. При этом у аудитора нет намерений «завалить» организацию как на экзамене, ведь он заинтересован в объективной оценке положения дел. Безусловно, аудитор может выявить несоответствия или какие-то нарушения требований информационной безопасности, но непредоставление информации для корректной оценки одного требования ведёт к отсутствию важных свидетельств выполнения других требований ГОСТ и, как следствие, к занижению итоговой оценки.

ШАГ 5: ПРЕДВАРИТЕЛЬНЫЕ РЕЗУЛЬТАТЫ

После работы непосредственно в компании аудитор консолидирует всю имеющуюся информацию, запрашивает некоторые уточнения и озвучивает предварительные результаты оценки соответствия вместе с краткими рекомендациями. Данный этап важен тем, что он позволяет обсудить спорные моменты и найти компромиссы, поэтому очень важно выделить достаточно времени на изучение предварительных результатов.

Мы рекомендуем оценить подробность и понятность данных аудитором рекомендаций, чтобы в дальнейшем внутренним специалистам по информационной безопасности в компании было легко с ними работать. Оценивать нужно

не только рекомендации или невыполненные, по мнению аудитора, требования, но также и выполненные, так как его аргументы и собранные свидетельства могут неточно отражать реальность. При этом свои комментарии мы рекомендуем раскрывать детально, так как формулировка «здесь мы не согласны» совершенно непродуктивна и только затянет процесс. Гораздо эффективнее, если комментарий будет иметь отсылку на не учтённый аудитором абзац в Политике информационной безопасности или содержать скриншот, подтверждающий реализацию требований. Также не следует бояться признавать выявленные недостатки системы информационной безопасности, потому что, как показывает практика, на этом этапе их возможно очень оперативно устранить и повысить оценку с учётом рекомендаций аудитора.

АУДИТ ПРОЙДЕН. ЧТО ДАЛЬШЕ?

Как только оценка соответствия будет завершена, отчёты получены и документы подписаны, нужно начинать готовиться к следующей оценке. На основе рекомендаций аудитора и в соответствии с целями организации следует подготовить план мероприятий по улучшению процессов ГОСТ и согласовать его как с руководством компании, так и со смежными подразделениями. Это позволит им быть в курсе действий службы информационной безопасности и при необходимости запланировать собственное участие.

В итоге в компании должен быть запущен постоянный продуктивный процесс по улучшению зрелости информационной безопасности, цель которого не только гарантировать соответствие ГОСТ и другим стандартам, но и обеспечить достижение бизнес-целей компании через осознанное управление рисками.



Анна МИХАЙЛОВА
менеджер по развитию бизнеса
группы компаний Angara

РАБОТАЕМ ВМЕСТЕ, РАБОТАЕМ ХОРОШО

ИНЖЕНЕРНЫЙ ЦЕНТР ANGARA PROFESSIONAL ASSISTANCE БЕРЕТ НА СЕБЯ ВСЕ РУТИННЫЕ, ТРУДОЕМКИЕ И НЕТИПОВЫЕ ЗАДАЧИ ПО ПОДДЕРЖКЕ ИБ-СИСТЕМ ЗАКАЗЧИКОВ

Управление распределенным комплексом средств защиты современной организации — это трудоемкая и высокотехнологичная задача. Когда у отдела ИБ не хватает ресурсов для массовых работ, компетенций для поддержки и тюнинга систем, есть ограничение бюджета для развития собственного штата профессионалов, оптимальным решением становится обращение в профильную сервисную организацию.

ВОЗМОЖНОСТИ ИНЖЕНЕРНОГО ЦЕНТРА

Angara Professional Assistance предлагает услуги технического сопровождения и аутсорсинга эксплуатации систем ИБ на базе Инженерного центра (ИЦ), позволяющие передать сервис-провайдеру выполнение рутинных, трудоемких и нетиповых задач по администрированию и обеспечению работоспособности систем ИБ компании. Обеспечение эффективной и бесперебойной работы средств защиты информации имеет критическую важность для любой компании, так как в случае неработоспособности или неполноценной настройки инструментов, направленных на защиту организации, компания мо-

жет оказаться под угрозой потери или компрометации данных. Кроме того, возрастает риск репутационных потерь.

Использование услуг профильного инженерного центра позволяет получать гарантированно высокий уровень поддержки и обслуживания систем на всем протяжении сервисных контрактов с заказчиком, пользоваться накопленной экспертизой и опытом инженерного состава, который аккумулируется со всех поддерживаемых инсталляций и решений, диверсифицировать риски ухода или удержания в своем штате высококвалифицированных специалистов и дают возможность снизить нагрузку на собственный персонал без увеличения штата сотрудников.

Работая в тесном сотрудничестве с экспертами всех практик группы компаний Angara, эксперты ИЦ оказывают услуги по сопровождению ИБ- и ИТ-систем таких направлений, как:

- ♦ межсетевые экраны, системы обнаружения и предотвращения вторжений, URL и спам-фильтры;
- ♦ системы противодействия утечкам информации, системы анализа защищенности;
- ♦ системы противодействия вредоносному ПО, атакам нулевого дня и целенаправленным атакам;

♦ системы защиты от НСД, средства доверенной загрузки и средства защиты виртуализации;

♦ системы защиты БД, анализа действия привилегированных пользователей;

♦ системы анализа и корреляции событий, системы контроля изменений конфигураций;

♦ криптографические шлюзы, системы организации удаленного доступа;

♦ системы управления учетными записями и привилегиями, системы сквозной аутентификации, а также системы управления смарт-картами, USB-ключами и биометрическими данными;

♦ инфраструктуры Microsoft: системы доменных имен, почтовые серверы, службы каталогов, системы аппаратной виртуализации.

На сегодняшний день на поддержке ИЦ находится более 120 различных ИБ- и ИТ-продуктов. В перечне вендоров — все крупнейшие производители средств защиты, представленные на российском рынке: «Лаборатория Касперского», «Код Безопасности», Palo Alto Networks, Trend Micro, Positive Technologies, «Гарда технологии», InfoWatch, Krontech, F5 Networks, Fortinet, R-Vision и другие.



Рисунок 1. Основные показатели Инженерного центра



Рисунок 2. Сервисы Инженерного центра

Для части вендоров ИЦ является авторизованным сервисным партнером. Например, является сервисным центром (Authorized Service Center, ASC) для Palo Alto Networks. Полученный статус позволяет оказывать клиентам на прямую квалифицированную техническую поддержку по всей линейке решений Palo Alto Networks на родном языке.

Помимо этого, у центра есть партнерские соглашения с вендорами на предоставление на базе их решений сервисов по подписке (модель Security as a Service). Например с «Лабораторией Касперского». Что говорит о высокой квалификации инженерного состава.

Работа ИЦ подразумевает полный цикл сопровождения систем, от предоставления решения по заявкам заказчиков, мониторинга работоспособности подконтрольного программно-аппаратного комплекса и решения инцидентов с высоким уровнем SLA (по критичным инцидентам — не более 10 минут) до конфигурирования, развития и регламентных работ по сопровождаемым системам.

«Мы понимаем, что нет одинаковых заказчиков, и каждому бизнесу важно решать максимально эффективно те задачи, которые перед ним стоят. Именно поэтому своим клиентам мы предлагаем конструктор сервисов при выборе обслуживания, в котором можно указать необходимые услуги и уровни обслуживания: от помощи в сопровождении, развитии или планировании системы ИБ до максимального уровня аутсорсинга и профессиональных сервисов, сервисов MSSP в соответствии со спецификой продукта», — комментирует Оксана Васильева, руководитель Angara Professional Assistance.

Инженерный центр обеспечивает поддержку как небольших моновендорных, так и крупных комплексных мультивендорных информационных систем заказчиков из разных секторов экономики. В частности, ИЦ оказывает крупнейшее комплексное сопровождение инфраструктуры одного из ведущих телеком-операторов России, а также поддержку и эксплуатацию 10 ключевых систем безопасности, более 35 000 рабочих станций и более 100 000 программных компонентов на всей территории РФ для федеральных органов исполнительной власти.

Работы выполняются любым удобным для клиента способом: удаленно с выездами на объекты эксплуатации систем и/или с постоянным присутствием специалистов на объекте эксплуатации сопровождаемых систем.

Только в 2020 году, несмотря на пандемию, эксперты ИЦ выполнили более 200 командировок на объекты клиентов по всем федеральным округам РФ. А за три последних года количество обрабатываемых обращений выросло более чем в 3 раза, в частности, для клиентов из банковского сектора — почти в 10 раз.

КАЧЕСТВО И УДОБСТВО

Для обеспечения высокого качества услуг, предоставляемые решения тестируются и апробируются в рамках собственной лаборатории, имеющей виртуальные профили, заточенные как под отдельные инсталляции клиентов, так и под разные версии поддерживаемых продуктов.

В качестве лабораторной среды в компании используется гиперконвер-

гентное решение Nutanix, объединяющее СХД и серверы в единое устройство.

Под каждый сервисный проект выделяется персональный сервис-менеджер, все работы сопровождаются регулярной отчетностью об оказанных услугах сопровождения, независимо от выбранного уровня сопровождения, что повышает прозрачность и качество услуг.

Перед началом действия сервисного контракта, сервис-менеджер проводит установочные встречи, где знакомит с командой, согласовывает матрицу коммуникаций, рассказывает основные принципы работы с клиентским порталом. Поэтому, когда контракт уже начат, заказчик не только знает объем услуг и уровень SLA, прописанный в контракте, но и команду, которая его сопровождает, и инструменты, которые можно использовать для коммуникаций.

Каждому заказчику предоставляется доступ в личный кабинет, где он, помимо регистрации, просмотра и изменения зарегистрированных обращений, может оценить уровень предоставляемых услуг и в режиме онлайн просмотреть статистику, включая процент выполнения SLA по предоставляемым услугам.

В своей работе Инженерный центр в полной мере применяет современные стандарты ITIL для сервисных практик.

«Вместе с клиентом мы формируем общее видение, ясные для бизнеса цели уровня услуг, их целевые показатели и оценки. Нахождение постоянно с клиентом на связи позволяет оперативно корректировать возможные отклонения от ключевых показателей сервисов», — заключает Оксана Васильева.



Игорь НАЛИВАЙКО
коммерческий директор
ООО «Кванттелеком»

БИЗНЕС-ВЕТВЬ ПОТОМКОВ ЛАНДАВШИЦА

BIS JOURNAL БЕСЕДУЕТ С ДИРЕКТОРОМ КОМПАНИИ
«КВАНТТЕЛЕКОМ» О КВАНТОВОМ РАСПРЕДЕЛЕНИИ
КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

Компания ООО «Кванттелеком» была учреждена в 2014 году группой энтузиастов, выпускников Университета ИТМО (Санкт-Петербург). Задача, поставленная перед компанией, была сформулирована предельно просто: создать отечественное производство систем квантовой связи, в том числе, квантовой криптографии. В очень упрощённом виде принцип квантовой связи может быть пояснён следующим образом: один бит информации передаётся одним квантом света. Такой канал передачи информации невозможно «вскрыть». Без преувеличения, в перспективе речь идёт о создании новой, высокотехнологичной отрасли промышленности.

Уже через несколько лет компания вошла в число лидеров рынка квантовых коммуникаций. Залогом успеха стало удачное взаимодействие с фундаментальной и прикладной наукой. Молодая команда выпускников Университета ИТМО сумела построить высокотехнологичный бизнес, используя лучшие традиции отечественной школы оптики, информатики, радиофизики, оптического материаловедения.

Удачный выбор научного направления и практические успехи с первых же шагов существования фирмы позволили очень быстро заявить о себе, получить заметное внешнее финансирование. В 2014 году ООО «Кванттелеком» становится резидентом Сколково, а в 2018 году стратегическим партнёром компании становится инновационная телекоммуникационная компания АО «СМАРТС».

В настоящее время ООО «Кванттелеком» выходит на рынок с целой линейкой продуктов для систем квантового распределения ключей (система КРК) для шифрования/дешифровки информации, передаваемой по телекоммуникационным сетям:

- ◆ система квантовой криптографической выработки и распределения ключей;
- ◆ источники и детекторы фотонов для систем квантовых коммуникаций;
- ◆ квантовые генераторы случайных чисел.

На вопросы BIS Journal отвечает коммерческий директор ООО «Кванттелеком» Игорь Наливайко.

— Хорошо известно, что в начале любого дела важно договориться о единстве терминологии. И здорово, когда используемые термины и понятия близки и к физической реальности, и отвечают нормам родного языка. В связи с этим первый вопрос:

насколько сформировалась терминология в той области, в которой работает ваша компания? Насколько, например, отвечает нормам русского языка в контексте представлений о физике и технике процесса термин «квантовое распределение ключей»?

И что всё-таки используется в СКРК — кванты света (множественное число) или одиночные фотоны (единственное число)?

— Существуют как системы КРК, использующие настоящие одиночные фотоны (например, с использованием спон-

танного параметрического рассеяния света), так и системы, использующие ослабленное лазерное излучение, в котором по статистике Пуассона один фотон есть в одном из 5–10–20 импульсов (в зависимости от избранного протокола).

Если говорить именно о формулировке «квантовое распределение ключей», то, на мой взгляд, она соответствует языковым нормам. Ведь технологии квантовой коммуникации именно квантовыми методами (с помощью одиночных квантов света) осуществляют распределение ключей по волоконным (или атмосферным) оптическим линиям связи.

В качестве методов шифрования могут использоваться известные системы с доказанной криптографической стойкостью, например, Шифр Вернама (одноразовый блокнот). «Квантовое распределение ключей» позволяет распределить эти ключи между удалёнными объектами и при этом гарантировать невозможность подслушивания в линии связи.

Уместно заметить, что разработка технологий квантовых коммуникаций имеет более чем 30-летнюю историю, поэтому терминологию можно считать сформировавшейся. Органы стандартизации — в России это ТК-26, за рубежом — профильные комитеты ETSI и ITU — выпускают и актуализируют методические указания, включающие в том числе и определения тех или иных терминов, часто используемых в квантовых коммуникациях. Сотрудники нашей компании принимают участие в создании подобных «методичек», так что можно сказать, что терминология формируется и нашими силами тоже.

— В информации о конкурентных преимуществах решения «Кванттелеком» фигурирует «технология рассылки ключа на боковых частотах». Одна из ассоциаций, всплывающих после прочтения такого текста, — утверждение кого-то из великих о том, что если учёный не может объяснить суть своих штудий школьнику, то это не только проблема школьника. В связи с этим возникает вопрос: можно ли в объёмах, существенно меньших тома Ландавшица по электродинамике сплошных сред, пояснить, альтернативой каких иных техноло-

Чтобы не зависеть от других производителей, мы ведём разработку собственного «источника фотонов», то есть лазера, «приёмника», то есть детектора, и устройства кодирования — модулятора света

гий «рассылки ключа» является «рассылка ключа на боковых частотах», используемая «Кванттелеком», и каковы достоинства этой технологии?

— До появления технологии КРК на боковых частотах в начале 2000-х годов была популярна так называемая «двухпроходная схема», в которой для компенсации поляризационных искажений сигнала в ВОЛС квантовый сигнал дважды проходил путь от отправителя к получателю, что замедляло скорость генерации конечных ключей. Для улучшения этой характеристики системы КРК нами была применена технология рассылки ключа на боковых частотах. Этот подход обладает рядом достоинств:

- ♦ можно сгенерировать несколько пар боковых частот, что позволяет передавать на каждой паре либо свой ключ, либо просто увеличивает пропускную способность, при этом, как и в двухпроходной схеме обеспечивается автокомпенсация поляризационных искажений сигнала;

- ♦ наша система может выпускаться как со счётчиком фотонов в приёмном устройстве (весьма нетривиальное и недешевое устройство) так и с устройством когерентного приёма, балансным гомодинным или гетеродинным детектором, что позволяет уменьшить габариты и стоимость приёмного устройства.

— Общее представление об аппаратной платформе, необходимое для реализации СКРК очевидно: источник фотонов (квантов), устройство (схема), формирующее «ключ», устройство шифрования, устройство (схема), принимающее «ключ» и зашифрованное «сообщение», устройство (схема) декодирования «сообщения». В связи с этим возникает ряд вопросов: имеются ли уже комплекты конструкторской и технологической документации на производство

этих (и возможно других) устройств? Насколько уникальны должны быть рабочие навыки производственного персонала и цеховое оборудование для реализации конструкторских задумок в «железе»? Насколько проблемным может оказаться снабжение производства материалами?

— Да, компанией «Кванттелеком» разработан полный комплект конструкторской и технологической документации на наши устройства. Чтобы не зависеть от других производителей, мы ведём разработку собственного «источника фотонов», то есть лазера, «приёмника», то есть детектора, и устройства кодирования — модулятора света. Компания «Кванттелеком» тесно сотрудничает с производителями материалов, необходимых для нашего оборудования, при необходимости мотивируя разработки нужных нам материалов.

— Знания, опыт, технологии живут не только в документации, но и в людях. Даже, возможно, в первую очередь в людях. Как налажено или планируется налаживать передачу и развитие наработок компании «Кванттелеком»?

— Конечно, самый главный наш актив — это люди, которые занимаются разработкой. Одна из важнейших задач, решаемых компанией «Кванттелеком» — возвращение молодого поколения специалистов, способных генерировать новые идеи в области квантовых коммуникаций, поддерживать и «актуализировать» имеющиеся разработки. Сотрудниками «Кванттелекома» в партнёрстве с Университетом ИТМО разработаны образовательные программы в области квантовых коммуникаций для бакалавров и магистров. Мы плотно работаем с факультетом фотоники и оптоинформатики Университета ИТМО, в стенах которого и зародилась, по сути, наша компания.



Александр БОДРИК
обозреватель BIS Journal

SOC-ФОРУМ LIVE 2020

ЦЕЛЕСООБРАЗНОСТЬ ПРОТИВ НЕОПРЕДЕЛЁННОСТИ
В ЭПОХУ ЦИФРОВОЙ ОБОРОНЫ

СОС-Форум Live 2020 оставил послевкусие 20-летнего портвейна — крепкий вкусный напиток, приятно опьянивший и зарядивший азартом. После него возникло ощущение движения, расширения мира и новое, по сути, желание не стоять на месте, обновлять энтотеку. Впрочем, в трезвом состоянии мы все пока держим цифровую оборону против последствий биологической угрозы — пытаемся не уронить уровень 2019 года.

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

Пленарное заседание СОС-Форума давно вышло за пределы заглавной тематики. И в этом году, по мнению

заместителя председателя правления Сбербанка Станислава Кузнецова, основой для киберустойчивости организаций, безусловно, является СОС, но значимый вклад в обеспечение кибербезопасности банка внесли также и платформы автоматизации безопасности (вероятно, SOAR — прим. автора), «озёра данных» в ИБ, DLP и «белые хакеры». По его словам, сегодня для развития и поддержания кибербезопасности мировой нормой является 12–15% от бюджета ИТ (рост в 1,5–2 раза за последние 10 лет — прим. автора), но Сбер и другие крупные российские компании тратят значительно меньше (банки около 3%), что может принести до 3,5 триллиона рублей убытков от действий.

Тем временем серьёзный удар приходится на граждан. По данным Станислава Кузнецова, за год количество мошеннических звонков выросло в два раза, и теперь каждый 12-й звонок в России — мошеннический. А вот эффективных национальных мер для адресации проблемы киберпреступности в условиях удалённой экономики пока не внедрено, поэтому киберпреступность за год выросла в 30 раз.

Со своей стороны первый заместитель директора ДИБ ЦБ РФ Артём Сычёв выразил опасение, что это лишь проба пера киберпреступности, настоящая волна накроет банки и их клиентов через год-два. В том числе нужно ожидать атак, связанных с OpenAPI и развитием экосистем.

Продолжая тему кибербезопасности банковской отрасли, была отмечена актуальность программ осведомлённости, и на этот раз такие программы дошли не только до сотрудников и клиентов, но и до топ-менеджмента. По словам руководителя департамента кибербезопасности Альфа-Банка Виталия Задорожного, чтобы качественно управлять рисками кибербезопасности бизнеса, бизнес должен понимать, какие решения он принимает и за что платит.

Функцией CISO в такой ситуации становится правильная коммуникация проблем бизнеса в кибербезопасность и понятная коммуникация проблем кибербезопасности в бизнес (на уровне бизнес-партнёра правления). Например, важно говорить об оттоке клиентов (customer churn), так как он может быть вызван в том числе и проблемами кибербезопасности.

Тем временем в чате SOC-Форума Live описали ситуацию, когда шифровальщик зашифровал большое количество данных, но генеральный директор не согласовал развитие функции ИБ.

А согласно мнению вице-президента по ИБ Ростелекома Игоря Ляпунова, осведомлённость населения в вопросах кибербезопасности может стать тем драйвером, что повысит спрос В2С-рынка на кибербезопасность (возможно, и того самого генерального директора — прим. автора).

А возможно, толку не будет, пока ИБ не научится готовить коммуникацию чётко под аудиторию. Например, что такое «горизонтальное перемещение» (цитата из буклета участника выставки) для представителя бизнеса? Не уверен, что все специалисты по ИБ угадают здесь lateral movement, и беда тут в том, что такой литературный подход — тенденция. В конце концов именно так, из-за усталости бизнеса и неумения безопасников понятно выражаться, ИБ может дойти до назначения на роли CISO специалистов по маркетингу или PR.

ЭКСПЕРТНЫЕ ДОКЛАДЫ

В докладе Ивана Мелехина («Информзащита») были подсвечены критически важные при аутсорсинге мониторинга ИБ моменты: как определить, что именно и как будет делаться при

аутсорсинге. Напомню, что на старте ракеты небольшое отклонение превращается в большую проблему потом. В мире SOC старт — это техническое задание. Кроме понятной истории формирования ожиданий, техническое задание на аутсорсинг сервисов мониторинга ИБ может помочь при смене подрядчика, проверке работы подрядчика, проработке претензий к качеству и как «шпаргалка» по составу работ.

Для эффективного выбора провайдера сервиса и работы с ним желательно договориться «на берегу» насчёт контролируемых источников событий и площадок, потока данных на входе, функциональности сервиса, SLA и параметров контроля сервиса. Важно также описать, какие документы должны быть на выходе сервиса (требования к документированию), с какими системами должен интегрироваться SOC, какие уже существуют компоненты SOC — система централизованного сбора логов, SIEM, вычислительные мощности и лицензии на другие системы, другие части SOC, например EDR и т.д.

А вот Игорь Залевский («Ростелеком-Солар») в докладе о современных киберугрозах рассказал о покупке за 350 рублей доступа в сеть крупной организации на киберпреступном маркетплейсе, а также о новой реализации старой истории (уязвимости в веб-площадках киберпреступников) — path traversal в данном маркетплейсе.

Переходя от работы команд защиты к работе команд атаки (RedTeam), Александр Зайцев («Лаборатория Касперского») подсветил ряд лучших практик для проведения redteam-проектов. В качестве целей симулированных атак он рекомендовал такие, как хищение интеллектуальной собственности, остановка производства и осуществление финансовых транзакций. Собственно, те же, что и цели реальных атакующих (прим. автора). В качестве стандартов организации работы:

- ◆ Hong-Kong — ICAST (2016).
- ◆ Singapore — AASE (2018).
- ◆ UK — CBEST (2014).
- ◆ The Netherlands — TIBER-NL (2016).
- ◆ EU TIBER-EU (2018).
- ◆ NATO — Cyber Red Teaming (2015).
- ◆ Saudi Arabia — FEER (2019).

КЛЮЧЕВЫЕ МЫСЛИ

Следующие восемь докладов «выжаты» каждый в одну ключевую мысль:

◆ Владимир Дрюков («Ростелеком-Солар»): за пять лет мы переходим к противодействию профилю действий злоумышленника (прим. автора: на Западе это называли intelligence-driven security ещё в 2010 г.).

◆ Данила Луцив (SecurityVision): без enrichment framework аналитики SOC неэффективны и выгорают.

◆ Александр Бондаренко (R-Vision): корпоративные сети скомпрометированы постоянно (прим. автора: некоторые зрелые и нестандартно мыслящие SOC в России специально не выдворяют злоумышленников — лучше держать их под колпаком, чем не знать, с какой стороны они ещё придут).

◆ Сергей Солдатов («Лаборатория Касперского»): автоаналитик (робот) ошибается реже живого при триаже (прим. автора: в контексте «Лаборатории» — почему нет? В контекстах других задач и другого разнообразия данных ситуация может быть другой).

◆ Алексей Павлов («Ростелеком-Солар»): ответственность за выполнение требований регуляторов передать невозможно (прим. автора: мысль не нова, но заслуживает постоянного повторения).

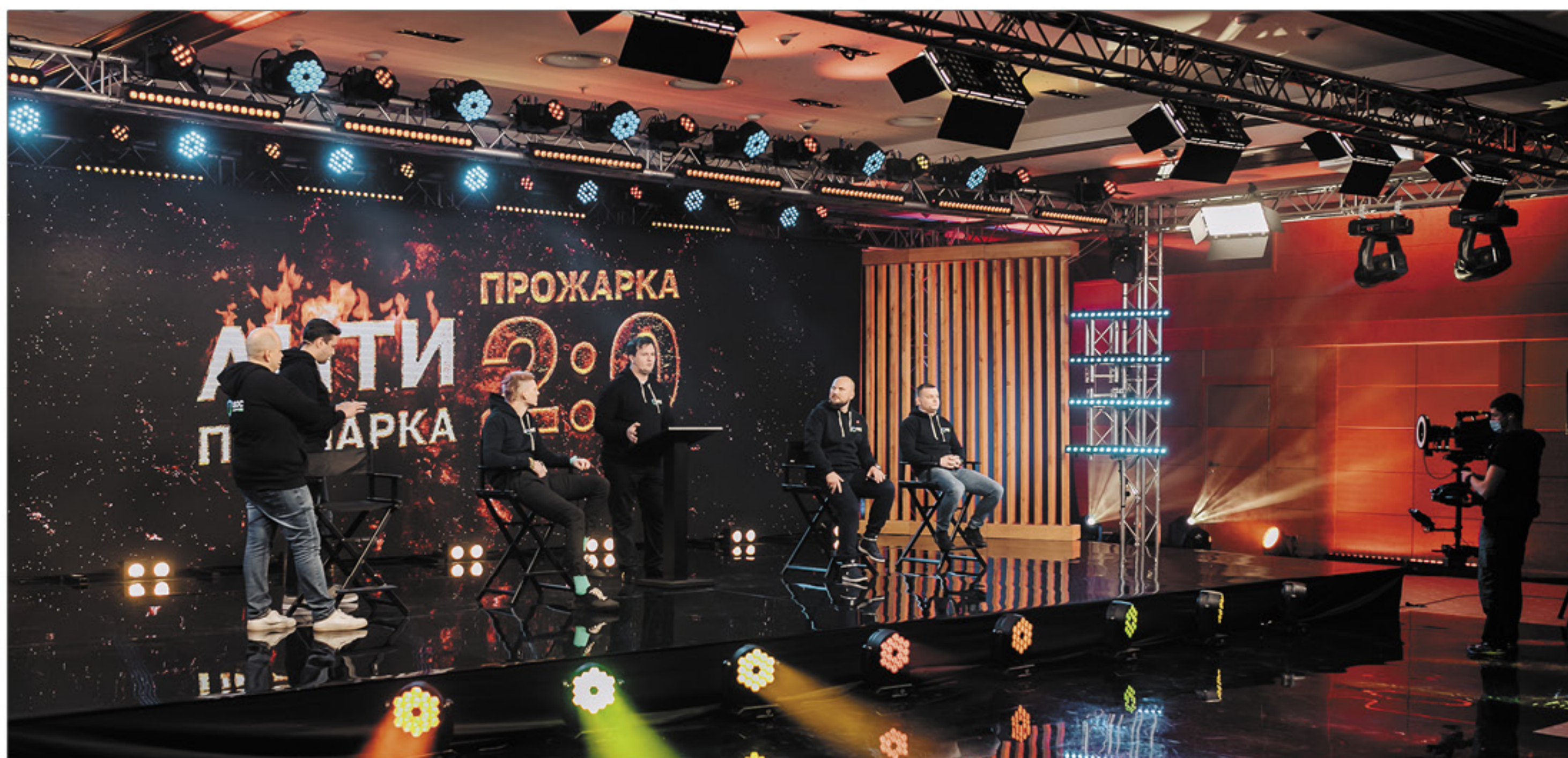
◆ Сергей Рысин (CISO ГТЛК): примерно через год использования SIEM стало понятно, что текущим штатом специалистов инциденты обработать не сможем, в итоге обратились к аутсорсингу.

◆ Антон Кокин (CISO ТМК): гибридный SOC оптимален с точки зрения скорости реализации сервисов мониторинга и объёма инвестиций для быстро развивающейся глобальной трубной компании.

◆ Александр Лимонов (CISO «Леруа Мерлен Россия»): что коммерческая IRP/SOAR, что IRP/SOAR с открытым кодом — и то, и другое требует наличия в штате выделенного специалиста с соответствующими компетенциями. Мы выбрали IRP/SOAR с открытым кодом.

МЕРОПРИЯТИЯ ФОРУМА

Были на форуме и специальные мероприятия: антипленарка, сессия «Опыт ошибок в SOC» и круглый стол о SOC в АСУ ТП.



На антиплеларке Владимир Дрюков рассказал историю о проблемах аутсорсинга SOC без технического контроля на стороне клиента и проблеме фальшивой коммодитизации SOC на тендерах — «все кошки ночью серые» (с точки зрения клиентов). Там же выяснилось, что наличие высокого, красивого и известного CISO — это конкурентное преимущество при формировании имиджа департамента ИБ организации, о чём стоит задуматься HR, если стратегия ИБ подразумевает наём большого количества специалистов.

Сессия «Опыт ошибок в SOC» фокусировалась на проблемах, связанных с эффективностью аналитиков при удалённой работе. Оказалось, эффективность аналитиков падает при полностью удалённом режиме работы, и нужно налаживать коммуникации дополнительно. Здесь же поставщики услуг мониторинга ИБ посетовали на отсутствие рациональности у определённых пожеланий потенциальных клиентов. Например, подключение источников происходит без учёта актуальных сценариев атак и профилей действий потенциальных атакующих.

А на круглом столе стало понятно, что SOC не просто научились собирать данные с популярных контролеров (Siemens, Schneider Electric и др.), но стали чётко представлять архитектуру сред АСУ ТП. А также задумываются,

как верно коммуницировать результаты работы ИБ в АСУ ТП руководству (дашборды). При этом характер беседы показал, что никаких чётких стандартов задачи мониторинга ИБ АСУ ТП нет, и даже не видно, когда таковые появятся. Судя по этому и по тому, что из пяти участников круглого стола лишь один представлял клиента, проекты по мониторингу ИБ АСУ ТП можно назвать спорадическими.

Отдельное спасибо организаторам за элементы фитнеса и красоты. Кстати, о фитнесе на удалёнке говорили и на американском онлайн-форуме SOCstock.

SOC-ФОРУМ (РОССИЯ) VS SOCSTOCK (США)

На следующий после SOC-Форум Live день на другом конце планеты американский SOAR-вендор Simplify провёл конференцию SOCstock. SOCstock оказался слабее и меньше SOC-Форума Live, в частности, в США фокусировка на мониторинге ИБ КИИ намного меньше, чем у нас, и в целом количество SOC с сервисами мониторинга (в отличие от аутстаффинга) в разы меньше на доллар ИБ-бюджетов, чем в России.

Впрочем, в паре моментов SOCstock преуспел. Удалось создать живую предметную дискуссию лидеров SOC о ежедневной операционной работе, а также привлечь эксперта (Антон Чубакина)

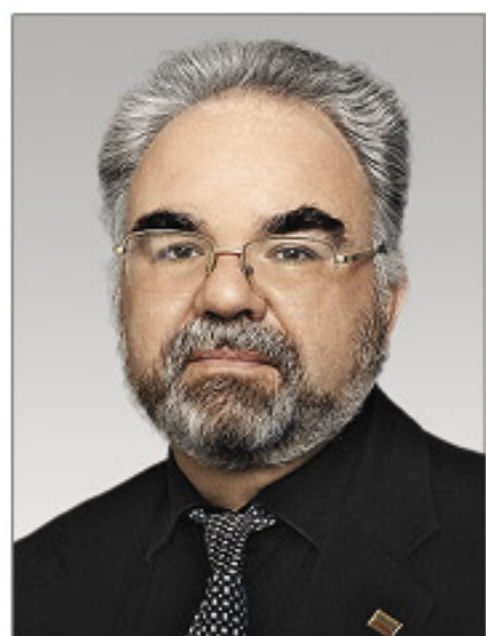
с отличным верхнеуровневым взглядом на развитие индустрии SOC (helicopter view) сквозь года.

РЕЗЮМЕ

SOC-Форум Live 2020 вышел отличным зеркалом SOC-индустрии в России, которая, если по-честному, находится в глобальном тупике. Внутри страны так и не появилось законодательства, требующего от организаций раскрытия утечек персональных данных, а как показывает практика создания SOC в развитых странах, без этого в среднем непонятно, зачем коммерческой организации выстраивать мощный центр мониторинга — нет мотивации руководства и акционеров. Экспортная история тоже проблематична. Тут частично постарались международные партнёры, а частично сама Россия, так и не отменившая валютный контроль и ряд других «граблей» для экспортёров.

Каким будет выход из положения? Возможно, он найдётся в обеспечении безопасности облаков, возможно, в трансформации затрат на ИБ в сервисную модель и предоставлении ИБ из облака... А возможно, и в оказании сверхэффективных услуг на базе открытого ПО или в комбинированном предложении киберстраховок и сервисов мониторинга ИБ.

Время покажет.



Алексей ЛУКАЦКИЙ
эксперт BIS Journal

СКАЧОК В СТОРОНУ ЗРЕЛОСТИ

МОНИТОРИНГ ИБ. ЧТО ИЗМЕНИЛОСЬ ЗА ГОД И КУДА
ДВИЖЕТСЯ РЫНОК?

СОС-Форум Live, прошедший в прошлом декабре, задал очень высокую планку для отечественных онлайн-мероприятий. И всё благодаря удачно найденной комбинации докладов и развлекательной части, вовлеченности участников и дискуссий. В отличие от львиной доли других онлайн-семинаров и конференций, которые проводились за время самоизоляции, и которые без особых потерь можно было просто посмотреть в записи, пропустить прямой эфир СОС-Форум Live было бы большой потерей. Но все-таки оставим в стороне хвалебные дифирамбы и попробуем оценить текущее состояние сегмента центров мониторинга ИБ и реагирования на инциденты, взяв за основу предположение, что на форуме выступали лидеры в этой области. Дополнили эту картину около десяти проектов по проектированию и аудиту СОС, в которых мне довелось принимать участие в ушедшем году.

НЕ ВЫРЫВАЯ ВОЛОС ИЗ ГОЛОВЫ

В целом, я бы охарактеризовал отечественный сегмент СОСов как выросший из детских штанишек, когда все спорят о том, какая SIEM лучше. Заказчики уже готовы рассматривать аутсорсинг центров мониторинга, особенно на первых порах обращения к

этой теме, когда нет ни ресурсов, ни квалификации, а задачу решать надо. Но со временем, когда растет и понимание стоящих задач, и есть возможность нанять квалифицированные ресурсы, многие возвращаются к модели «сделай сам» («Do-It-Yorself»), но уже на совершенно другом уровне зрелости. Производители и интеграторы перестали продавать SIEMы, сосредоточившись на новых дорогих игрушках — SOAR, TIP, IRP и т.п. Ну а хаке-ры живут своей жизнью, не оценивая зрелость своей деятельности, а просто зарабатывая деньги, оптимизируя под это свои процессы и инструменты. При этом стоит помнить, что действительно сложных атак, за которыми стоят иностранные государства, сегодня менее 1% (рис. 1), и поэтому задачу построения корпоративного СОС сегодня можно решить за вполне приемлемые

деньги, не вырывая из головы волосы от того, что мы не можем противостоять целому государству.

ПРО СКУЧНЫХ РЕГУЛЯТОРОВ

Начать краткий обзор мне хотелось бы с регуляторов, которые так и не нашли времени, чтобы сказать что-нибудь полезное. Да, я не ждал, что они поделятся тем, как они сами мониторят свои собственные инфраструктуры (а это было бы очень интересно). Но один регулятор, ФСТЭК, установила требования к аутсорсинговым центрам мониторинга, а также разработала два национальных стандарта — по мониторингу ИБ и по решениям класса SIEM. Поэтому ее позиция была более чем интересна для всех интересующихся этой темой. Особенно в отношении деятельности СОСов в условиях пандемии. Например, можно ли осуществлять

На стороне заказчика	На рынке ИБ	На стороне хакеров
• Нехватка персонала. Бюджеты проще выделить на SOCaaS, чем на хайринг • Нежелание отдавать ИБ на сторону • Низкая квалификация	• Дорогостоящие решения для построения СОС — SIEM, SOAR, IRP, TIP... • Аутсорсинг на определенном отрезке дешевле, чем DIY (CapEx vs OpEx)	• Большинство инцидентов краткосрочны (несколько часов) • Реальных АРТ — меньше 1%

Рисунок 1. Текущее состояние рынка мониторинга ИБ. Взгляд с трех сторон

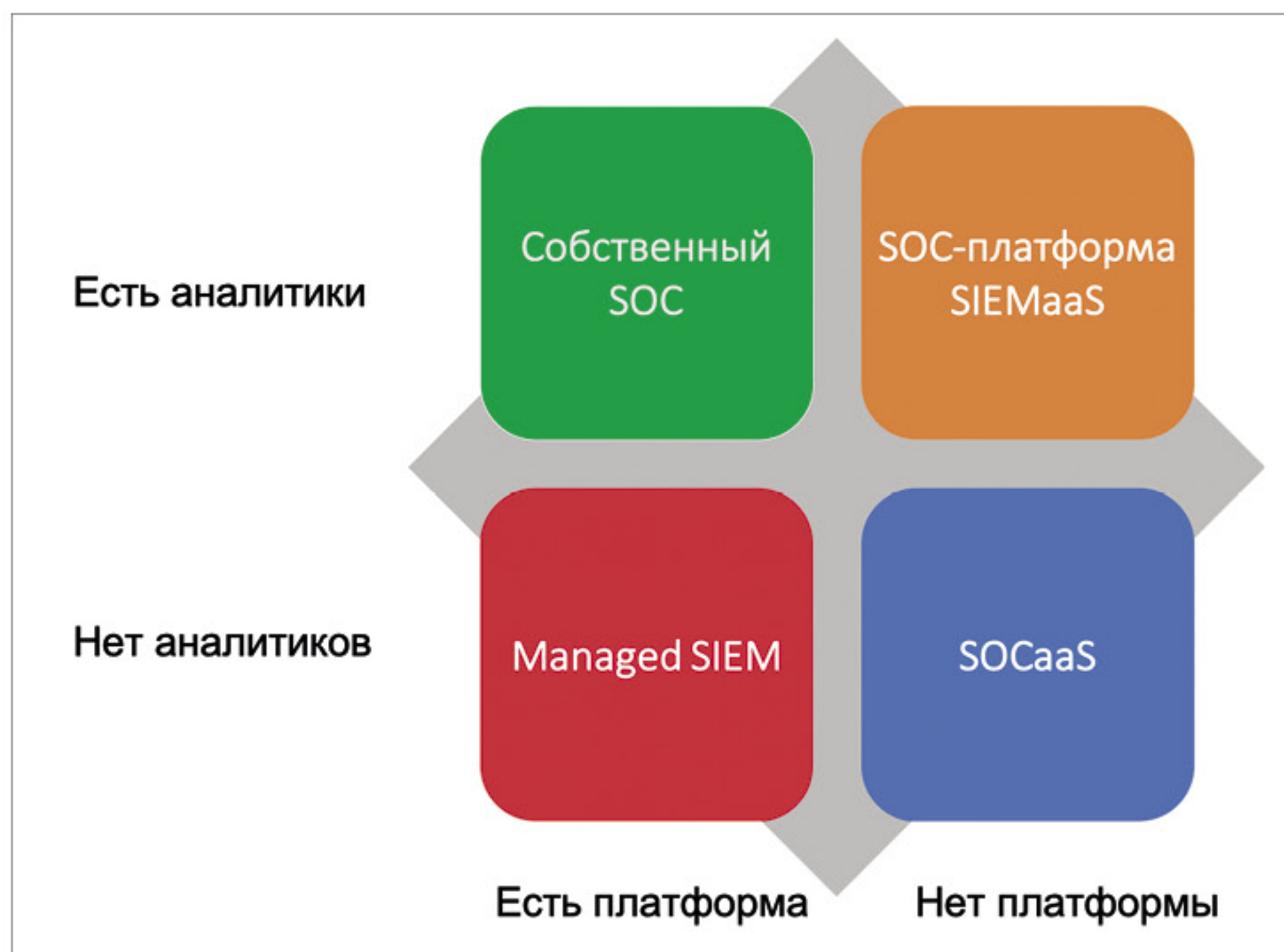


Рисунок 2. Варианты альтернатив построения SOC

деятельность по мониторингу из дома? А как сочетаются требования ФСТЭК по привязке SOC к физическому адресу, указанному в лицензии, с такой модной современной темой как мобильные или виртуальные СОСи? Наконец, очень интересным представляется вопрос о возможности применения облачных SIEM, особенно зарубежных, в деятельности российских СОСов. Формально, это запрещено как требованиями по лицензированию, так и законодательством по безопасности КИИ, однако у нас есть лицензиаты ФСТЭК, которые не чураются использования таких решений.

От второго регулятора хотелось бы увидеть, спустя три года после выхода закона о безопасности КИИ, давно обещанных рекомендаций по реагированию на инциденты, но увы... Выступление представителя НКЦКИ было достаточно скучным. Вроде бы ГосСОПКА и НКЦКИ существуют уже не первый год, но доклады по-прежнему строятся вокруг «присылайте данные по инцидентам в НКЦКИ и мы обработаем их в нашей TИP». Неужели нет ничего более интересного, что НКЦКИ мог бы рассказать для специалистов? Как работает TИP? Какой жизненный цикл и workflow по получаемым и обрабатываемым данным? Каково

распределение по типам инцидентов за время, прошедшее с прошлого SOC-Форума? Статистика должна была накопиться уже достойная, и она явно не секретная, чтобы ее утаивать...

Но если не хочется делиться практикой, расскажите про нормативку. Почему на методических рекомендациях по реагированию на инциденты висит «гриф»? Как решать вопрос с передачей данных об инцидентах дочкам иностранных компаний (эта тема уже несколько лет «висит» и НКЦКИ обещал ответить на нее еще в позапрошлом году)? Когда и какие появятся требования к средствам ГосСОПКА, о которых говорится и в приказах ФСБ и в проектах НПА Правительства и Президента по импортозамещению в КИИ? Да много каких вопросов накопилось к регулятору именно в контексте реагирования на инциденты. Но нет... Жаль...

ПРО АУТСОРСИНГ

Вернемся, однако, к SOC-Форуму Live. Большую долю докладов составляли рассказы со стороны представителей аутсорсинговых центров мониторинга. Этим отличался этот форум от всех предыдущих, на которых превалировали доклады тех, кто строил SOC для себя. С одной стороны, это говорит о

постепенном развитии этого сегмента, когда процессы уже частично выстроены и можно начать предлагать их внешней аудитории, не стесняясь брать за это деньги. А с другой, есть и ряд нюансов, которые должны быть учтены при использовании этой модели. Да, аутсорсинг — модель полезная и интересная. И особенно там, где хочется фокусироваться на основных компетенциях, а все непрофильное отдать вовне и уйти от капитальных затрат в сторону операционных. Но есть у этой модели (помимо всего прочего) и такой отрицательный момент, как отсутствие роста внутренних компетенций сотрудников и потеря производительности.

Поэтому, когда в штате есть квалифицированные сотрудники и не хочется терять их квалификацию в связи с переходом в аутсорсинговый SOC, можно посмотреть на альтернативные варианты решения задачи мониторинга ИБ, которых существует несколько. Разумеется, все они применимы в том случае, когда у нас есть персонал, но нет возможности и ресурсов для покупки и развертывания технических платформ SOC, в ядро которых входит система сбора, анализа и корреляции событий (SIEM), платформа автоматизации реагирования на инциденты (SOAR или IRP), платформа анализа угроз (TIP) и платформа для коммуникаций и обмена знаниями. Вот их-то и можно попробовать зааутсорсить, оставив у себя все компетенции и не попадая в полную зависимость от партнера.

Возможных альтернатив построения SOC, а точнее его технологического ядра, я бы назвал еще две, которые встречаются в тех случаях, когда у заказчика есть инструменты, но нет людей, и наоборот, есть люди, но нет инструментов для мониторинга. В этих вариантах можно использовать варианты Managed SIEM (кто-то управляет вашим, когда-то купленным SIEM) и облачные SIEM или SOC-платформа соответственно (рис. 2). Первый из них в России не представлен (хотя на Западе популярен), а вот второй вполне доступен. И хотя большинство игроков облачных SIEM/SOC-платформ тоже зарубежные, в России представлено, как минимум, два из них — Cisco и Microsoft.



Рисунок 3. Потребители услуг SOC, которым рынок предлагает свои услуги

КУДА НЕ СПЕШАТ АУТСОРСЕРЫ?

На форуме я заметил и еще одну, не очень хорошую тенденцию. Аутсорсеры не всегда желают делиться своим опытом. Они готовы рассказывать о том, почему заказчики обращаются к теме SOC и какие ошибки последние допускают, в расследовании каких серьезных инцидентах они участвовали, какие лицензии у них есть и как они их получали и т.п. Но вот поделиться более приземленной, но гораздо более интересной именно для практического использования информацией об индикаторах компрометации, об извлеченных уроках, об используемых инструментах и т.п., почему-то аутсорсеры не спешат.

Но, конечно, есть и исключения. Например, такой процесс как гитхабизация ИБ дошел и до России, и отечественные специалисты стали участвовать на общественных началах не только в подготовке и экспертизе нормативных актов регуляторов, но и в обмене опытом и разработке практических рекомендаций по мониторингу и реагированию на инциденты. Например, в рамках международной инициативы OSCD (Open Security Collaborative Development) существует ряд проектов, в которых участвуют российские специалисты, а именно в совместной разработке правил Sigma для обнаружения угроз, которые можно использовать в рамках тестов Atomic Red Team, обнаружения инцидентов в TheHive и Cortex, в сценариях RE&CT и т.п.

АНАЛИТИКИ ТОЖЕ УСТАЮТ

Другим интересным изменением стало обращение к теме усталости аналитиков SOC. Я в свое время на SOC-Форуме делал доклад о психофизиологических особенностях работы аналитиков центров мониторинга ИБ, о психологической слепоте, о пропусках из-за этого атак, и о том, как решить эту задачу. На SOC-Форуме Live эту тему, которая становится заглавной и на международных конференциях по SOCам, также не обошли вниманием, что говорит о том, что времена, когда SOCстроители фокусировались только на технических вопросах построения центров мониторинга, постепенно проходят, и они уже задумываются о том, как сделать свою работу эффективнее.

ПРО ОЦЕНКУ ЭФФЕКТИВНОСТИ SOC

К этому же направлению можно отнести и тему проверки способности SOC выполнять свои задачи. Да, до нормальной оценки эффективности и применения метрик ИБ дело еще не дошло, но качественная оценка того, насколько эффективен SOC и его аналитики, уже начинает проводиться более активно, чем раньше. В первую очередь речь идет о киберучениях, которые позволяют выявить слабые места как в процессе обнаружения инцидентов и реагирования на них, так и в коммуникациях между различными специалистами и командами SOC.

Вообще, я бы сказал, что 2020 год прошел под знаком киберучений и

киберполигонов, которые устраивали и проводили многие компании. Думаю, эта тема продолжится и в 2021-м году и первым крупным мероприятием, где будут проведено сразу несколько разноплановых и разноформатных киберучений по ИБ, станет форум «Кибербезопасность. Наши дни», который пройдет под Магнитогорском во второй половине февраля.

ПРИЯТНО ВСПОМНИТЬ, ПОЛЕЗНО СРАВНИТЬ

Прошлогодний SOC-Форум Live коренным образом отличался от того, что происходило на первом SOC-Форуме в 2015 году. Тогда я даже написал, что это был не SOC-Форум, а SIEM-Форум или даже Arcsight-Форум, так как очень уж много говорилось о конкретных технических решениях. Сегодня SOC-Форум стал гораздо более зрелым в этом вопросе, позволяя всем специалистам найти для себя что-то интересное (рис. 3).

И те, кто только начинает задумываться о своем SOC, и те, кто уже работает в этой сфере не один год, и заказчики, и поставщики услуг... Все уходят с форума с новыми идеями и знаниями, которые и являются залогом развития сегмента центров мониторинга ИБ и реагирования на инциденты, сделавшего за последние 5 лет качественный скачок и достигшего большей зрелости.

**Евгений НОВИКОВ**

заместитель директора
Департамента экономической
безопасности в ТЭК
Министерства энергетики РФ

БЕЗОПАСНОСТЬ ТЭК — 2020

НЕОБХОДИМО ОБЕСПЕЧИТЬ КООРДИНАЦИЮ ДЕЙСТВИЙ

В конце 2020 г. в Сочи состоялась выездной семинар «Актуальные и спорные вопросы в сфере обеспечения безопасности и антитеррористической защищенности объектов ТЭК: диалог бизнеса и регуляторов». Семинар проводился под общим руководством Министерства энергетики РФ, активное участие в подготовке и проведении мероприятия приняли представители ПАО «Россети». Вел мероприятие директор Департамента экономической безопасности в ТЭК Минэнерго России А. Ю. Семейкин.

В первый день в рамках трех сессий рассматривались правовые вопросы. Первая сессия была посвящена арбитражным и уголовно-правовым аспектам, вторая — преступлениям,

связанным с нарушением административного и налогового законодательства, третья — преступлениям на предприятиях ТЭК.

Второй день семинара в основном был посвящен вопросам обеспечения информационной безопасности объектов КИИ ТЭК. В своем выступлении директор Департамента экономической безопасности в ТЭК Минэнерго России А. Ю. Семейкин дал характеристику текущей обстановки в области борьбы с правонарушениями ТЭК, довел до присутствующих организационную структуру Департамента и решаемые им задачи. Особо была отмечена необходимость обеспечения безопасности КИИ предприятий ТЭК, одним из перспективных направлений определено создание единой системы управления кибербезопасностью в ТЭК.

Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации» фактически определены три основных этапа его реализации:

1. Категорирование объектов критической информационной инфраструктуры, выделение значимых объектов и включение их в соответствующий реестр.

2. Построение системы защиты значимых объектов в соответствии с требованиями регуляторов.

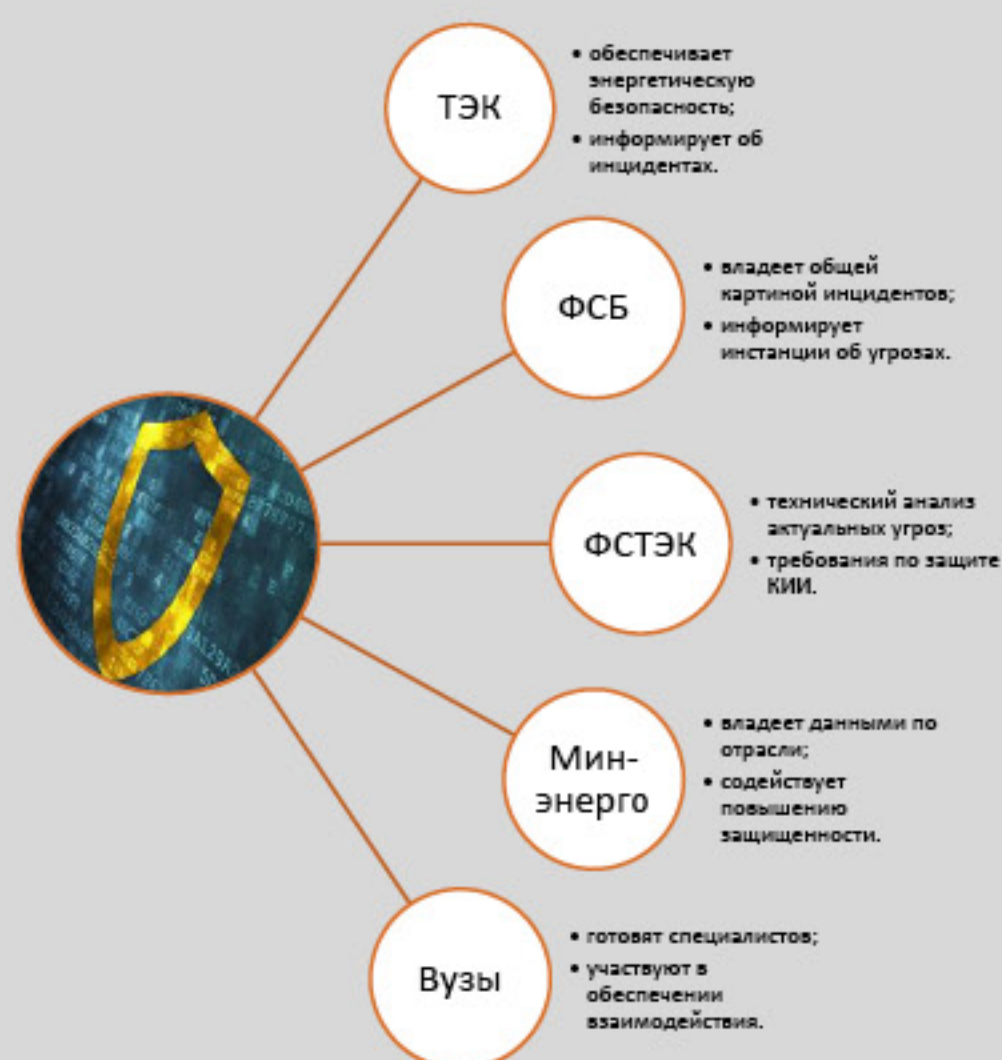
3. Эксплуатация систем защиты значимых и иных объектов, выявление компьютерных атак, взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (ГосСОПКА), контроль и совершенствование систем защиты.

В настоящее время в организациях отрасли категорирование фактически завершено, начинается переход ко второму этапу. Вместе с тем, параллельно идет организационная работа по налаживанию взаимодействия корпоративных центров мониторинга с Национальным координационным центром по компьютерным инцидентам, обеспечивающим работу ГосСОПКА.

В выступлении представителя РГУ нефти и газа (НИУ) им. И. М. Губкина Д. И. Правикова были описаны современные геополитические вызовы, связанные с угрозой воздействия на критическую информационную инфраструктуру, отмечены проблемные вопросы, связанные с подготовкой кадров,



СТРАТЕГИЯ ВЗАИМОДЕЙСТВИЯ



Представляется целесообразным описать стратегию взаимодействия в виде отдельного документа: «Стратегия информационной безопасности (кибербезопасности) топливно-энергетического комплекса Российской Федерации». Цель – выработка подходов к оценке реального уровня кибербезопасности предприятий ТЭК (функция от времени выявления и сложности АРТ атак).

Слайд из презентации представителя РГУ нефти и газа (НИУ) им. И. М. Губкина Д. И. Правикова

способных на предприятиях ТЭК обеспечить выявление и фиксацию компьютерных инцидентов.

В выступлении заместителя директора Департамента экономической безопасности в ТЭК Минэнерго России Е. В. Новикова были доведены статистические данные о выполнении процедуры категорирования предприятий ТЭК, проведенной в соответствии с положениями постановления Правительства РФ «Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений», а также отмечены недостатки, выявленные межведомственной экспертной группой в ходе мероприятий по оценке защищенности объектов критической информационной инфраструктуры электроэнергетики.

В выступлении представителя национального координационного центра по компьютерным инцидентам (НКЦКИ) И. В. Минаева была рассмотрена практика взаимодействия субъектов критической информационной инфраструктуры ТЭК и НКЦКИ.

Одними из ключевых участников второго дня стали представители компании «Ростелеком». Вице-президент

ПАО «Ростелеком» по информационной безопасности И. В. Ляпунов прочитал доклад «Практические вопросы взаимодействия субъектов КИИ ТЭК при отражении и нейтрализации кибератак», в котором был сделан акцент на возможностях выявления компьютерных инцидентов. Руководитель экспертного пресеяла центра мониторинга и реагирования на кибератаки Solar JSOC «Ростелеком-Солар» А. В. Павлов в своем докладе рассказал об актуальных трендах киберугроз энергетической отрасли.

Как показали результаты семинара, на текущий момент наиболее острым вопросом, препятствующим эффективной реализации систем защиты КИИ, является отсутствие на низовых звеньях организационной структуры предприятий ТЭК подготовленных кадров, способных обеспечить выявление компьютерных инцидентов, фиксацию их следов и восстановление нормального функционирования. При этом подготовка кадров должна носить систематический характер, проводиться с использованием киберполигонов в условиях, максимально приближенных к реальным, учитывать актуальный ландшафт угроз. Исходя из имеющегося опыта, сотрудники предприятий должны как минимум несколько раз принять участие в киберучениях для получения

необходимых навыков реагирования на киберинциденты.

Анализируя сложившуюся ситуацию можно отметить, что в настоящее время в реализации Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» принимают участие:

- ♦ компании ТЭК как субъекты критической информационной инфраструктуры;
- ♦ ФСТЭК России как регулятор, определяющий требования к системам защиты КИИ;
- ♦ НКЦКИ и ФСБ России как регулятор, определяющий порядок функционирования ГосСОПКА;
- ♦ Министерство энергетики РФ как отраслевой регулятор;
- ♦ вендоры — поставщики решений по информационной безопасности для предприятий ТЭК;
- ♦ научные и учебные заведения, обеспечивающие подготовку кадров.

* * *

В сложившихся условиях представляется целесообразным обеспечить координацию действий заинтересованных сторон, направленную в первую очередь на создание эффективной системы выявления компьютерных атак в целом по отрасли и обеспечение подготовки персонала низовых звеньев.



THE STANDOFF



Валерий КУЛИКОВ
обозреватель BIS Journal

Фото: standoff365.com

THE STANDOFF 2020

КИБЕРБИТВА НА ФОНЕ ГЛОБАЛЬНОЙ КОНФЕРЕНЦИИ

Ряска повторной самоизоляции, затянув просветы KICC и CISO Форума, превратила событийный фон «ибэшных» мероприятий в унылое виртуальное Zoom-болото. Сообщение о командировке на The Standoff заставило взбодриться.

RED ПРОТИВ BLUE

Живое общение с организаторами позволило понять, что вожжи стремительно разворачивающейся «тачанки» The Standoff находятся в опытных руках Positive Technologies, а само по себе мероприятие — это почти то же самое, что и «масштабное хакерское соревнование, проведённое в ходе PHDays 2018» и «высокотехнологичный ночной клуб, воссозданный устроителями PHDays 2019». Только в прошлые годы слова The Standoff отходили на второй план, уступая первое место бренду PHDays.

Но SARS-CoV-2 вывел бренд The Standoff в группу лидеров в короткой череде действительно масштабных

дистанционных мероприятий в сфере ИБ. Шесть дней в режиме нон-стоп 29 команд red team атаковали цифровой город, защищаемый шестью командами blue team. Среди объектов — транспортная инфраструктура (аэропорт, морской порт, железнодорожный узел), ТЭК (нефтяное месторождение, газораспределительная станция, нефтепереработка), банк и деловой центр, рекламно-информационная инфраструктура города, парк развлечений.

Конференция «при The Standoff» тоже получилась впечатляющей: более 70 докладов и круглых столов, свыше 20 тыс. посетителей.

С ПОПРАВКОЙ НА РЕАЛЬНОСТЬ

Продвинутые зрители следили за киберсражением, используя профессиональный инструментарий Positive Technologies и Cisco. Простые обыватели полагались на отчёты пресс-службы и видеотрансляции бесед с экспертами и участниками событий.

Учитывая, что участники спали мало, нерегулярно питались и не всегда были выбриты, данные постстрелизов и устные заявления в режиме реального времени частенько расходились в деталях (реализованы по одним источникам 24 риска, по другим 29, деньги из взломанного банка по одним выведены, по другим нет), но всегда верно отражали картину в целом. И картина эта была такой же живой и многомерной, как и само мероприятие. Соответственно, разные трактовки имели полное право на существование.

НЕКОТОРЫЕ ИТОГИ

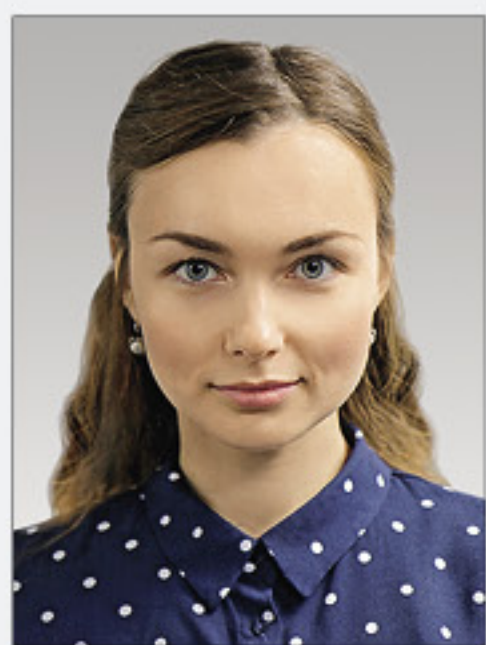
К концу шестидневной битвы были выведены из строя системы аэропорта, парка развлечений, газораспределительной станции, нефтедобывающей компании и электростанции. Потери понесли банк и деловой центр. Под управление атакующих попали рекламные экраны.

Плачевные результаты?

«КАК И В ИГРЕ, В РЕАЛЬНОСТИ МЫ НА СТОРОНЕ BLUE TEAM»

BIS-ИНТЕРВЬЮ С ГЕРОЯМИ THE STANDOFF 2020

В результате шестидневной кибервойны цифровой город пал практически полностью. Устояли (!!!) только морской порт и железная дорога. Эти объекты защищала команда Re@ct — профессионалы RosatomCERT из ИТ-интегратора атомной отрасли АО «Гринатом». Они обеспечили коэффициент доступности защищаемой инфраструктуры 0,9416. Обозреватель BIS Journal Валерий Куликов не мог не познакомить наших читателей с героями этой незабываемой битвы.



Екатерина ЖБАНОВА

старший специалист группы разработки и техэкспертизы, капитан команды

— Представьте, пожалуйста, вашу команду.

— Средний возраст — около 30 лет. Почти все мы работаем в одном подразделении «Гринатома» в Нижнем Новгороде, также в составе команды несколько экспертов из Москвы. Ребята имеют хорошую подготовку, окончили технические вузы по направлениям ИТ и ИБ, стаж работы в сфере ИБ от двух лет и более.

— Был ли у команды опыт в сфере red/blue team?

— У участников команды обширный опыт в сфере blue team — это наша

ежедневная работа. А функции red team мы выполняем, когда определяем потенциальные векторы атак, проверяем уровень защищённости периметра сетевой инфраструктуры. Нужно постоянно спрашивать себя: «Что бы мы сделали на месте атакующих?»

— А как команда попала на The Standoff 2020? Отправили заявку или вас специально пригласили?

— Мы слышали об этой площадке, и в этом году организаторы пригласили нас принять участие.

— То есть на этом киберполигоне вы впервые?

— Да, это наш первый опыт работы на The Standoff.

— Для подготовки к соревнованиям были организованы специальные сборы?

— Мы продолжали работать, а вечерами собирались для тренировок и изучения полигона. Организаторы The Standoff предоставили нам все возможности для знакомства с его инфраструктурой и для удалённой работы на площадке в период подготовки.

— Объекты для защиты выбирала команда?

— Нет, объекты были назначены организаторами мероприятия.

— Проводился ли «разбор полётов» после соревнований? Какие «уроки» были извлечены?

— После соревнований мы обсудили наши действия, расследованные атаки, выявили ошибки и сильные стороны. Мы определили направления, которые нужно укрепить практическими знаниями, подготовили примерный план дальнейшего развития.

— Есть ли у команды «командные планы» на будущее?

— В сфере ИБ необходимо всегда захватывать максимальное количество областей для развития, и мы к этому стремимся. Планируем совершенствоваться как индивидуально, так и в командном формате, делиться опытом, приобретать новые знания. Выступление в качестве red team пока не обсуждалось, в следующем году планируем снова поучаствовать в киберучениях The Standoff на стороне blue team.

Результаты такие, какие и должны быть при нынешнем состоянии ИТ-технологий и квалификации персонала, строящего и обслуживающего КИИ. Организаторы заложили в инфраструктуру города около 60 уникальных рисков, атакующие «реализовали» около половины этих рисков,

причём — любопытный и неожиданный факт — два из «реализованных» не входили в число, изначально заложенных организаторами.

Так хороший результат или плохой?

Дмитрий Серебренников, директор по анализу защищённости Positive Technologies, в своём комментарии

заявил, что в этом году уровень атакующих заметно вырос. «Мы не ожидали, что половина рисков будет реализована».

Против атакующих выстояли лишь морской порт и железная дорога. Банк и «нефтянка» подверглись нападению в первые же часы, сила атак не

**Эмиль АЛТЫНБАЕВ**

начальник отдела кибербезопасности,
член команды

— В сфере кибербезопасности в качестве базовой «идеологии» сейчас доминирует так называемый риск-менеджмент. Альтернатива ей — управление кибербезопасностью «по требованиям». Какой подход ближе вашей команде?

ослабевала постоянно. И хотя поначалу проникшие довольно быстро были изгнаны из банка, в конце концов пали и финансовая инфраструктура, и КИИ нефтегазового комплекса.

Такая тактика оправдана?

Вполне возможно, такой ход событий был спровоцирован методикой оценки результатов и стереотипами современного мышления, для которого финансы и «Газпром» являются олицетворением экономики. С практической же точки зрения, если сразу остановить транспорт, то и нефтедобыча, и нефтепереработка встанут сами по себе. И это следует учитывать и при оценке реальных рисков, и при разработке тактики кибервойны.

«КОММУНИЦИРУЕМ, ОБЩАЕМСЯ, ЛОМАЕМ»

Уже упомянутый Дмитрий Серебренников и Алексей Новиков, директор экспертного центра безопасности Positive Technologies, при подведении первых итогов отмечали, что они с интересом изучали новинки инструментария атакующих, техники и тактики атак команд, продемонстрировавших в этом году резко возросшие возможности проникновения. Среди оригинальных решений защитников Алексей

— Команда представляла на соревнованиях «Гринатом» — многофункциональный общий центр обслуживания и ИТ-интегратор госкорпорации «Росатом». Это и определяет необходимость придерживаться традиционного для наших структур подхода в сфере обеспечения кибербезопасности на основе управления рисками.

— Что дало вам участие в соревнованиях на The Standoff 2020?

— Полезный опыт. В мировых реалиях тезис о том, что «проникновение неизбежно», слишком часто подтверждается практикой. В этих условиях изучение паттернов поведения нападающих на полигоне, их инструментария позволяет неплохо подготовиться к реальным атакам.

Новиков отметил приём, при котором одна из команд защитников специально открыла пару серверов для атакующих и далее с интересом наблюдала за топтанием red-team-слонов в посудной лавке.

О бесценности вновь обретенного опыта упоминали и многие участники команд. Антон Куранда, технический директор RBK.money, компании, предоставившей свою финансовую платформу для оснащения киберполигона, высоко оценил возможность обкатки платформы в ходе киберучений и выразил желание продолжить сотрудничество с организаторами The Standoff.

«Коммуницируем, общаемся, ломаем», — так охарактеризовал три источника, три составные части пользы от участия в The Standoff лидер одной из команд-победительниц.

Уместно заметить (без каких-либо комментариев), что победные места по условиям The Standoff присваивались только командам атаки — по совокупному числу баллов, которые им присуждали за реализацию бизнес-рисков, отчёты «по внутренней багбаунти» и некоторые другие успехи.

Среди команд защиты победители не выделялись, однако вёл рейтинг команд, учитывающий разные

— Сегодня киберучения становятся ключевыми событиями в череде мероприятий по подготовке к отражению атак из киберпространства. Ваша организация уже использует похожие на The Standoff 2020 учения во внутрикорпоративной практике?

— Если задаться такой целью, то наши ресурсы и опыт позволили бы создать нечто подобное, но не по мановению волшебной палочки. Инфраструктура The Standoff во многом уникальна и является результатом не только больших инвестиций, но и труда многих людей и компаний. Поэтому наиболее эффективно участие наших специалистов в киберучениях на уже созданных полигонах. The Standoff — это один из такого рода положительных примеров.

показатели: число проведённых расследований, доступность инфраструктуры, скорость расследования.

МУЗЫ НЕ МОЛЧАЛИ

Уместно вспомнить, что The Standoff 2020 — это не только битва в киберпространстве, но и конференция. И если бы в этой части мероприятия также были предусмотрены призы, возможно, награду за оригинальность темы получил бы Роберт Селл, президент компании Trace Labs. Он рассказал, как хакеры трудятся над получением физического доступа к оборудованию. А также о том, как преступники проводят разведку, что делают в ходе тестовых попыток проникновения (включая приготовление объяснений на случай поимки), а для наглядности представил подробное описание инструментов для физического взлома замков и способов сокрытия их в здании до момента использования.

Что касается основной части докладов и дискуссий, то классифицировать их можно вполне традиционно — (1) визионерство, (2) новости (breaking&hot) и (3) сообщения о планомерно развиваемых исследованиях.

В этой связи уместно отметить, что искусственный интеллект плавно пе-

BIS-ИНТЕРВЬЮ



Иван ПАУШКИН

руководитель Корпоративного центра ГосСОПКА, член команды

— Отрабатывались ли в ходе The Standoff вопросы взаимодействия с ГосСОПКА? Как вы могли бы прокомментировать этот аспект киберучений?

— В ходе киберучений The Standoff взаимодействие с ГосСОПКА не отрабатывалось — такой сценарий организаторами не закладывался. Хотя было бы продуктивно и более приближено к нашей повседневной работе, если бы все команды защитников имели общий реестр атак нападавших команд.

— В киберучениях принимают участие уже достаточно подготовленные специалисты. Какие «технологии» повышения квалификации сотрудников подразделений кибербезопасности используются в вашей организации?

— Мы изначально отбираем специалистов с хорошей фундаментальной технической подготовкой.

— Позвольте уточнить. «С хорошей фундаментальной технической подготовкой». Речь идёт о подготовке в сфере ИБ? Или ИТ? Или об общей фундаментальной подготовке, например, в области математики?

— Оптимально работать с теми, кто получил сильную подготовку в ИТ. Для достижения высокого практического уровня в сфере ИБ у нас развита система наставничества, есть возможности повышать квалификацию в Технической академии Росатома, также мы отправляем сотрудников в учебные центры при крупных компаниях и вузах.

— В какой пропорции представлены в линейке ваших доверенных учебных центров структуры вузовские и корпоративные?

— Около 60 процентов — это корпоративные учебные центры вендоров и 40 процентов — вузовские.

— Какой рабочий инструментарий используют ваши службы ИБ? «Коробочные» продукты или кастомизированные?

— Чуть более половины — инструментарий от вендоров, также есть Open Source и собственные разработки.

— А вы не боитесь санкций при такой зависимости от вендоров?

— Слово «вендор» не всегда подразумевает иностранного поставщика. У нас давно взят курс на импортозамещение,

и мы в значительной степени используем отечественный инструментарий.

— На сентябрьской конференции Kaspersky Industrial CyberSecurity Conference 2020 представитель «Русатом автоматизированные системы управления» упомянул, что в своих проектах по автоматизации АЭС он и его коллеги занимаются и кибербезопасностью, и безопасностью информационной, и иными безопасностями, упоминаемыми в отечественной нормативной базе, в рекомендациях МЭК и документах МАГАТЭ. А какими нормативными документами руководствуетесь вы?

— Мы неукоснительно выполняем все требования регуляторов. Кроме того, нами создан и развивается необходимый набор внутренних нормативных документов.

— Как вы выстраиваете свои взаимоотношения с другими подразделениями и, в частности, с ИТ-департаментом? В ряде организаций это своеобразный камень преткновения.

— Тот «необходимый набор внутренних нормативных документов», о котором я сказал, как раз и содержит, в частности, и регламенты нашего взаимодействия с ИТ.

— Благодарю за знакомство с командой «Гринатома» Re@ct. Желаю новых побед на поприще ИБ!

рётёк в разряд (3) и теперь его возможности оцениваются профессионалами более чем трезво и достаточно рутинно применяются для фильтрации спама, пассивного анализа трафика, сбора информации, подбора паролей и т.д.

В разделе (2) запомнились обсуждения «фальшивой биометрии». Создание «синтетических» личностей становится всё проще, а борьба с ними — сложнее. Что, впрочем, не мешает экспертам выявлять ограничения технологий подмены и синтеза биометрических данных и предлагать их для обнаружения фактов компрометации биометрии. Этой теме был посвящён, в частности,

доклад учёных из компании BBVA Next Technologies.

«Безопасное программирование», проверка качества кода — это пример сквозной, планомерно развиваемой темы в ИБ, как и использование Open Source-инструментария. Денис Макрушин из Huawei поделился опытом своей компании и рассказал, в частности, о SonarQube — платформе с открытым исходным кодом для анализа качества и защищённости программного кода. Сергей Горохов, архитектор решений компании ЕРАМ, рассказал о важности тесного взаимодействия подразделений AppSec и Security Testing.

ДО НОВЫХ ВСТРЕЧ

В ближайших планах организаторов The Standoff — глубокий анализ данных, собранных на поле битвы. В планах на перспективу — организация новых учений. В инфраструктуру полигона могут быть добавлены медицинские учреждения и системы спутниковой связи. Рассматриваются возможности увеличения числа команд обороняющихся и доведение их количества до той цифры, что характеризует атакующую сторону. Изюминкой новой битвы может стать разрешение командам blue team атаковать «красных».

А мы будем следить ещё и за анонсами PHDays. Как уживутся два медведя в одной берлоге?



Григорий СТРИЖАКОВ
кандидат юридических наук



Вячеслав ЧЕРТКОВ
юрист

ПЕРЕДАЧА И ПЕРЕДОВЕРИЕ

ПРАВОВЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ЭП

ПЕРЕДАЧА

Передача электронной подписи руководителя организации или индивидуального предпринимателя

В рамках осуществления своей деятельности многим хозяйствующим субъектам необходимо взаимодействие в электронной форме. При таком взаимодействии чаще всего, как минимум на начальных этапах, например при регистрации на определенных информационных ресурсах (личные кабинеты на сайтах ФНС России, Росреестр), требуется электронная подпись, являющаяся аналогом собственноручной подписи¹, именно руководителя. Однако информационных ресурсов много. Одни для заключения сделок, другие для представления отчетности в контролирующие органы.

¹ В целях заключения гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронными сообщениями, обмен электронными сообщениями, каждое из которых подписано электронной подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами (часть 4 статьи 11 Федерального закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

Чем больше охват деятельности хозяйствующего субъекта, тем меньше, как это часто бывает, времени у его руководителя (индивидуального предпринимателя). Очевидно, что при таких условиях руководитель (индивидуальный предприниматель) не будет самостоятельно регистрироваться на данных информационных ресурсах, а значит, повышается вероятность неурегулированной передачи электронной подписи руководителя (индивидуального предпринимателя) другому лицу для совершения вышеуказанных действий, что нередко приводит к компрометации данной электронной подписи.

При использовании усиленных электронных подписей участники электронного взаимодействия обязаны обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия².

Полагаем, что для решения данного вопроса в целях обеспечения такого согласия возможно применение специальной формы согласия, в которой должны быть определены: время и дата использования электронной подписи руководителя (индивидуального

² Пункт 1 части 1 статьи 10 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».

предпринимателя), информационный ресурс, в рамках которого будет использована данная электронная подпись, действия и документы, которые планируется ею удостоверить.

Дополнительно необходимо использовать форму отчета о применении электронной подписи руководителя (индивидуального предпринимателя), в которой должны быть определены результаты применения такой электронной подписи, исходя из атрибутов согласия.

Кроме того, при каждом случае использования электронной подписи руководителя (индивидуального предпринимателя) требуется оформление акта передачи данной подписи от ответственного за её хранение лицу, непосредственно её применяющему, и наоборот. Форма данного акта должна включать точный адрес места хранения электронной подписи руководителя (индивидуального предпринимателя), включая помещение (комнату, офис), вплоть до сейфа.

Оформление данных документов позволит точно определить дату, время, информационный ресурс, документы и действия, совершаемые с использованием электронной подписи, а также лицо, которое её использовало, и тем самым снизить риск компрометации электронной подписи, вызванный отсутствием согласия руководителя.



ДОВЕРЕННОСТЬ И СЕРТИФИКАТ

Доверенность и сертификат ключа проверки электронной подписи

В связи с последними изменениями в Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи», вступившими в силу 01.07.2020, участники электронного взаимодействия не вправе устанавливать иные, за исключением предусмотренных законом, ограничения признания усиленной квалифицированной электронной подписи. Нарушение запрета на ограничение или отказ от признания электронных документов, подписанных квалифицированной электронной подписью, соответствующей предъявляемым к ней требованиям, равнозначными документам на бумажном носителе, подписанным собственноручной подписью, а также нарушение запрета операторами государственных и муниципальных

Лицо, получившее усиленную квалифицированную электронную подпись, сможет использовать её без каких-либо технических ограничений на всех электронных площадках и во всех взаимоотношениях в электронном формате

информационных систем, информационных систем, использование которых предусмотрено нормативными правовыми актами, или информационных систем общего пользования на предъявление требований о наличии в квалифицированном сертификате информации, не являющейся обязательной в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» и принимаемыми в соответствии с ним нормативными правовыми актами, по любым причинам,

кроме предусмотренных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», не допускается³.

Это означает, что лицо, получившее усиленную квалифицированную электронную подпись, сможет использовать её без каких-либо технических ограничений на всех электронных площадках и во всех взаимоотношениях в электронном формате.

³ Часть 2 статьи 10 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Когда усиленная квалифицированная электронная подпись применяется по доверенности вне электронных площадок, проверить полномочия по такой доверенности без её направления контрагенту невозможно

При использовании усиленной квалифицированной электронной подписи на электронных площадках, в том числе торговых, в случаях, когда владельцем сертификата ключа проверки электронной подписи является юридическое лицо, а физическое лицо выступает от его имени на основании доверенности, данная доверенность прилагается (её может увидеть и проверить контрагент) и у оператора данной площадки возникает возможность её просмотра.

В случаях, когда усиленная квалифицированная электронная подпись применяется по доверенности вне электронных площадок (например, при регистрации личных кабинетов на сайтах ФНС России, Росреестр, направление документов на адрес электронной почты контрагента), проверить полномочия по такой доверенности без её направления контрагенту невозможно, так как в силу части 2 статьи 17 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» включение информации о полномочиях, обозначенных в такой доверенности, в квалифицированный сертификат не предусмотрено.

Полагаем, что урегулирование данного вопроса возможно путём закрепления соответствующих норм, позволяющих контрагентам обеспечить проверку полномочий по доверенности самостоятельно или через третьих лиц, например, доверенной третьей стороной⁴.

⁴ Доверенная третья сторона — юридическое лицо, осуществляющее деятельность по проверке электронной подписи в электронных документах в конкретный момент времени в отношении лица, подписавшего электронный документ, для обеспечения доверия при обмене данными и электронными документами и иные функции, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» (пункт 17 статьи 2 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи». Начало действия редакции — 01.01.2021).

УКАЗАНИЕ СВЕДЕНИЙ В СЕРТИФИКАТЕ

Указание в сертификате ключа проверки электронной подписи сведений об уполномоченных представителях

В рамках достижения своих целей иногда юридическим лицам в силу разных причин (например, территориальная удалённость, отсутствие квалифицированного персонала и другие) затруднительно самостоятельно выполнять те или иные действия (например, совершать сделки (подписывать контракты), выполнять государственную регистрацию имущества). В связи с этим им приходится обращаться к услугам представителей, которые смогут осуществить данные действия за них.

Отношения между юридическими лицами и представителями оформляются в том числе с помощью договоров поручения, комиссии, агентирования, доверительного управления имуществом.

Кроме того, представители выступают от имени юридического лица на основании доверенности.

Очевидно, что такими представителями могут выступать и юридические лица, на которых также распространяются положения законодательства о доверенности.

Соответственно, при совершении сделки одним юридическим лицом (представителем) от имени другого юридического лица (представляемого) по доверенности именно представитель будет подписывать документы по сделке.

Но так как юридическим лицом признаётся организация, то ввиду того, что организация самостоятельно не может иметь собственноручную подпись, собственноручную подпись будет проставлять лицо (физическое лицо), действующее на основании учредительных документов.

Вместе с тем в случае взаимодействия лиц в электронном формате юридическое лицо сможет использовать свою

именно электронную подпись, так как Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» предусматривает возможность юридическому лицу наравне с физическим лицом быть владельцем сертификата ключа проверки электронной подписи⁵.

Необходимо обратить внимание на то, что в данном сертификате указывается наименование юридического лица и физическое лицо, действующее от имени юридического лица на основании учредительных документов юридического лица или доверенности.

Это означает, что при совершении сделки в электронном формате юридическим лицом будет применяться электронная подпись юридического лица. Применять данную подпись будет или непосредственно руководитель данного юридического лица, или лицо по доверенности, но отображаться в электронном документе будет именно как подпись юридического лица.

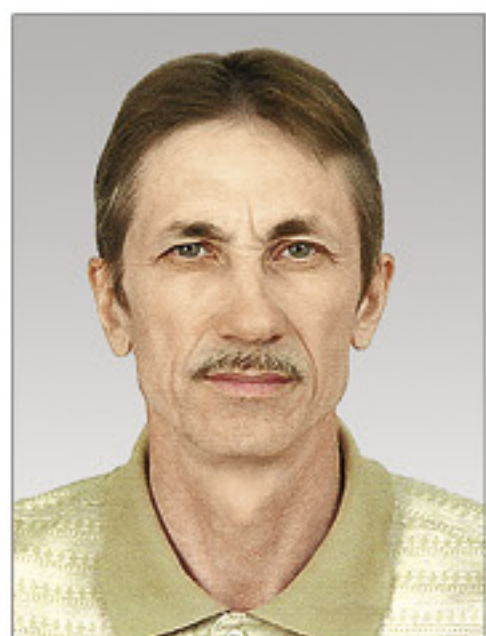
Когда юридическое лицо выступает в гражданских правоотношениях в качестве представителя, и сделка совершается в электронном формате, значит, юридическое лицо (представитель) должно использовать электронную подпись юридического лица (представляемого), в которой наряду с указанием наименования юридического лица (представляемого) будет указано юридическое лицо (представитель), действующее на основании доверенности.

При этом данная сделка непосредственно создаёт, изменяет и прекращает гражданские права и обязанности представляемого.

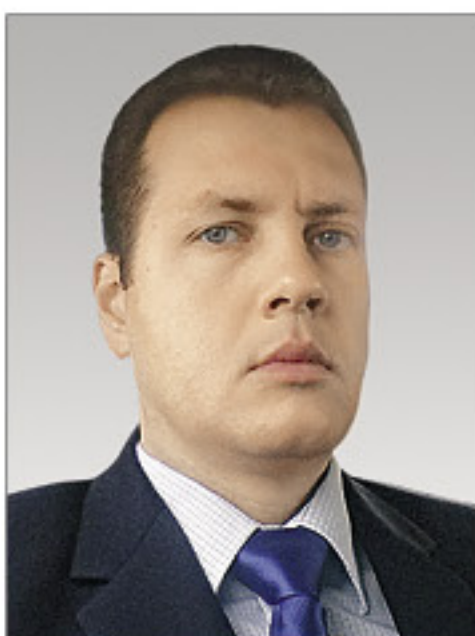
Однако реализовать такой подход в настоящее время затруднительно, поскольку в Федеральном законе от 06.04.2011 № 63-ФЗ «Об электронной подписи» говорится только об упоминании в качестве владельцев сертификата ключа проверки электронной подписи одного юридического лица и одного физического лица.

Урегулирование данного вопроса возможно путём внесения соответствующих изменений в Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

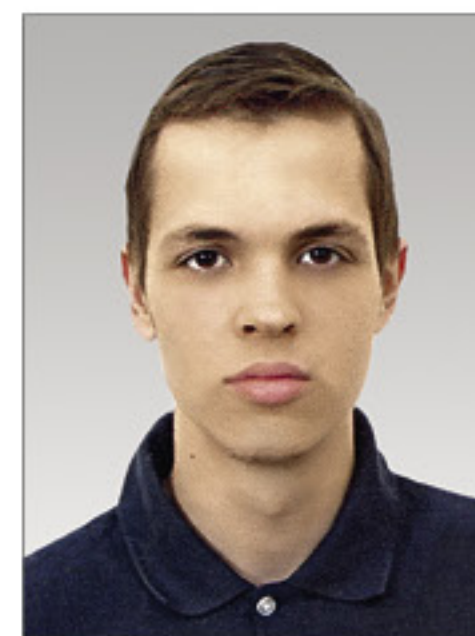
⁵ Часть 3 статьи 14 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».



Валерий ХУРМАТУЛЛИН
эксперт, начальник группы,
Радиотехнический институт
им. академика А.И. Минца, к.э.н



Дмитрий КОЛЕСНИКОВ
руководитель направления,
ПАО Сбербанк



Андрей КОЛЕСНИКОВ
ведущий специалист,
концерн «Автоматика»

ПРИ ОБЪЕДИНЕНИИ СИСТЕМ

ВОПРОСЫ СОХРАННОСТИ ИНФОРМАЦИИ ПРИ
ИСПОЛЬЗОВАНИИ АВТОМАТИЗИРОВАННОЙ
ИНТЕГРИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ СОЗДАНИЕМ
И ПРАКТИЧЕСКОЙ РЕАЛИЗАЦИЕЙ РЕЗУЛЬТАТОВ НИОКР

В статье рассматриваются вопросы сохранности информации при использовании автоматизированной интегрированной системы управления созданием и практической реализацией результатов научно-исследовательских, опытно-конструкторских и технологических работ (НИОКР) при взаимодействии исполнителя НИОКР и заказчика НИОКР.

МЕРЫ ПО НЕДОПУЩЕНИЮ

Понятие «информационная безопасность» применительно к нашей действительности в сфере научно-технической деятельности является достаточно широким понятием. В общем случае информационную безопасность можно определить как комплекс организационно-технических мероприятий и мер по недопущению без уполномоченного разрешения использования, раскрытия, искажения, изменения, записи или обработки, уничтожения передачи третьим лицам наработанной в ходе выполнения научно-исследовательских, опытно-конструкторских и технологических работ (НИОКР) информации или научно-технического знания. Это понятие может применяться в самых различных аспектах, вне зависимости

от формы представления данных, информации, знания.

Всё это актуально при автоматизации процессов управления созданием и практической реализацией различного вида результатов НИОКР, с применением автоматизированных информационных систем различных видов [1], в данном конкретном случае — автоматизированной интегрированной системы управления созданием и практической реализацией результатов НИОКР [2]. Применение данной системы позволяет расширить функциональные возможности и решать вопросы сквозного управления процессами создания и практической реализации различных видов результатов НИОКР, созданных в ходе выполнения контрактов за счёт бюджетного и внебюджетного финансирования.

Указанная система объединяет автоматизированные информационные системы организации — исполнителя НИОКР и организации-заказчика НИОКР. При этом устраняется информационный разрыв между уровнями управления процессами создания и практической реализации результатов НИОКР путём интеграции информационных систем организации и заказчика в части программно-аппаратного обеспечения.

СОВОКУПНОСТЬ БЛОКОВ

Автоматизированная интегрированная система управления созданием и практической реализацией результатов НИОКР (рис. 1) представляет собой совокупность информационных блоков, каждый из которых является самостоятельной информационной единицей.

КЛАССИФИКАЦИЯ ВИДОВ

Рассматривая вопросы сохранности информации и информационной безопасности в контексте предотвращения несанкционированной утечки сведений и данных применительно к составляющим информационным блокам данной интегрированной системы, можно определить, виды какой информации, данных, полученных или накопленных знаний представляют интерес для третьих лиц или конкурентов.

Ниже представлен один из возможных вариантов классификации видов информации, данных, конкретных научно-технических результатов, циркулирующих в интегрированной системе. Также предлагаются возможные способы их защиты от несанкционированного использования. Данные виды информации, данных, конкретных знаний в условиях современной

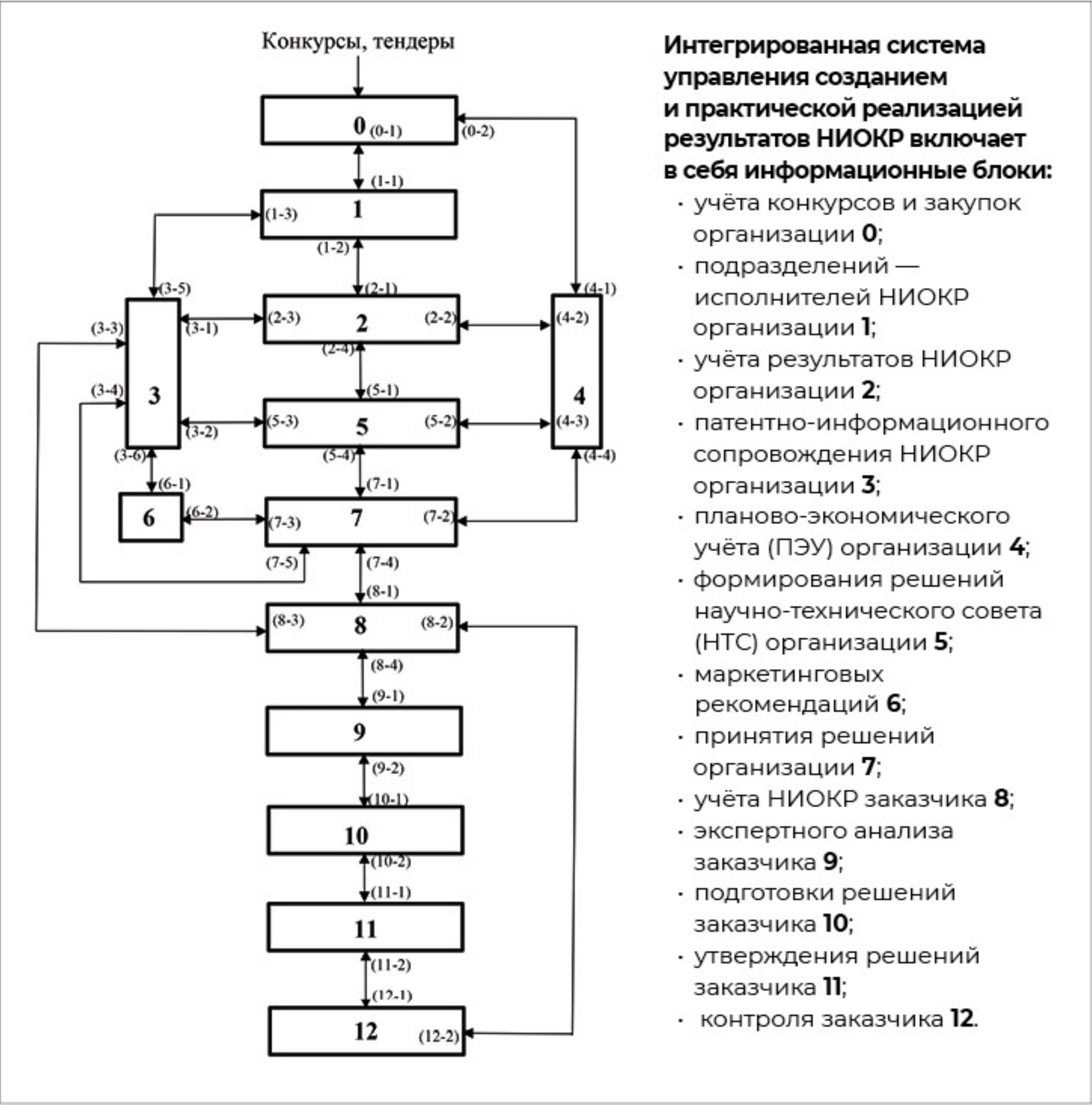


Рисунок 1. Интегрированная система представляет собой совокупность информационных блоков, каждый из которых является самостоятельной информационной единицей

технологической конкуренции всегда будут представлять интерес для компаний-конкурентов или иных третьих лиц (таблица 1).

Основная задача информационной безопасности НИОКР при использовании автоматизированных информационных систем в контексте сохранности информации от несанкционированного использования — это осуществление сбалансированной защиты конфиденциальности, целостности и доступности данных, информации. При этом применяемые меры со-

хранности информации, данных должны учитывать вопросы целесообразности применения такого рода систем и учитывать вопросы парирования отрицательного влияния на эффективность деятельности организаций, выполняющих НИОКР прикладного характера. Взаимодействие организации — исполнителя НИОКР и организации — заказчика НИОКР посредством интегрированной системы управления созданием и практической реализацией результатов НИОКР должно осуществляться с учётом необходимых мер информационной безопасности на организационном и аппаратно-программном уровнях.

Наименование информационного блока	№ блока в составе системы
Блок учёта конкурсов и закупок	0
Блок подразделений — исполнителей НИОКР	1
Блок учёта результатов НИОКР организации	2
Блок патентно-информационного сопровождения НИОКР	3
Блок планово-экономического учёта организации	4
Блок формирования решений НТС организации	5
Блок маркетинговых рекомендаций	6
Блок принятия решений организации — исполнителя НИОКР	7
Блок учёта НИОКР заказчика	8
Блок экспертного анализа заказчика НИОКР	9
Блок подготовки решений заказчика	10
Блок утверждения решений заказчика	11
Блок контроля заказчика	12

ИСТОЧНИКИ

1. «Практические аспекты использования автоматизированных информационных систем управления интеллектуальной собственностью, в том числе в банковской сфере» (на основе патентных документов). © BIS Journal № 4/2019 г., в соавторстве.
2. «Интегрированная система управления созданием и практической реализацией результатов научно-исследовательских, опытно-конструкторских и технологических работ». © Патент Российской Федерации № 2703678, М., 2019 г., в соавторстве.

Вид информации, данных, знаний	Ценность информации, данных, знаний (техническая коммерческая, правовая, иная)	Способы защиты информации, данных, знаний
База данных контрактов и договоров, технических заданий, ведомостей исполнения, календарных планов	Анкеты НИОКР с фактографическими данными о разработке, стоимости, сроках	Ограничение доступа, дозирование и предоставление данных по учтённым запросам
База данных результатов НИОКР по этапам, интегральная база данных созданных результатов НИОКР в целом по научно-техническим центрам	Конкретные виды научно-технических, технологических результатов НИОКР с достигнутыми техническими параметрами	Использование технических и программных средств исполнителей НИОКР без выхода во внешние сети
Интегральная база данных созданных результатов НИОКР в целом по организации	Конструкторская и технологическая документация с ключевыми техническими решениями и секретами производства	Применение режима гостайны (при необходимости), режима коммерческой тайны
База данных отчётов по патентным исследованиям по темам. База данных формы по учёту результатов НИОКР по темам. База данных поданных заявок на патентование. База данных охраняемых результатов интеллектуальной деятельности. База данных лицензионных соглашений	Аналитические материалы по уровню техники, патентная аналитика, сведения о запатентованных технических решениях, информация о патентно-лицензионной политике организации	Использование режима коммерческой тайны. По отдельным базам данных доступ к информации после заключения экспертных комиссий
База данных и договоров, актов сдачи-приёмки по темам, сводные ведомости о ходе выполнения НИОКР	Агрегированная информация о выполненных разработках, о финансовом состоянии организации, её финансово-экономической устойчивости	Использование режима конфиденциальной информации
Научная и техническая информация об уровне готовности выполняемых тематических разработок	Информация о создании прорывных технико-технологических решениях или об их отсутствии, а также рекомендации по использованию в дальнейшем созданных результатов НИОКР	Применение режима гостайны (при необходимости), режима коммерческой тайны
База данных результатов маркетинговых исследований. База данных по рынку технологий. База данных конкурентов и потенциальных покупателей	Коммерческая информация по рынку и его сегментам	Применение режима коммерческой тайны
Данные о принятых решениях по практической реализации созданных организацией результатов НИОКР	Научно-техническая и маркетинговая информация	Применение режима гостайны, (при необходимости), режима коммерческой тайны
Корпоративная база данных созданных организациями результатов НИОКР. База данных предложений организаций по практической реализации созданных результатов НИОКР	Данные о результатах НИОКР по корпорации или отрасли. Направления технико-технологического развития	Применение режима гостайны (при необходимости), режима коммерческой тайны
База данных экспертных оценок научно-технической и коммерческой ценности результатов НИОКР, созданных организациями	Сведения о техническом уровне созданных результатов НИОКР. Сведения о предполагаемых вариантах применения созданных результатов НИОКР.	Применение режима коммерческой тайны
База данных проектов решений заказчика НИОКР	Результаты оценки научно-технической и коммерческой ценности. Формализованные описания проектов по практической реализации результатов НИОКР	Применение режима коммерческой тайны
База данных решений о целесообразности конкретного варианта практической реализации результатов НИОКР	Сведения об утверждении/неутверждении решений по конкретному варианту практической реализации результатов НИОКР	Применение режима коммерческой тайны
Результаты анализа об эффективности реализованных проектов на основе созданных организациями отрасли результатов НИОКР	Интегральные показатели результативности реализованных инновационных проектов на основе созданных организациями отрасли результатов НИОКР	Использование режима конфиденциальной информации

Таблица 1. Один из возможных вариантов классификации видов информации, данных, конкретных научно-технических результатов, циркулирующих в интегрированной системе. Также предлагаются возможные способы их защиты от несанкционированного использования

МИФЫ И ЛЕГЕНДЫ ПОВЫШЕНИЯ ОСВЕДОМЛЁННОСТИ

СТАТИСТИКА ПРОТИВ ОБЩЕСТВЕННОГО МНЕНИЯ



Ольга ЛИМОНОВА
психолог
ООО «Антифишинг»



Андрей ЖАРКЕВИЧ
редактор
ООО «Антифишинг»

Людям свойственно доверять своему опыту. Такой подход позволяет принимать обоснованные и взвешенные решения, когда речь идёт о технических уязвимостях и средствах защиты от них. Опыт в сочетании с логикой быстро приносит нужный результат.

Однако при построении защиты компании важно учитывать не только технический, но и человеческий фактор, поскольку неправильные действия людей также могут нанести серьёзный ущерб. В отношении сотрудников среди ИБ-специалистов существует несколько крайне стойких заблуждений, которые мешают выстроить эффективные процессы безопасности.

В процессе исследований, которые на системной основе проводит ООО «Антифишинг», мы собрали статистические данные, которые развенчивают пять главных мифов о человеческом факторе в ИБ. В этой статье мы поделимся полученными результатами, чтобы помочь специалистам грамотно и эффективно вести процессы повышения осведомлённости сотрудников, базируясь не на вере, а на научно обоснованных фактах.

1. ОБУЧАЮЩИХ КУРСОВ ДОСТАТОЧНО ДЛЯ СНИЖЕНИЯ РИСКА ЧЕЛОВЕЧЕСКОГО ФАКТОРА В ИБ

«Главное — это правильные обучающие курсы. Если они не помогают, значит, курсы недостаточно хороши: у них не тот дизайн, не хватает геймификации, материал слишком сложный».

Борьба за повышение эффективности информирования сотрудников превращается в «дегустацию» бесчисленного множества обучающих курсов в попытках выяснить, как же всё-таки преподнести информацию, чтобы сотрудники её усвоили, и как их мотивировать пройти ещё один по-модному оформленный курс о самом важном.

На самом деле. Повышение осведомлённости, состоящее только из обучающих курсов,

практически не влияет на поведение сотрудников. Нам не удалось выявить корреляции между декларируемым качеством курсов, их дизайном, геймификацией и действиями сотрудников.

Изучая этот вопрос, мы в течение года наблюдали за группой сотрудников, которые проходили исключительно обучение, но не тренировку навыков. Оказалось, что через год, в течение которого сотрудники проходили несколько обучающих курсов, поведение изменилось в положительную сторону лишь у 9% сотрудников (рисунок 1).

Полученные результаты отражают закон забывания Г. Эббингауза, в соответствии с которым курсы обучения эффективны в течение трёх дней, а затем 90% материала забывается.

Прохождения курсов недостаточно. Необходимо формировать навыки, закрепляя полученные знания с помощью тренировок. При добавлении к обучению тренировки в виде рассылки имитированных атак эффективность информирования повышается в 5 раз, с 9 до 49% (рисунок 2).

Что делать. Кроме курсов обучения, обязательно тренируйте навыки безопасной работы сотрудников, чтобы закрепить полученные ими знания и сделать их частью автоматического, «рефлексивного» поведения.

2. БУХГАЛТЕРИЯ И АДМИНИСТРАТИВНЫЙ ПЕРСОНАЛ — САМЫЕ ЛЕГКОМЫСЛЕННЫЕ СОТРУДНИКИ

Ещё одно стойкое заблуждение ИБ-сотрудников состоит в том, что бухгалтерия, менеджеры и административные сотрудники представляют наибольшую проблему с точки зрения безопасности. На рисунке 3 приведены данные опроса ведущих специалистов ИБ.

На самом деле. Согласно данным, полученным в результате 100 тыс. имитированных фишинговых атак, в которых приняли участие 20 тыс. сотрудников 48 компаний-клиентов «Антифишинг», наибольшее число

небезопасных действий совершают представители «творческих» профессий, а также стажёры и ИТ-специалисты (рисунок 4).

Что делать. Оценивать реальную защищённость всех сотрудников, тренировать навыки по объективным результатам — рейтингу поведения каждого сотрудника, а не на основе «веры» в то, какой отдел более уязвим.

3. РАССЫЛКИ РАЗ В ПОЛГОДА ПОМОГУТ СФОРМИРОВАТЬ НАВЫКИ ИБ У СОТРУДНИКОВ

«Достаточно совершать рассылку имитированных атак раз в полгода, раз в год, чтобы формировать и поддерживать навыки ИБ у сотрудников».

На самом деле. Редкие атаки ничего не меняют. Статистика демонстрирует аморфный набор данных о поведении сотрудников без выраженной тенденции к повышению уровня безопасного поведения, как в случае с мифом № 1. Время от времени встречаются «резкие выбросы» в отрицательную сторону при повышении сложности атаки.

Редкие рассылки не позволяют сформировать навыки и являются инструментом проверки изменений в поведении пользователей за период.

Важно проводить рассылку имитированных атак регулярно, поддерживая максимальное разнообразие психологических манипулятивных приёмов в самих атаках (см. Классификация Антифишинг), чтобы действительно формировать и закреплять навыки и настороженность сотрудников в части ИБ.

Что делать. Проводить тренировку навыков с помощью имитированных атак раз в месяц или чаще.

4. ЧАСТОТА ВАЖНЕЕ СОДЕРЖАНИЯ РАССЫЛОК. РЕГУЛЯРНЫЕ ОДНОТИПНЫЕ АТАКИ ПОМОГУТ ИЗМЕНИТЬ ПОВЕДЕНИЕ СОТРУДНИКОВ

«Мы не видим смысла тренировать сотрудников против внешнего спама», «У нас невозможно подделать письмо от лица коллег», «У нас есть ежеквартальная корпоративная рассылка, её мы и будем регулярно имитировать», «Мы видим заметный прогресс — поведение людей действительно изменилось».

На самом деле. Когда специалисты ИБ не отслеживают содержание имитированных атак или застревают на одном и том же виде рассылок, получается эффект спама. Сотрудники действительно быстро натренировываются, но только против одного вида атак. Устойчивость к одному виду манипулятивного воздействия

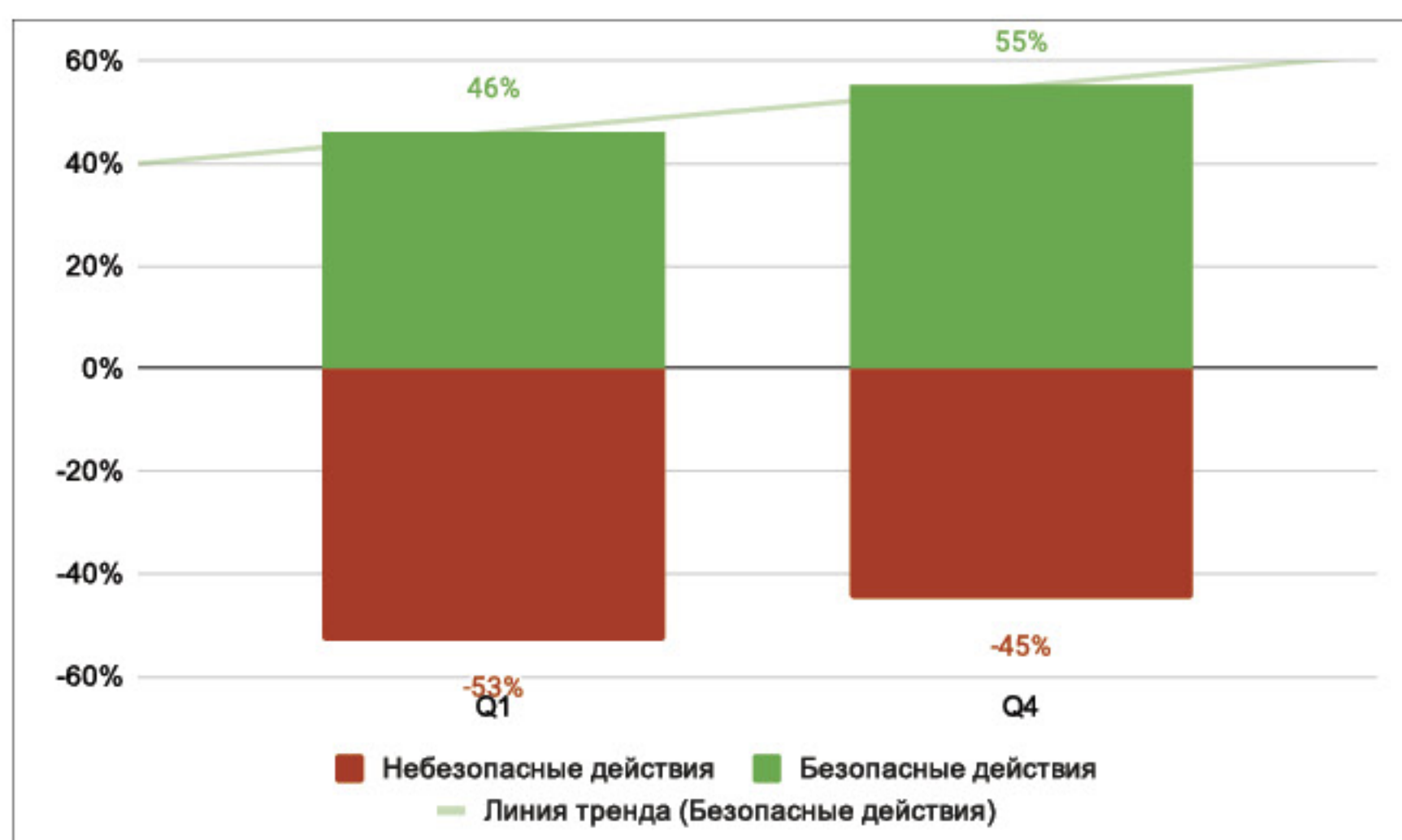


Рисунок 1. Изменения поведения пользователей, проходивших только обучающие курсы

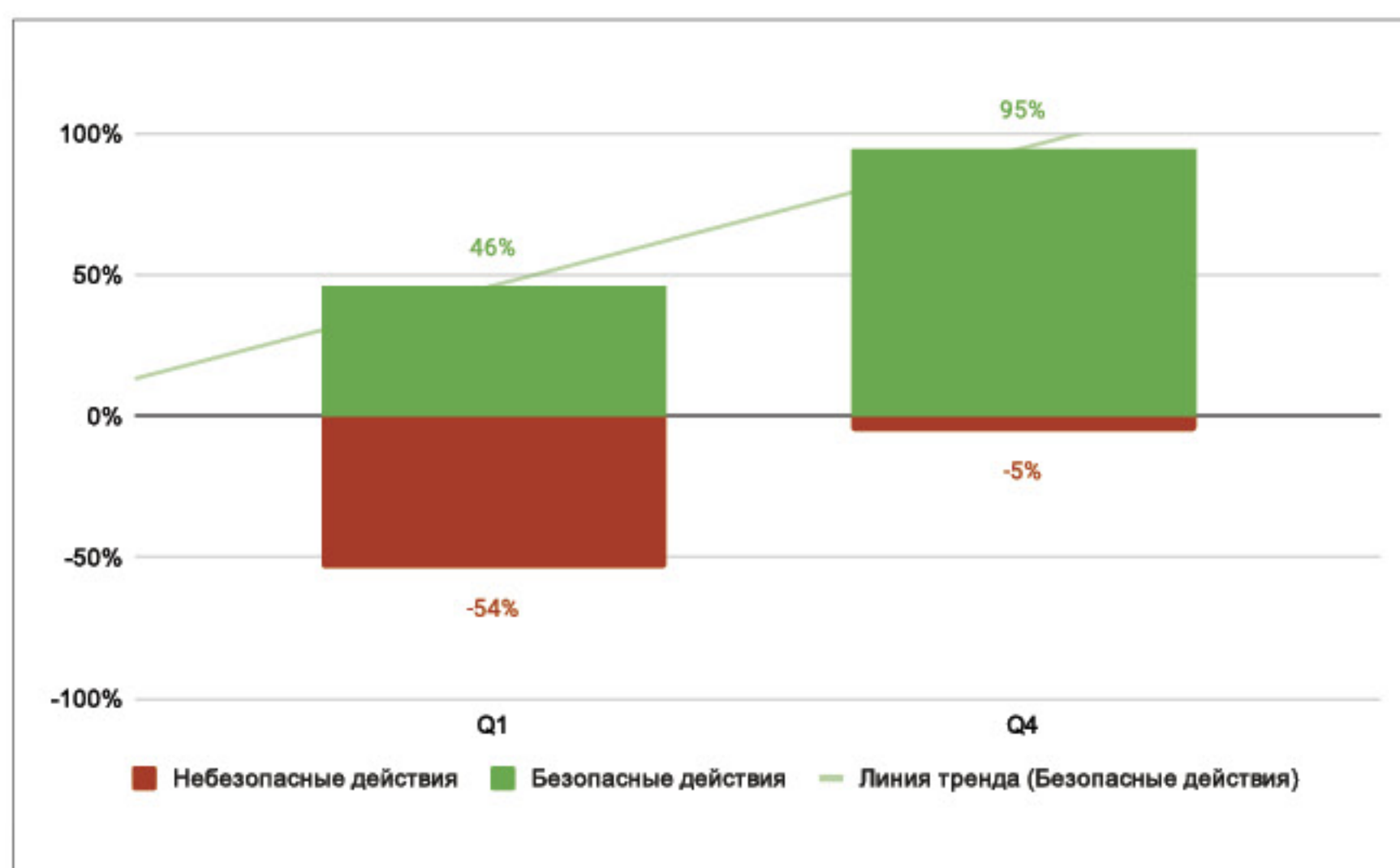


Рисунок 2. Изменения поведения пользователей, проходивших обучающие курсы и тренировку навыков через имитированные атаки

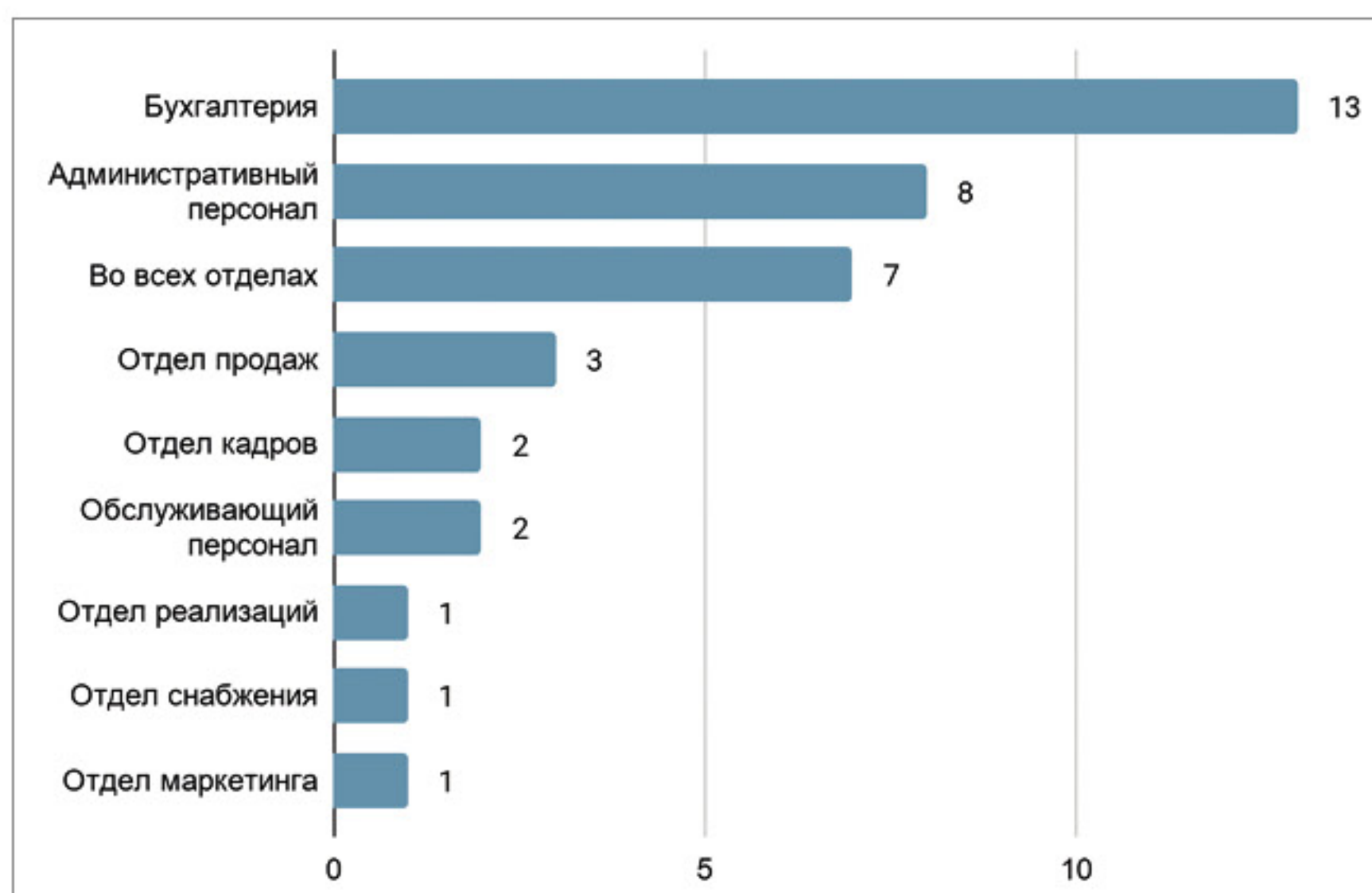


Рисунок 3. Самые «небезопасные» сотрудники с точки зрения ИБ-специалистов

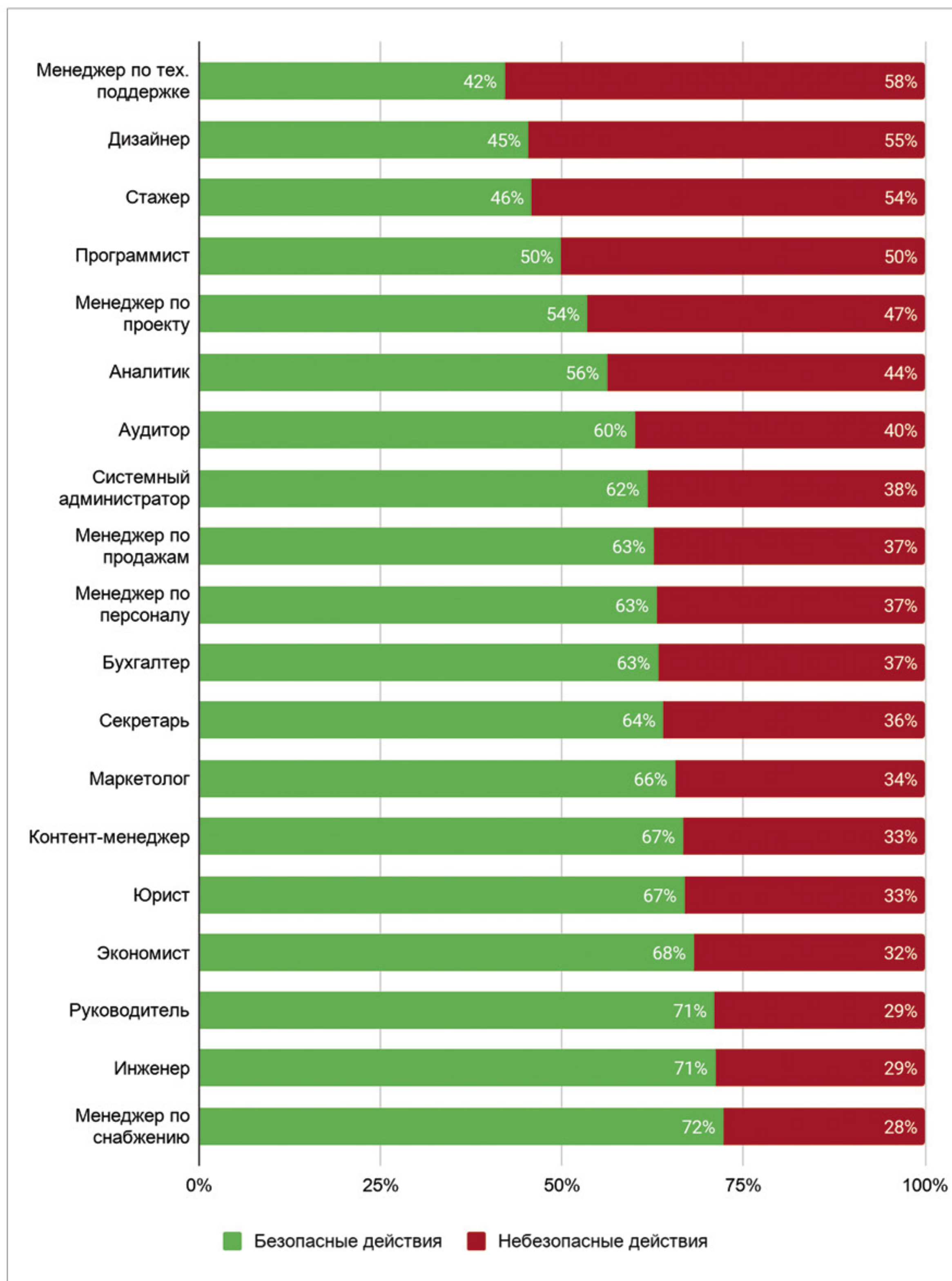


Рисунок 4. Распределение безопасных и небезопасных действий среди подразделений

делает самоуверенных сотрудников более уязвимыми к другим видам воздействия в атаках.

Хорошим примером этого является следующий кейс с естественной, не навязанной маркетингом динамикой безопасного поведения сотрудников (рисунок 5).

Естественная динамика обучения чему-либо — постепенный прогресс, с застреваниями

и периодическими «откатами» (кривая процесса обучения А. Бандуры), а не ракета, устремлённая в космос, как обычно рисуют маркетологи.

На рисунке 5 отслеживается рост динамики эффективности навыков безопасного поведения. Однако периодически устойчивость сотрудников «проседает». Причина — в поддержании

разнообразия и постепенном усложнении «обучающего материала», т.е. самих атак.

Более ярко эта тенденция видна при изучении «микродинамики» прогресса тренировки навыков у сотрудников в разрезе отдельных факторов, например источника атаки — внешний и корпоративный.

Далее представлены графики эффективности тренировки сотрудников по разным источникам атак (рисунки 6–7).

Как видно из рисунков, эффективность тренировок по источнику более выражена. Тем не менее нельзя исключать, что, кроме источника атаки, были и другие векторы воздействия на сотрудников, которые тоже оказывали влияние на периодическую «неготовность» сотрудников противостоять им.

Что делать. Сделайте атаки более разнообразными, используйте в них разные психологические и технические векторы.

5. ПОЛЬЗОВАТЕЛИ НЕ ОБУЧАЕМЫ. ТЕКУЧКА ПЕРСОНАЛА НЕИЗБЕЖНО СЛОМАЕТ ВСЬ ПРОЦЕСС

Безопасники часто не могут подойти к вопросу человеческого фактора системно. Им кажется, что знания и навыки людей нельзя сформировать, а поведение нельзя изменить. Это заставляет их с грустью листать каталоги вендоров защитных решений, выбирая то, что точно должно сработать и не будет зависеть от людей и их эмоций.

На самом деле. Поведение людей улучшается даже при высоком уровне текучки персонала. Это видно из графиков в мифах № 1 (улучшение поведения однородной выборки) и № 4 (улучшение поведения разнородной выборки). Разумеется, высокий уровень текучки снижает положительную динамику безопасного поведения, однако она всё равно присутствует.

Что делать. Системно и регулярно тренировать навыки ИБ у сотрудников и контролировать результаты, выбирая самые эффективные типы атак.

* * *

Факты и статистика — наши лучшие друзья. Поведение людей — значимая проблема, но её грамотное решение вполне по силам ИБ-специалистам. Главное при этом — использовать научный подход, вести процесс системно и методологически грамотно!

Больше полезных фактов будет доступно в годовом отчёте «Антифишинга» за 2020 год. Следите за анонсами в телеграм-канале «Антифишинга» и публикациях BIS Journal.



Рисунок 5. Распределение безопасных и небезопасных действий при частых однотипных атаках

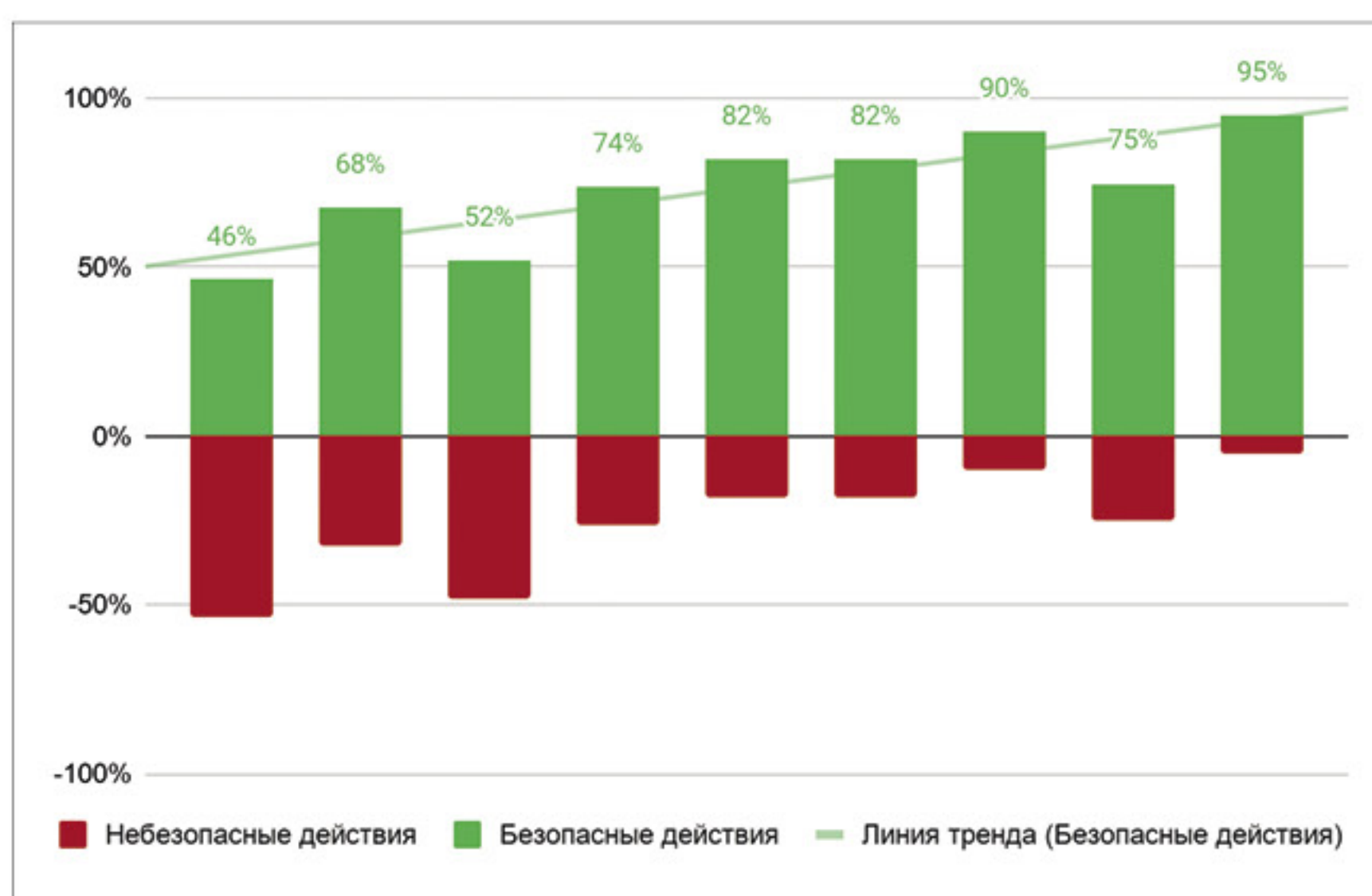


Рисунок 6. Эффективность тренировки по внешнему источнику

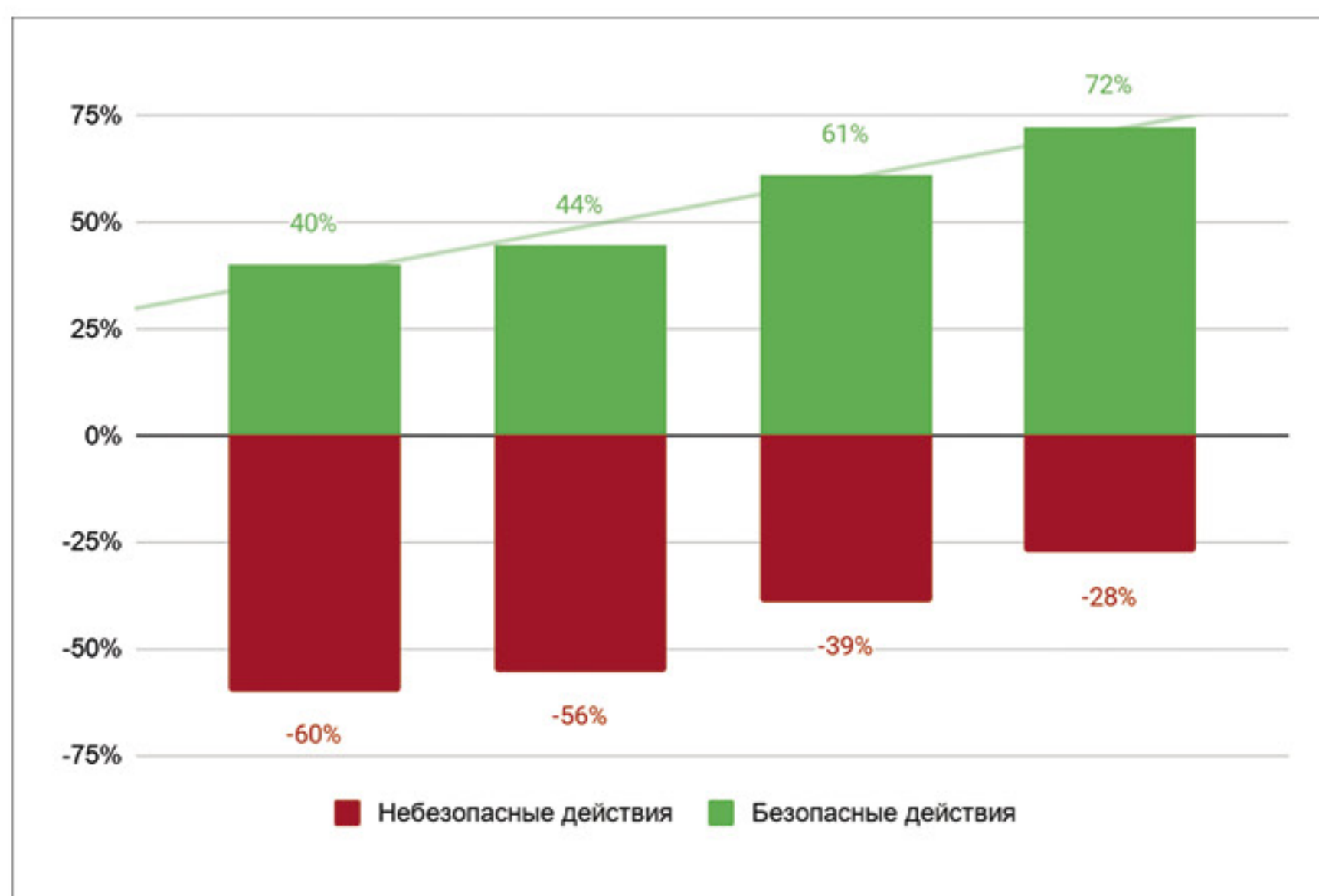


Рисунок 7. Эффективность тренировки по корпоративному источнику

«ОТДЕЛКА ЩЕНКА ПОД КАПИТАНА»

РАБОТА С ВОЗРАЖЕНИЯМИ СОТРУДНИКОВ
В ПРОЦЕССАХ ОБУЧЕНИЯ И ТРЕНИРОВКИ НАВЫКОВ ИБ¹



Ольга ЛИМОНОВА
психолог
ООО «Антифишинг»



Андрей ЖАРКЕВИЧ
редактор
ООО «Антифишинг»

5. «ЭТО ВСЁ РАВНО НИЧЕГО НЕ ДАСТ»

Причины. Редкий и неприятный тип возражений. Рациональной причиной может быть скептицизм и непонимание практической значимости. Как правило, достаточно обычного информирования с конкретными показателями, чтобы снять такую причину.

Нерациональными же причинами данного возражения обычно являются низкая самооценка сотрудника, его депрессивный склад личности или снова лень, прикрытая неудачной и непродуманной отговоркой. В первом случае нужен более деликатный подход, во втором хорошо работает всё та же «обязаловка».

Важно! Если вы сталкиваетесь с ярко выраженным депрессивным эпизодом со стороны сотрудника, не стоит предпринимать активных действий. Целесообразно передать информацию в HR-отдел для безопасного урегулирования этой ситуации.

Краткосрочные решения

а. Объясните, что данные процессы являются обязательной частью работы.

б. Ознакомьте сотрудников с наглядной статистикой (общей или по компании) имеющегося ущерба и потенциальных рисков от киберугроз.

Долгосрочные решения

а. Транслируйте ценность обучения/тренировок для компании и сотрудника в карьере и личной жизни посредством вводной информации в курсах обучения, информационных баннеров/плакатов и т.п. Используйте наглядные примеры и реальные цифры.

Ценность ИБ знаний/навыков для компании:

- предотвращение финансовых хищений,
- сохранение и улучшение репутации компании,
- конкурентное преимущество,
- лояльность и доверие клиентов,
- сохранение коммерческих конфиденциальных данных, секретов успеха компании,
- сохранение конфиденциальной информации сотрудников,

- обеспечение своевременного исполнения обязательств,
- сохранение рабочих процессов,
- отсутствие санкций регуляторов.

Ценность ИБ знаний/навыков для сотрудников в карьере:

- подтверждение профессионализма,
- доверие со стороны руководства, коллег и клиентов,
- возможность продвижения по службе,
- повышение ценности на рынке труда, привлекательности для новых работодателей,
- сохранение рабочих файлов,
- отсутствие штрафов,
- отсутствие ненужных ограничений на рабочем месте.

Ценность ИБ знаний/навыков для сотрудников в личной жизни:

- возможность обучить безопасному поведению семью и близких, тем самым защитив,
- исключить утечку личной конфиденциальной информации,
- защита от шантажа и «сливов»,
- защита от финансовых потерь,
- защита от слежки,
- защита от взлома домашнего интернета и устройств «умного дома»,
- возможность обезопасить себя и близких в общественных местах.

б. Транслируйте ценность ИБ, сообщая сотрудникам, сколько атак удалось зафиксировать вообще и с их помощью за период.

с. Создайте систему положительной мотивации, где выявление настоящих атак и оповещение об этом отдела ИБ влечёт какое-либо вознаграждение.

6. «НА МЕНЯ НЕТ АТАК! ЗАЧЕМ МЕНЯ КОМУ-НИБУДЬ ВЗЛАМЫВАТЬ?»

Причины. Подобные возражения свидетельствуют о полном непонимании существующих киберугроз или являются отговоркой. В первом случае сотрудник нуждается в подробном информировании про фишинг, в особенности целевой, и компрометацию деловой переписки (BEC), а

¹ Продолжение. Начало в №4/2020

также в ознакомлении с актуальной статистикой по причинённому ущербу в отрасли компании. Во втором случае достаточно настоять на обязательности прохождения обучения/тренировок. Подобный тип возражений не представляет большой сложности для разрешения, так как за ним нет никаких рациональных аргументов, к которым может апеллировать сотрудник.

Краткосрочные решения

а. Кратко ознакомить через письмо или назначить курс обучения по целевому фишингу и ВЕС.

б. Ознакомить с актуальной статистикой ущерба в результате атак на сотрудников компании.

с. Напомнить про обязательность обучения/тренировок для всех сотрудников.

Долгосрочные решения

а. Транслируйте ценность обучения/тренировок для компании и сотрудника в карьере и личной жизни, посредством вводной информации в курсах обучения, информационных баннеров/плакатов и т.п. Используйте наглядные примеры и реальные цифры.

б. Транслируйте ценность ИБ посредством информирования сотрудников о количестве атак, которые удалось детектировать вообще и с их помощью за N период и т.п.

7. «ИЗВИНИТЕ, ЗАБЫЛ»

Причины. Подобные фразы не являются возражением в чистом виде, однако демонстрируют пассивное сопротивление сотрудников. В исключительных случаях рациональной причиной забывчивости может оказаться ранняя деменция, но в остальных ситуациях это либо отговорка, либо свидетельство по-настоящему большой рабочей нагрузки сотрудника.

В случае отговорки отлично работает напоминание об «обязаловке» и системе штрафов, а в случае отсутствия свободного времени — регулярные автоматические напоминания и возможность самостоятельно выбрать удобное время для прохождения обучения/тренировок.

Краткосрочные решения

а. Предложите выбрать удобное время/день для прохождения обучения/тренировок (при фиксации обязательных временных рамок).

б. Регулярно напоминайте про обучение/тренировки при необходимости.

Долгосрочные решения

а. Автоматизируйте систему напоминаний о необходимости пройти сотрудникам обучение/тренировки. Например, рядовым сотрудникам достаточно напоминать о необходимости пройти обучение/тренировки не чаще раза в месяц, а тем, кто более одного раза нарушил сроки обучения/

тренировок, стоит отправлять напоминания еженедельно в начале или середине рабочей недели.

б. Введите официальную систему штрафов за N нарушений сроков обучения/тренировок. К примеру, в случае нарушения сроков обучения/тренировок более чем два раза можно накладывать на сотрудника денежный штраф или ограничивать в «технических» доступах, искусственно создавая «неудобные» условия работы.

8. «У ВАС ТАМ ЧТО-ТО ГЛЮЧИТ, ВСЁ ПОЛОМАНО...»

Причины. Встретившись с подобными возражениями, в первую очередь важно разобраться, нет ли действительно технических проблем, и лишь затем ориентировать сотрудника на необходимость проявлять большую активность в процессе обучения/тренировок. Кроме технических проблем, причиной этого возражения может быть техническая неграмотность сотрудника, сложность конструкции курса обучения или платформы, а также отсутствие или сложность прилагающихся инструкций. Очевидно, чтобы это разрешить, нужно обеспечить, чтобы инструкции по использованию системы были максимально простыми, короткими и понятными для любой категории сотрудников.

Краткосрочные решения

а. Проверьте корректность технических настроек.

б. При обнаружении ошибок помогите устранить их.

с. Дайте дополнительные пояснения к имеющимся инструкциям, если сотрудникам что-то конкретное непонятно.

д. Предложите воспользоваться другим рабочим местом для прохождения обучения.

Долгосрочные решения

а. Создайте или переработайте имеющиеся инструкции к обучению/тренировкам, сделав их максимально короткими и понятными для любой аудитории.

б. Регулярно контролируйте актуальность оборудования и ПО сотрудников, его совместимость с контентом обучения/тренировок. При возможности автоматизируйте данный процесс.

с. Заранее объясните сотрудникам, что делать в случае возникновения технических ошибок в процессе обучения/тренировок. Для этого в существующих инструкциях следует добавить разделы, описывающие алгоритм действия сотрудника в подобных ситуациях.

9. «ЭТО НЕ ВХОДИТ В МОИ ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ»

Причины. Подобные возражения возможны только в случае, если в трудовом договоре,

должностной инструкции или других документах не были прописаны обязательства сотрудника в части соблюдения правил ИБ и необходимости своевременно проходить назначенное обучение/тренировки. Грустно, если сотрудник просто не помнит о таких пунктах и не понимает необходимости соблюдения требований ИБ. Решением данного типа возражений может быть только отсылка к регламентным документам, подтверждающим должностные обязанности сотрудника в части соблюдения ИБ в компании.

Краткосрочные решения

а. Объясните, что данные процессы являются частью обязательной работы, даже если до этого сотрудник никогда с такими требованиями не сталкивался.

б. Ознакомьте с наглядной статистикой (общей или по компании) имеющегося ущерба и потенциальных рисков от киберугроз.

Долгосрочные решения

а. Внесите необходимость и обязательность обучения/тренировок в стандартные трудовые договоры, типовые должностные инструкции и другие нормативные документы.

б. Транслируйте ценность обучения/тренировок для компании и сотрудника в карьере и личной жизни посредством вводной информации в курсах обучения, информационных баннеров/плакатов и т.п. Используйте наглядные примеры и реальные цифры.

10. «ВСЁ РАВНО ВЫ МНЕ НИЧЕГО НЕ СДЕЛАЕТЕ»

Причины. При столкновении с этим типом возражений не стоит искать рациональной причины. Здесь имеет место пассивная агрессия со стороны сотрудника, который намеренно создаёт конфликт и/или таким образом самоутверждается, демонстрируя собственную неуязвимость. Возникновение данного типа возражений говорит о несостоятельности или полном отсутствии проактивных мер контроля и наказания со стороны отдела ИБ. Проработка этих мер и будет искомым решением для данной ситуации.

Важно! Проявляйте стойкость и не допускайте эмоциональной реакции на подобные заявления сотрудников.

Краткосрочные решения

а. Объясните, что эти процессы являются частью обязательной работы и что их невыполнение ведёт к штрафам.

б. Используйте авторитет вышестоящего руководителя: обратитесь к руководителю сотрудника, чтобы тот самостоятельно выбрал и назначил время/дату прохождения обучения/тренировок для данного сотрудника.

Долгосрочные решения

а. Разработайте и внедрите систему поощрения и штрафов (материальных и нематериальных), которая будет содействовать ИБ-процессам.

б. Транслируйте ценность обучения и тренировок ИБ как часть корпоративных ценностей компании, которые обязаны разделять все сотрудники компании.

11. «А ЧТО МНЕ ЗА ЭТО БУДЕТ?»

Причины. Этот тип возражения чаще всего приходит от любителей поторговаться. Не стоит воспринимать такие сообщения негативно. Просто некоторые сотрудники нуждаются в более выраженной системе внешней мотивации, а значит, им нужно обеспечить её, чтобы в дальнейшем с подобным не сталкиваться.

Краткосрочные решения

а. Объясните, что данные процессы являются частью обязательной работы.

б. Проинформируйте о существующей системе вознаграждения за прохождение обучения/тренировок.

Долгосрочные решения

а. Разработайте и внедрите систему поощрения и штрафов в компании, которая будет содействовать ИБ-процессам. Здесь важно прописать все условия, сделав их максимально понятными и прозрачными.

б. Создайте систему рейтинга для поощрения конкуренции и наглядности личных успехов. В данном случае сотрудники отлично будут видеть, чего им не хватает для вознаграждения, и будут иметь возможность принимать проактивное участие в этом.

с. Транслируйте ценность обучения/тренировок для компании и сотрудника в карьере и личной жизни посредством вводной информации в курсах обучения, информационных баннеров/плакатов и т.п. Используйте наглядные примеры и реальные цифры.

12. «Я УВОЛЮСЬ, ЕСЛИ НЕ ОТСТАНЕТЕ»

Причины. Этот тип возражений является открытой манипуляцией, попыткой сыграть на эмоции страха у специалиста ИБ. Такие сотрудники склонны к пассивной агрессии, чрезмерно уверены в собственной незаменимости и, соответственно, неуязвимости. Реже подобные возражения можно услышать от людей, прикрывающих свой страх неудачи громкой риторикой, но такое тоже встречается. Единственной корректной стратегией решения данного возражения является объяснение важности ИБ в компании и в целом, а также апелляция к регламентирующим документам.

Важно! Не пытайтесь этот тип возражений решить исключительно своими силами. Подобные

кейсы необходимо делать максимально публичными, чтобы урегулировать ситуацию с привлечением вышестоящего руководства.

Краткосрочные решения

а. Объясните, что данные процессы являются частью обязательной работы.

б. Используйте авторитет вышестоящего непосредственного руководителя: обратитесь напрямую к руководителю сотрудника для выяснения обстоятельств подобного поведения. Возможно, человек испытывает сильный стресс по семейным обстоятельствам либо и так уже находится на грани увольнения. Вместе с руководителем же вы можете решить, какие меры в итоге стоит применить.

с. Помогите сотруднику соотнести потенциальные риски от киберугрозы с его профессиональной ценностью для компании. Для этого может быть собран даже целый дисциплинарный совет, так как подобное поведение несёт в себе настоящую угрозу безопасности компании и должно решаться не только отделом ИБ.

Долгосрочные решения

а. Внедрите в начальный этап собеседования кандидатов в компанию вопросы об отношении к ИБ и готовности соблюдать правила и требования отдела ИБ. Для этого обратитесь к HR-отделу и поясните данную необходимость ввиду потенциальных неприятных инцидентов.

б. Внесите необходимость и обязательность обучения/тренировок в ТД, ДИ или другие регламентационные документы.

с. Транслируйте ценность обучения и тренировок ИБ как часть корпоративных ценностей компании. Если сотрудник в данных обстоятельствах не согласен с обучением/тренировками ИБ, то он явно в компании долго не продержится, поэтому можно давать знак HR-отделу начинать искать ему замену или распределять его рабочие функции между другими коллегами.

13. «МОЙ НАЧАЛЬНИК НАСТАИВАЕТ, ЧТОБЫ Я СНАЧАЛА СДЕЛАЛ СВОЮ РАБОТУ»

Причины. Среди рациональных причин этого типа возражений может быть реальное пренебрежение процессами ИБ со стороны непосредственного руководителя сотрудника либо ярко выраженная нехватка рабочего времени и горящие сроки. Но помимо этого, такое возражение может быть отговоркой, попыткой сотрудника прикрыться авторитетом и дружескими отношениями со своим руководителем. Чтобы предотвратить такую ситуацию, важно давать инструкции и вовлекать всех руководителей в процессы ИБ, наделяя их дополнительными полномочиями и необходимыми средствами.

Не стоит рассчитывать на проактивность сотрудников в процессах, напрямую не связанных с их основным родом деятельности

Краткосрочные решения

а. Задействуйте в решении этой ситуации непосредственного руководителя сотрудника: уточните наличие рациональных причин, наличие ближайшей возможности пройти обучение/тренировки, оцените в целом компетентность руководителя в данных процессах и потребности в дополнительном инструктаже или переобучении.

б. Предложите сотруднику вместе с руководителем выбрать удобное время для его обучения/тренировок.

Долгосрочные решения

а. Проводите дополнительное обучение руководителей на местах тому, как организовывать и мотивировать сотрудников соблюдать правила ИБ, проходить обучение и тренировки.

б. Чтобы снять рациональные возражения, обеспечьте гибкость графика обучения/тренировок, возможность выбора сотрудниками удобного для них времени обучения/тренировок.

14. «МЕНЯ НЕ ПРЕДУПРЕЖДАЛИ, НЕ РАССКАЗАЛИ ПРАВИЛА, Я ТУТ НИ ПРИ ЧЁМ...»

Причины. Этот тип возражений может возникнуть, если в компании отсутствует или слабо развита система оповещения и инструктирования сотрудников по процессам ИБ. Но значительно чаще за подобными формулировками скрывается обычная отговорка в попытке избежать ответственности за собственную лень, некомпетентность или невнимательность. Не стоит рассчитывать на проактивность сотрудников в процессах, напрямую не связанных с их основным родом деятельности. Чтобы не давать возможности пользоваться подобными возражениями, достаточно проработать и активно использовать систему оповещений и напоминаний по ключевым процессам ИБ, в которых задействованы сотрудники. В краткосрочной перспективе в этом может помочь разработка полноценной программы адаптации персонала к процессам ИБ.

Краткосрочные решения

а. Разработайте и внедрите массовое инструктирование персонала перед обучением/тренировками. Это обязательный пункт, без которого существование подобных возражений сотрудников абсолютно оправдано.

б. Используйте систему оповещений, включая напоминания о необходимости пройти назначенное обучение/тренировки. Планируя оповещения, продумайте оптимальную периодичность и структуру процесса: предварительное оповещение, оповещение о назначенном актуальном обучении/тренировке, напоминание о необходимости пройти обучение/тренировку, оповещение о скором окончании сроков прохождения обучения/тренировки, оповещение о назначении повторного обучения/тренировки и т.д.

с. Ознакомьте дополнительно с имеющимися регламентирующими документами по процессам ИБ, сошлитесь на необходимость их соблюдения.

Долгосрочные решения

а. Совместно с HR-отделом внедрите в начальный этап собеседования кандидатов в компанию вопросы об отношении к ИБ, готовности соблюдать правила и требования отдела ИБ.

б. Внесите необходимость и обязательность обучения/тренировок в трудовые договоры, должностные инструкции и другие нормативные документы.

с. Разработайте и внедрите систему адаптации персонала к процессам ИБ, включая необходимый инструментарий в виде регулярных оповещений, напоминаний, информирования.

15. ПОЛНОЕ ИГНОРИРОВАНИЕ

Причины. Этот тип возражений самым распространённый и один из самых неприятных. Игнорирование — универсальная защитная форма поведения, а также вариация проявления пассивной агрессии. Как правило, если удаётся добиться общения, игнорирование трансформируется в один из перечисленных выше типов возражений и может иметь самые разные причины и пути разрешения. Именно поэтому важно действовать проактивно, чтобы сотрудник осознал, что демонстративное игнорирование не поможет ему избавиться от необходимости пройти назначенное обучение/тренировки.

Краткосрочные решения

а. Организуйте встречу с сотрудником. Игнорировать дистанционно гораздо проще,

ПРИНЦИПЫ РАБОТЫ С ВОЗРАЖЕНИЯМИ

Поскольку, кроме описанных возражений, вы можете столкнуться с другими их формами, приведём принципы обработки новых их разновидностей:

1. Выслушивайте сотрудника и задавайте уточняющие вопросы. Дайте сотруднику возможность высказать своё мнение. Только так можно распознать истинную причину возникшего возражения и понять, насколько она рациональна. Не торопите и не давите раньше времени. Не стесняйтесь спрашивать и уточнять, чтобы лучше разобраться в ситуации.

2. Осмыслите и найдите причину возражения. Не отвечайте однотипными директивными сообщениями. Подходите к каждому возражению индивидуально. Приведённые ранее способы разрешения возражений помогают сформировать общее представление о типах возражения и их способах решения у не подготовленных к этому ИБ-специалистов. В реальности часто требуется более деликатный подход и дополнительное осмысление возражений.

3. Благодарите сотрудников. Элементарная вежливость позволяет наладить общение и заложить фундамент положительного отношения к отделу ИБ. Если сотрудники будут чувствовать, что их возражения не пустой звук, что они могут быть полезны, они будут более активно участвовать в процессах ИБ.

4. Предложите разные варианты решения проблемы. Обеспечьте сотруднику иллюзию выбора в виде нескольких устраивающих вас вариантов. Это позволит сотрудникам

чувствовать себя более комфортно, поскольку они будут считать, что вам пришлось подстроиться под них. Как вариант, предлагайте сотрудникам разрабатывать собственные варианты решения проблем, развивая коммуникации и формируя их сопричастность.

5. Всегда аргументируйте свои требования. Аргументы давят на логику сотрудников и выводят их на рациональный уровень мышления. Вас никогда не будут воспринимать как тирана, если вы докажете полезность и ценность ваших требований, а тем более если ваши аргументы будут содержать пояснение выгоды лично для сотрудника.

6. Используйте «стадный инстинкт». Сотрудники становятся куда сговорчивее, когда видят чужой пример или узнают, что все в его отделе прошли обучение/тренировки, а он нет. В первую очередь это работает благодаря нежеланию отбиваться от команды и быть хуже кого-либо. Не нужно стесняться использовать эту особенность при столкновениях со сложными кейсами.

7. Обязательно убедитесь, что проблема устранена. Не пускайте всё на самотёк. Молчание не всегда означает согласие. Держите руку на пульсе.

8. Зафиксируйте сработавший способ устранения возражения и попытайтесь его оптимизировать («шлифовка»). Формируйте собственную базу удачных решений и ответов сотрудникам, доводите их до ума. Это позволит в дальнейшем сэкономить много времени во время отработки новых возражений.

чем глядя в глаза. Всего одна личная встреча в большинстве случаев решает данную ситуацию, создавая у сотрудника понимание того, что стратегия игнорирования может создать ему большие неприятности.

б. Задействуйте в решении данной ситуации непосредственного руководителя. Игнорировать собственного руководителя гораздо сложнее, чем малознакомых специалистов из другого отдела. Поэтому не стесняйтесь и обращайтесь за помощью в разрешении данных ситуаций к непосредственным руководителям.

с. Отправьте предупредительные оповещения о необходимости пройти обучение/тренировки. Используйте для этого систему из двух-трёх «предупредительных выстрелов». Если сотрудник не реагирует, применяйте актуальную систему штрафов, которая побудит его самого связаться с вами для разрешения данной неприятной ситуации.

Долгосрочные решения

а. Регулярно обучайте руководителей на местах тому, как организовывать и мотивировать сотрудников соблюдать правила ИБ, проходить обучение и тренировки.

б. Пригласите непосредственных руководителей принять участие в контроле / мониторинге обучения / тренировок подчинённых им сотрудников.

с. Разработайте и официально внедрите алгоритм поведения в случае возникновения данных ситуаций, в том числе после какого количества предварительных оповещений сотрудник получит штраф.

* * *

Возражения и работа с ними — объективная реальность, с которой сталкиваются не только продавцы, но и специалисты ИБ, внедряющие новые процессы в компании. Правильная обработка возражений — залог успеха почти любой выстроенной стратегии обучения и тренировки навыков. Каждое возражение требует индивидуального подхода и имеет свои особенности, с которыми нужно считаться. Приведённая в статье классификация возражений и методы их обработки помогут ИБ-специалистам разобраться в данном вопросе, повысить эффективность обучения сотрудников и улучшить кибербезопасность компании.

ЧТО МОЖЕТ ПОЙТИ НЕ ТАК?

Несмотря на все принятые меры, в редких случаях возможны эскалации и попытки сотрудников продолжить сопротивляться «навязываемым» процессам ИБ. Причинами подобного поведения могут быть:

1. Несогласие с аргументами. Здесь важно пересмотреть их и всегда совершенствоваться в собственных формулировках.

2. Несогласие с предложенными условиями обучения/тренировки. Здесь можно попытаться пойти навстречу в случае адекватных требований со стороны сотрудника либо применить однозначную директивность в стиле «с террористами переговоров не ведём».

3. Плохое настроение. Здесь может помочь терпение и попытка возобновить процесс обсуждения в другое время/день, когда сотрудник успокоится.

4. Желание самоутвердиться любой ценой. Здесь уместно терпение и однозначная директивность в своих требованиях.

5. Процесс «торговли». Здесь важно терпение и понимание, что для некоторых людей процесс в целом важнее итогового результата. Хорошо работают разные шуточные приёмы.

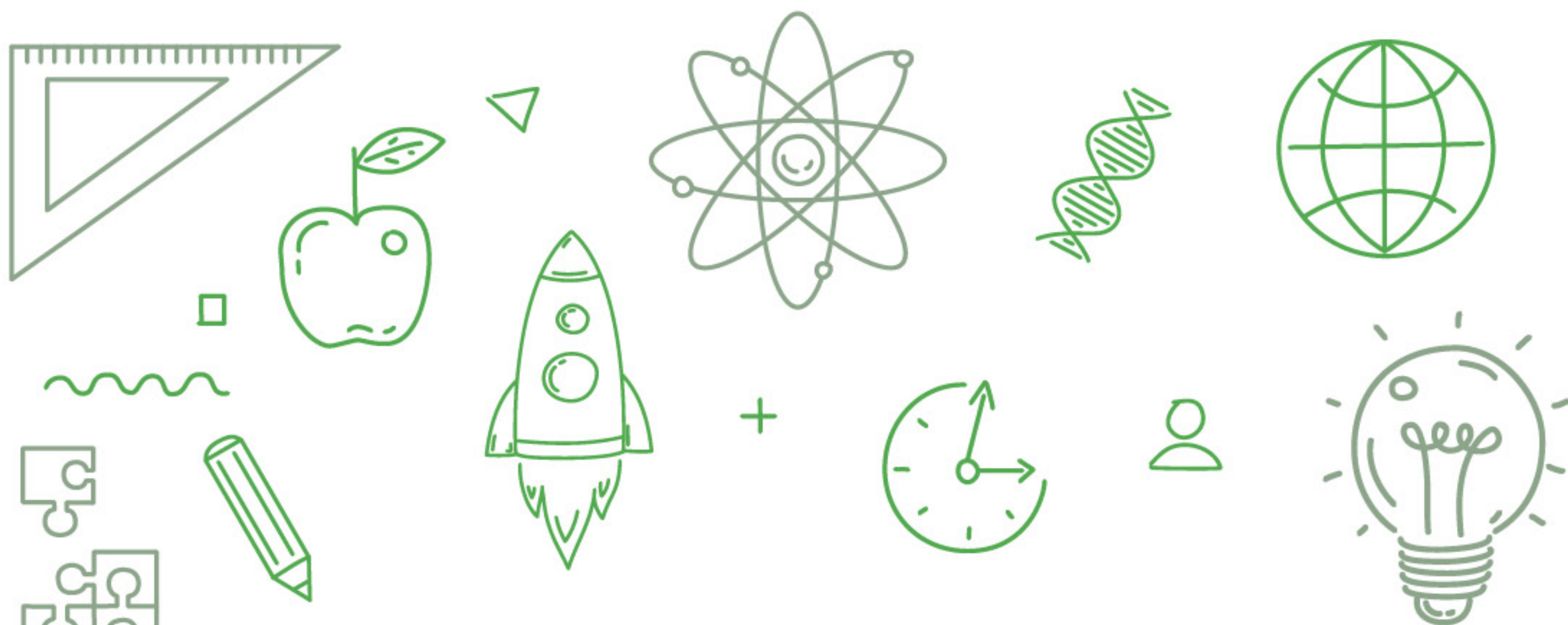
6. Желание оставить «козырь в рукаве». Здесь процесс «торговли» имеет свойство перерасти в манипуляцию, что разрешается только директивностью и воздействием через непосредственного руководителя.

ЧЕГО НЕ СТОИТ ДЕЛАТЬ

В любом процессе возможны ошибки. Вот чего точно не стоит делать при обработке возражений сотрудников:

- ◆ спорить;
- ◆ директивно приказывать, не выслушав до конца или не выяснив причин возражения;
- ◆ уходить от диалога в монолог;
- ◆ показывать свою некомпетентность;

- ◆ переадресовывать к другим специалистам;
- ◆ стесняться сотрудничать с руководителями на местах;
- ◆ бояться отвечать на самые дерзкие возражения;
- ◆ воспринимать возражения как что-то негативное;
- ◆ считать сотрудников дураками, а обработку возражений — бессмысленной.



«ВСЕ НА БОРЬБУ С НЕГРАМОТНОСТЬЮ!»

ЮНИСЕФ И ВСЕМИРНЫЙ БАНК БЬЮТ ТРЕВОГУ

Лозунг столетней давности становится актуальным в наши дни — проблемы в знаниях из-за карантина 2020–2021 гг. угрожают национальной безопасности многих стран. Тревогу бьют не только родители учеников, но и международные организации, такие как ЮНИСЕФ и Всемирный банк.

УКОЛОЛСЯ... И НА УРОК

Пандемия COVID-19 нанесла серьёзный ущерб образованию детей во всём мире. Вакцинация учителей считается важным шагом к тому, чтобы вернуть ситуацию в прежнее русло.

По данным ЮНИСЕФ¹, на пике первой волны коронавируса в конце апреля 2020 года закрытие общеобразовательных школ нарушило учебный процесс почти 90% учеников в мире. И, хотя к зиме 2020/2021 г. ситуация немного улучшилась, нет подтверждений, что закрытие школ замедляет распространение заболеваний. По мнению чиновников ЮНИСЕФ, школы не являются основным источником передачи инфекции. Но в связи со стремительным ростом числа заражённых многие страны принимают решение вновь закрыть учебные заведения. По состоянию на 1 декабря 2020 г. каждый пятый ученик в мире (или 320 млн детей) не посещает школу из-за карантина.

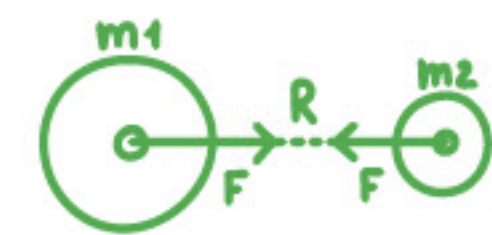
С началом кампании по вакцинации COVID-19 ЮНИСЕФ призвал вакцинировать преподавателей после медицинского персонала и групп населения, подверженных высокому риску заражения. Это поможет защитить учителей от вируса, позволит им выйти на работу и открыть школы.

Последствия продолжительных каникул и нарушения учебного процесса могут стать необратимыми, особенно для маргинализированных слоёв населения и бедных стран. Чем дольше дети остаются вне школы, тем меньше вероятность их возвращения к учёбе и тем сложнее их родителям вернуться на работу.

Решения об очерёдности вакцинации сложные, но приоритет учителей позволит защитить будущее подрастающего поколения. Ответственность за него лежит на сегодняшних руководителях государств, считают в ЮНИСЕФ.

ПРОГРАММЫ ПРИДЁТСЯ МЕНЯТЬ

«В 2018 году Группа Всемирного банка приступила к реализации Проекта развития человеческого капитала — глобальной инициативы, призванной помочь ускоренному осуществлению более масштабных и эффективных инвестиций в людей во имя упрочения социальной справедливости и роста экономики», — говорится в годовом отчёте Всемирного банка за 2019 г. Среди целей и задач Проекта — улучшение качества медицинского



Марина БРОДСКАЯ
обозреватель
BIS Journal

¹ ЮНИСЕФ — Детский фонд ООН, англ. United Nations Children's Fund, — специализированное учреждение ООН по координации программ помощи детям.

обслуживания и образовательных программ в беднейших странах мира, например Бангладеш, Замбии и Йемене, поддержка стран, запрашивающих финансирование или техническую помощь для достижения целей устойчивого развития.

Одна из целей — обеспечить доступ к качественному образованию и возможностям обучения на протяжении всей жизни для всех граждан к 2030 г. Для осуществления этих целей разработана Рамочная программа действий в области образования до 2030 г., она станет «дорожной картой» для стран-участников.

Но 2020 г. поставил перед Международным банком другие проблемы — последствия карантина COVID-19. Первый отчёт о ситуации в области среднего образования в странах Европы и Центральной Азии вышел в мае 2020 г., он был обновлён в конце ноября того же года, и, как отмечают его авторы, сбор данных продолжается.

Карантинные меры COVID-19 первой волны весны 2020 г. привели к фактической потере знаний и вероятным неблагоприятным последствиям для будущего поколения. Поэтому важно максимально смягчить долгосрочные последствия пандемии, которая нанесла урон образованию во всём мире.

COVID-19 КАК УГРОЗА БЕЗОПАСНОСТИ БУДУЩЕГО

Закрытие школ из-за карантина привело к серьёзным сбоям в процессе образования в странах Европы и Центральной Азии. По данным исследований, пандемия приводит не только к потере знаний, что выявляется тестированием учащихся, но и к увеличению социального неравенства. Страны с высоким уровнем дохода справляются с ситуацией быстрее, а в странах с более низким уровнем дохода граждан положение ухудшается.

На пике пандемии весной 2020 г. 45 стран Европы и Центральной Азии закрыли школы, от чего пострадали 185 млн учащихся. Из них 22 млн — дети, живущие в семьях с доходами ниже национального порога бедности. Такие семьи есть в 19 странах Европы и Центральной Азии. С учётом летних

каникул перерыв в обучении составил до полугода. Такая ситуация приведёт к сокращению числа несовершеннолетних, посещающих школы, которые и без пандемии всё чаще бросают учёбу.

Потери уже реальны. Первые результаты исследований показывают, что даже в благополучных странах Европы (Бельгия, Нидерланды, Швейцария, Великобритания, где школы были закрыты на 2–3 месяца) растёт социальное неравенство и ухудшаются показатели знаний учащихся. В Казахстане заметно ухудшились показатели знаний учащихся.

Потери знаний намного выше среди учащихся из малообразованных семей. Исследования показывают, что дети из социально и экономически благополучных семей получали большую поддержку родителей во время учёбы в период закрытия школы.

Ещё один аспект дистанционного образования — цифровизация экономики. По данным на 2016 г. 64% жителей Европы и Центральной Азии были подключены к интернету. Данные исследований Всемирного банка говорят об охвате 53% граждан в странах-клиентах Банка в регионе, что намного выше среднемирового показателя. Однако это «средняя температура по больнице», на практике существуют существенные различия: 20% охвата интернетом жителей Таджикистана и 75% — Литвы.

Учителя и администрация школ оказались неподготовленными к переходу на удалённую работу и экстренно создавали системы дистанционного обучения. По состоянию на начало декабря 2020 г. в странах Европы и Центральной Азии потеряны 5623 учебных дня: в среднем дети не ходили в школы по 3–4 месяца. С начала марта 2020 г. большинство школ в странах были закрыты.

Одной из главных проблем экстренного перехода на дистанционное образование (ДО) и самого ДО является отсутствие взаимодействия между учителем и учеником. Оно невозможно в условиях видео-конференц-связи или трансляции уроков в записи. Страны по-разному решали вопросы взаимодействия учителей и учеников: социальные сети, электронная почта,

мессенджеры, телефон и даже почта. Но способов обучения лучше прямого взаимодействия учителя и ученика на уроке не придумано.

ЦИФРОВИЗАЦИЯ КАК ПРИЧИНА СОЦИАЛЬНОГО НЕРАВЕНСТВА

Стараясь сохранить непрерывность образования, многие страны перешли на дистанционное обучение. Выбор методов обучения ещё больше углубил социальное неравенство как среди учеников, так и среди стран.

В одних странах были созданы или обновлены образовательные ресурсы на специализированных веб-сайтах. Другие (например, Россия и Турция) предлагают интерактивные онлайн-занятия, а учителя должны готовить онлайн-контент. В странах с низким проникновением интернета были задействованы традиционное телевидение и радиовещание для обеспечения непрерывности обучения, особенно для детей из социально уязвимых групп.

Если брать общемировую картину, то тенденции к сокращению знаний подрастающим поколением удручают.

Несмотря на значительный технологический потенциал, даже европейские страны с высоким уровнем доходов столкнулись с проблемами обучения и ростом неравенства при переходе к ДО. Что уж говорить о менее развитых странах, где технологический потенциал ниже, а большинство семей живёт за чертой бедности.

Треть стран Европы и Центральной Азии не полностью подключена к интернету. Только 50% школ имеют материально-техническую базу и IT-специалистов для подключения к интернету, чтобы предоставлять минимальный уровень образовательного контента. Можно ожидать, что негативные последствия закрытия школ для стран со средним и низким уровнем доходов будут значительными.

Как отмечают эксперты Всемирного банка, в будущем за порогом школы потери в образовании могут обернуться серьёзными проблемами. Снижение результатов тестов учащихся напрямую связано с сокращением занятости в перспективе. И наоборот, повышение

успеваемости и увеличение продолжительности обучения приводит к значительному увеличению доходов на протяжении всей жизни.

Осенью-зимой 2020 г. в связи с ростом числа случаев COVID-19 прошла вторая волна закрытия школ. Методы обучения со времён первой волны не сильно изменились, поэтому проблемы остались теми же: сокращение уровня образования, ограниченный доступ к высшему образованию, меньшая конкурентоспособность на рынке и более низкие доходы в будущем.

ЧТО ДЕЛАТЬ?

Эксперты Группы Всемирного банка для исправления ситуации в области образования предлагают план из трёх пунктов.

1. Восстановительные учебные программы. Для отстающих учеников должна быть разработана программа поддержки. Первый шаг — проведение тестирования для выявления таких учеников и их потребностей.

12-недельные учебные программы могут заменить 3–5 месяцев обычной учёбы. В Италии учащиеся средних школ, имевшие три часа онлайн-уроков

в неделю с компьютера или гаджетов, продемонстрировали рост успеваемости по математике, английскому и итальянскому языкам на 4,7 %.

Нестандартные учебные мероприятия, которые объединяют учащихся по уровню знаний, а не по возрасту или классу, и адаптированные учебные программы, ориентированные на базовые навыки, также приводят к улучшению показателей. Адаптированные образовательные системы, опирающиеся на текущий уровень знаний учеников, оказывают значительное влияние на результаты обучения, особенно среди отстающих. Педагоги лучше других знают потребности своих учеников, поэтому необходимо поддерживать учителей дополнительными ресурсами и обучением.

2. Сохранение и увеличение бюджета на образование. Для обеспечения устойчивого восстановления системы образования важно, чтобы государственный бюджет на образование был сохранён на прежнем уровне или увеличен. Школы при необходимости должны получать дополнительную финансовую поддержку. Чтобы помочь наиболее уязвимым группам

учащихся, правительства должны направить большую часть финансовых средств и ресурсов на поддержку школ и учеников, особенно если эти школы работают в социально неблагополучных областях.

В условиях «удалёнки» состоятельные семьи нанимают детям репетиторов, семьям с низкими доходами такие услуги не по карману. Здесь на помощь может прийти государство. Например, Великобритания объявила о создании Фонда поддержки учеников в размере 1 млрд фунтов стерлингов, часть средств пойдёт на Национальную программу репетиторства с бюджетом 76 млн фунтов стерлингов. Эти меры призваны подтянуть знания учеников на докарантинный уровень.

3. Создание платформ для различных форм обучения. Необходимо использовать опыт пандемии, чтобы подготовиться к будущим кризисам. Для этого важно разрабатывать платформы и программы ДО, чтобы иметь инструмент для быстрого перехода с очной на дистанционную форму обучения, разработать гибкие учебные программы, которые можно преподавать очно или онлайн. Для этого надо улучшать материально-техническую базу школ и повышать квалификацию преподавателей в области ИТ.

* * *

Найти альтернативные и эффективные методы обучения, способные заменить очное образование, сложно. Длительное закрытие школ не только усугубляет проблемы с образованием и психическим здоровьем, но и ставит в невыгодное положение учащихся из более бедных семей. Всё это наносит ущерб не только экономике стран в длительной перспективе, но и национальной безопасности: через 20–30 лет нынешние школьники придут на смену родителям. Конечно, необходимо стремиться, чтобы школы работали без длительных перерывов во время учебного года. Однако жизнь вносит свои коррективы, и необходимо заранее искать альтернативные и эффективные методы обучения.

ЦИФРЫ И ФАКТЫ ПО ЕВРОПЕ И ЦЕНТРАЛЬНОЙ АЗИИ

◆ Более 185 млн школьников вынуждены сидеть дома в период пандемии, часть из них учатся с помощью дистанционных технологий.

◆ 22 млн школьников в 19 странах Европы и Центральной Азии живут в семьях с доходами ниже национального порога бедности; многие из этих детей не ходили в школу или не участвовали в дистанционных уроках полгода.

◆ В дополнение к летним каникулам потеря трети учебного года отрицательно скажется в будущем на детях из семей с низким уровнем доходов. Отсев учеников из старшей школы может быть значительным.

◆ Студенты на «удалёнке» чаще бросают учёбу в высшем учебном заведении или получают более низкую квалификацию по сравнению со сверстниками, которые учатся очно.

◆ Увеличение неравенства доходов из-за пандемии коронавируса и вероятной рецессии будет угнетать развитие навыков в будущем у лиц из бедных слоёв общества.

◆ 16 % учителей в Европе сообщают о необходимости повышения квалификации по использованию информационно-телекоммуникационных технологий для дистанционного обучения, которые активно применяются для смягчения последствий коронавируса.

◆ Последствия COVID-19 могут увеличить разрыв в результатах обучения 104 млн учащихся из стран с высоким уровнем дохода и 59 млн человек, живущих в странах со средним уровнем дохода. Отмечается разрыв в 13 % между средним индексом человеческого капитала в этих странах.

ОНЛАЙН ПО-РУССКИ

ПРОБЛЕМ, КАК ВСЕГДА, ДВЕ: УЧИТЕЛЯ, УЧЕНИКИ... И ИХ РОДИТЕЛИ

В прошлом номере BIS Journal мы представили обзор онлайн-платформ для дистанционного обучения школьников в США. А что же происходит у нас? Роспотребнадзор продлил Санитарно-эпидемиологические правила для образовательных организаций и других объектов социальной инфраструктуры для детей и молодежи до 1 января 2022 г. Значит, учиться вдали от школ детям придётся ещё долго.

ЭКСПЕРИМЕНТ

7 декабря 2020 г. было принято Постановление Правительства Российской Федерации № 2040 «О проведении эксперимента о введении цифровой образовательной среды (ЦОС)». Согласно документу, в 10-дневный срок со дня вступления в силу постановления требуется разработать и утвердить порядок отбора субъектов РФ для проведения эксперимента, а также в течение одного месяца по согласованию с Минцифры РФ разработать и утвердить дорожную карту по проведению эксперимента.

Регионам, где с 10 декабря 2020 г. по 31 декабря 2022 г. будет проведён эксперимент, в течение двух месяцев со дня его начала необходимо заключить с Минпросвещения и Минцифры соглашение о взаимодействии в рамках эксперимента, а также в течение трёх месяцев разработать и утвердить свою дорожную карту по проведению эксперимента по согласованию с данными ведомствами.

«Этот документ, прежде всего, призван гарантировать всем учащимся, вне зависимости от того, где они живут, равные условия для получения качественного образования. Внедрение цифровой образовательной среды (ЦОС), о которой идёт речь в постановлении, никоим образом не подменяет собой традиционный, очный формат обучения как ключевой для российской системы образования», — отметил министр просвещения РФ Сергей Кравцов, слова которого приведены в сообщении ТАСС.

ОСНОВНЫЕ ЗАДАЧИ

В числе основных задач эксперимента указаны:

- ♦ создание, ввод в эксплуатацию, развитие и эксплуатация информационных систем и информационно-телекоммуникационной инфраструктуры, входящих в состав платформы цифровой образовательной среды;
- ♦ апробация функциональных возможностей платформы;
- ♦ оснащение школ материально-технической и информационно-телекоммуникационной инфраструктурой (интернетом, компьютерным, мультимедийным, презентационным оборудованием и программным обеспечением в соответствии с утверждённым стандартом, а также видео-конференц-связью в помещениях школ);
- ♦ развитие технологий и решений обработки и управления данными участников образовательных отношений на базе портала госуслуг;
- ♦ обеспечение возможности реализации образовательных программ с использованием дистанционных образовательных технологий и электронного обучения и применением портала госуслуг, информационной системы Минпросвещения России и информационно-коммуникационной образовательной платформы и т.д.

ГЕОГРАФИЯ

Летом 2020 г. Минпросвещения заявило о проведении эксперимента в 14 субъектах РФ. Это Алтайский край, Астраханская область, Калининградская область, Калужская область, Кемеровская область, Московская об-

ласть, Нижегородская область, Новгородская область, Новосибирская область, Пермский край, Сахалинская область, Тюменская область, Челябинская область, Ямало-Ненецкий автономный округ.

ПРИНЦИПЫ

Регионы получают средства из федерального бюджета на реализацию эксперимента в рамках госпрограммы «Развитие образования». Будет охвачено 1700 школ, им выделяют средства на обеспечение высокоскоростным доступом в интернет, компьютерами, программным обеспечением. Согласно проекту, основными принципами создания ЦОС, в частности, являются безопасность, приоритет отечественным технологиям, multifunctionality использования.

КАК В РЕАЛЬНОСТИ?

Однако в режиме дистанционного образования многие регионы, в том числе не попавшая в список пилотных Москва, с небольшими перерывами на посещение школы учатся с весны 2020 г. Кратко расскажем о том, как происходит обучение.

ЗОМ — ПОПУЛЯРНЫЙ, НО УЯЗВИМЫЙ

Программа Zoom стала необычайно популярной по всему миру весной 2020 г., когда массовый переход на дистанционную работу и образование вынудил пользователей искать удобную платформу для организации видеоконференций. Выбор, собственно, оказался невелик: Zoom, Skype, WhatsApp...

Основными принципами создания цифровой образовательной среды, в частности, являются безопасность, приоритет отечественным технологиям, multifunctionality использования



zoom

Популярный ранее для видео-конференц-связи (ВКС) Skype ограничивал численность участников, Google Classroom не нашёл широкого распространения и поддержки у преподавателей, а Zoom оказался на слуху и благодаря простоте в установке и использовании мгновенно стал востребованным по всему миру.

Учителей не смущали ограничения по времени бесплатной конференции (40 минут для урока достаточно), максимальное число участников — 100 человек — превышает втрое среднестатистический класс.

Среди обычных проблем платформы — зависания и внезапные отключения из-за повышенных нагрузок. Весной были популярны взломы ВКС в Zoom посторонними лицами. Исследователи безопасности находили бреши в информационной

безопасности (например, трафик шёл без сквозного шифрования) и уязвимости в приложении. Специалисты Zoom выпускали патчи, однако дыры в безопасности платформы по-прежнему остаются. Для их ликвидации компания наняла в апреле 2020 г. компанию Luta Security. За 90 дней планировалось улучшить вопросы ИБ и конфиденциальности информации пользователей, а также запустить программу bug bounty, в рамках которой всем нашедшим уязвимости в платформе и уведомившим компанию будут выплачивать вознаграждения.

Если судить по ленте новостей, число хакерских атак на участников zoom-конференций в конце года сократилось. Мелькают редкие сообщения о хакерских атаках из хулиганских побуждений на несколько школ и университетов в США.

TEAMS. МОСКОВСКАЯ АЛЬТЕРНАТИВА УВЯЗЛА В БОЛОТЕ

Что выбрать вместо уязвимого для хакеров Zoom? Этой осенью московские школьники и их родители столкнулись с альтернативной платформой — встроенной в Московскую электронную школу (МЭШ) Microsoft Teams. Если верить рекламе, то платформа должна была стать инструментарием для полноценной дистанционной работы ученика и учителя. Что вышло на практике?

Обкатка системы началась внезапно, во время вынужденных осенних «каникул». И тут в прессе начался разговор о многом: о полном непонимании большинством учителей и родителей основ IT, о неспособности авторов МЭШ — сотрудников Департамента информационных технологий города



Москвы — сделать работоспособный продукт, о неготовности школ к «удалёнке», об отсутствии материально-технической базы у учебных заведений и в семьях.

TEAMS. МЫТАРСТВА ПОЛЬЗОВАТЕЛЕЙ

Начнём с простого — с установки системы. Для этого родитель должен зайти под своей верифицированной заранее учётной записью и создать пароль для ребёнка (логин создаётся системой). После чего он должен перелогиниться под именем ребёнка, с его паролем войти в систему и зайти в онлайн-урок, открыв его в браузере своего устройства.

Сколько сил ещё весной ушло у пользователей на привязку аккаунта ребёнка к родительскому для создания пароля! По собственному опыту автора

и опыту других родителей эта элементарная функция, которая должна создаваться автоматически, начинала работать с третьей жалобы в техподдержку.

Дальше — больше. «Срочно удалите свой аккаунт на mos.ru и создайте аккаунт ребёнка, через час будет тренировочное подключение», — обычное для осени сообщение от учителя в чате класса. Следовали возмущённые возгласы родителей. В процессе выяснялось, что удалять ничего не надо, следует зайти под логином ребёнка. Дальше начинали выяснять, что такое браузер и как открыть Teams на телефоне по прямой ссылке в Google Chrome...

Все рекламные проспекты о том, как круто и легко работать в Teams, как просто записать и пересмотреть урок, как легко сделать домашнюю работу, которую также легко и просто

проверит учитель, в моём случае так и остались рекламными слоганами и красивыми картинками. Моему ребёнку толком проучиться в Teams так и не удалось — система висла, глючила, отключалась...

Виноватыми в этом объявлялись дети, которые «сломали» всё до начала уроков, родители, которые не купили своим детям компьютеры или хотя бы ноутбуки, а нашли деньги только на телефоны или в лучшем случае планшеты и не обеспечили детей отдельными комнатами, чтобы была возможность учиться с включённой веб-камерой, а также не провели домой высокоскоростной интернет... И учителя, которые не смогли заставить родителей думать о детях. Администрация школы снимала и снимает с себя всю ответственность за происходящее.

TEAMS. О БЕЗОПАСНОСТИ

О безопасности платформы Teams, которая противопоставлялась небезопасному Zoom, говорить не приходится. Родительские чаты полны рассказами о взломах Teams во время уроков, демонстрации порнографии и нецензурной брани под логинами учеников. Если сопоставить эти сообщения с новостями об утечке по вине сотрудников ДИТ Москвы данных о заболевших COVID-19 москвичах, то вопросы, кто виноват и что делать, очевидны даже неспециалисту в области информационной безопасности.

В СТИХИЙНОМ ПОИСКЕ

Часть школ и учителей тихо вернулась в Zoom. Некоторые выбрали другой инструмент — Discord, бесплатный мессенджер с поддержкой VoIP. Собственно, это известный ВКС, предназначенный для использования различными сообществами по интересам. Discord популярен у геймеров, однако его возможности — закрытые каналы, жёсткое модерирование участников и привязка их к классам и предметам — оказались полезными и для образовательных учреждений. По отзывам пользователей, попробовавших с детьми все возможные варианты образовательных платформ и систем ВКС типа MS Teams или Zoom, Discord оказался самым удобным и безопасным инструментом для учёбы. А функциональность платформы позволяет наполнить урок дополнительной информацией.

В ЧАСТНЫХ ШКОЛАХ

Много разнообразных образовательных платформ есть у частных школ. Например, платформа International Blended Learning School (IBLS). Она создана задолго до пандемии COVID-19 и реализует примерно тот контент, о котором заявлял ДИТ Москвы. Более того, она работает с МЭШ как с дополнительным инструментом. На базе этой платформы учатся дети с 1 по 11 класс, на ней реализованы видеоуроки, а также онлайн-уроки через Zoom, если есть желание послушать учителя вживую. Учебный план привязан к расписанию, есть промежуточная аттестация — контрольные работы и тесты по предметам, с разборами ошибок

и их объяснениями. Если нет желания выполнять промежуточные работы, то есть одна большая триместровая контрольная по каждому предмету.

Родитель может следить за расписанием ребёнка, видит его успеваемость, изучаемые темы и всегда может помочь. Если есть вопросы по конкретному уроку, в конце занятия есть форма обратной связи с учителем. Если в системе идёт обновление программного обеспечения, сообщения об этом присылаются заранее, а на выполнение самостоятельных и контрольных даётся отсрочка.

Недостаток таких платформ один — они поддерживаются частными школами и потому учёба на их базе платная. Однако и жалоб на взлом и противоправные действия во время уроков от пользователей частных образовательных онлайн-платформ нет.

В МУЗЫКАЛЬНЫХ ШКОЛАХ

В стороне от традиционного школьного образования в дистанционном формате стоит обучение музыке. Никто не мог предположить, что и освоение музыкальных инструментов и сольфеджио перейдёт в онлайн-режим. Кто-то проводит уроки по теории в Zoom или по Skype. Кто-то выкладывает домашние задания и требует отчитываться по ним на электронную почту или в WhatsApp. Есть и новинки в подходе к образованию: с весны 2020 г. на видеохостинге Youtube появилось много заданий по сольфеджио в формате музыкальных диктантов. Их активно используют преподаватели сольфеджио.

Мучением для всех участников процесса стали уроки по инструменту. Тут всё зависит и от учителя, и от ученика и его родителей, и... от администрации школы. Хорошо, если произведения начали разбирать очно в начале учебного года и ученик успел поучиться в музыкалке несколько лет в обычном режиме. Тогда сложностей с дальнейшим обучением меньше. Горе, если ученик первокурсник и ничего не умеет.

Многие учителя просто проводят урок через Zoom, Skype или WhatsApp, расположив камеру так, чтобы было видно ребёнка и инструмент. Тут самое сложное — не только настроить веб-камеру и в процессе 20–30-минутного

урока отработать материал, но и исправить технику игры. Главная проблема — отсутствие физического контакта. На то, что в классе можно сделать одним движением или личным примером учителя, в дистанционном формате уходит гораздо больше времени.

Отдельная песня начинается в музыкальных школах, где администрация не доверяет своим сотрудникам и ученикам. Бывают требования записывать занятия с трёх камер, чтобы в кадр попали ученик, его руки на инструменте и монитор, в котором виден учитель, проводящий урок. О качестве такого обучения речи уже не идёт — все участники процесса пребывают в постоянном стрессе.

Финальным аккордом занятий становятся экзамены. И если теорию можно формализовать в тесты в виде опросов на базе Yandex или Google, то со сдачей экзаменов по инструменту или вокалу начинаются проблемы: попасть в фонограмму, совпасть с присланным от аккомпаниатора темпом игры или просто записать выступление на телефон, исключив посторонние звуки и не забыв надеть концертные туфли... в общем, это то самое, где музыка и заканчивается. Итоги многократных перезаписей заливаются на сайт и просматриваются учителем. При необходимости процесс повторяется до получения удовлетворительного результата. Иного способа обучения музыке не придумано.

* * *

Что станет итогом дистанционного обучения школьников? Какие последствия такого образования мы получим через 5–10 лет? Многие родители и учителя уже сейчас бьют тревогу, пытаясь доказать, что очное образование становится привилегией для состоятельных граждан. Пока все нормативные документы по эксперименту говорят о добровольности онлайн-образования и его совместимостью с традиционной, очной, формой. Время многое покажет. Ясно одно — качественное образование детей остаётся заботой их родителей. Как и обеспечение информационной безопасности образовательного процесса.

ТУМАННЫЙ ЛОНДОН ЗАКРЫЛ ШКОЛЫ

НО ОБЕСПЕЧИЛ ПРИ ЭТОМ КАЧЕСТВЕННОЕ
ОБРАЗОВАНИЕ ДЛЯ ВСЕХ СЛОЁВ НАСЕЛЕНИЯ

В начале января 2021 года Правительство Великобритании приняло решение ввести национальный карантин и закрыть школы в связи с ухудшением эпидемиологической обстановки. Об этом заявил премьер-министр Борис Джонсон во время телеобращения к нации. Попробуем разобраться, как при этом организовано дистанционное обучение школьников.

МИНОБР РАБОТАЕТ НА НАЛОГОПЛАТЕЛЬЩИКОВ

Раздел «Образование и уход за детьми во время коронавируса (COVID-19)» на официальном сайте правительства Великобритании был создан ещё весной 2020 г. и регулярно обновляется Министерством образования с учётом новых обстоятельств.

Портал предназначен для родителей и опекунов детей от 2 лет, учеников начальной и средней школ, детей с особенностями развития, есть немного информации для студентов колледжей и университетов. «Никто не ожидает, что родители станут учителями или обеспечат деятельность и обратную связь, как в школе или детском саду. Родители и опекуны должны делать всё возможное, чтобы помочь детям учиться, занимаясь при этом своими делами», — говорится на сайте правительства. Раздел содержит подробное руководство по обучению детей дома, организации дня и учебного процесса. Не забыт и вопрос безопасности детей в сети.

ДИСТАНЦИОННОЕ ОБУЧЕНИЕ

Здесь собрано много информации: рекомендации, ресурсы и техническая поддержка для родителей, учителей и руководителей школ по обучению учеников и студентов во время коронавируса. Есть и ссылка на законодательную базу, отражены вопросы по

обеспечению безопасности учебного процесса онлайн, ссылки на образовательные ресурсы, включая разработки ресурсного центра Oak National Academy, который предоставляет бесплатные уроки и ресурсы для учителей и учеников в возрасте от 4 до 16 лет. Есть информация для местных властей, академических фондов и школ: об устройствах, доступе и работе в интернете, необходимых для обеспечения

дистанционного образования и социальной помощи детям во время коронавируса. На сайте можно составить план индивидуального обучения для детей с особыми потребностями в образовании или детей-инвалидов.

Школы и ученики могут отправить заявку на компенсационное финансирование и поддержку образования через Национальную программу репетиторства (NTP), на которую выделено

GOV.UK

[Home](#)

Part of Coronavirus (COVID-19)

Education and childcare

Guidance and support [Open all](#)

Pupil wellbeing and safety	+
Testing in schools, colleges and universities	+
Home learning during coronavirus	+
Exams and managing a school or early years setting	+
Funding and support for education and childcare	+
University students and higher education	+

Скриншот сайта www.gov.uk/coronavirus/education-and-childcare



650 млн фунтов стерлингов. Программа доступна для поддержки отстающих учеников, помощи и увеличения доступа к качественному образованию для малоимущих и социально уязвимых детей, помощи школам в реализации учебных программ, например получении средств на покупку дополнительных устройств или учебников. Известно, что в программе уже зарегистрировались почти 70 тыс. учеников.

НЕ НАДО «ИЗОБРЕТАТЬ ВЕЛОСИПЕД». ИЗОБРЕТЁН И СОЗДАН ПОЧТИ ГОД НАЗАД

Осенью 2020 г. школьники пошли в школы и, казалось, учебный процесс перешёл в традиционное русло. Однако ресурсы по поддержке дистанционного образования содержались в актуальном состоянии. Последнее обновление было сделано накануне Рождества, и свежая информация пришлась кстати преподавателям, которые с началом нового года и очередной волны карантина вернулись с каникул на платформы дистанционного образования.

Многие учебные заведения ещё весной смогли использовать единую интерактивную платформу — Microsoft Teams или Google Classroom — для обеспечения удалённого обучения. На базе этих и аналогичных платформ можно создавать виртуальные классы, используя информацию из школьных информационных систем управления, обеспечивать единую точку доступа для всех уроков и ресурсов. Учителя проводят живые занятия и размещают записанные уроки.

Сегодня школы могут подать заявку на государственную поддержку через ресурс The Key for School Leaders и получить доступ к одной из двух бесплатных платформ цифрового образования: G Suite for Education от Google или Office 365 Education разработки компании Microsoft. Чтобы помочь сделать наиболее подходящий выбор для школы, The Key также предлагает сравнение функций и тематические исследования о том, как школы максимально используют эти платформы.

Платформы можно усовершенствовать с помощью приложений, которые

позволяют легко записывать видео уроков. Одно из приложений для записи видео — Loom — многие учителя считают простым в использовании, его можно легко связать с Microsoft Teams.

Помимо уроков, важной частью эффективного обучения являются тесты и викторины. При онлайн-обучении учителя могут задавать вопросы конкретным ученикам, а школьники — задавать вопросы учителям или друг другу с помощью функции «Чат», которая реализована в различных платформах. Формы Google, Kahoot, Classkick, Socrative, Edpuzzle — это лишь несколько примеров приложений, которые хорошо работают для быстрой обратной связи и позволяют выставлять оценки в реальном времени.

Школы могут использовать образовательные платформы для реализации большей части обычной учебной программы. Записанные уроки, электронные и печатные пособия удобно использовать дома в качестве дополнения и подготовки домашних заданий или в условиях, когда на несколько

детей дома приходится один компьютер и необходим доступ к записанным урокам. Это позволяет ученикам учиться в любое время, а опросы, обратная связь и иные формы обмена информацией о школьной работе в интерактивном или автономном режиме помогают оставаться в социуме. Платформы могут упростить учителям мониторинг успеваемости учеников, поскольку работы легко просматривать или отправлять через единую систему.

Дополнительные ресурсы, включающие качественные бесплатные и платные онлайн-сервисы, также могут быть встроены в популярные платформы. Например, ресурс Департамента образования Isaac Physics предоставляет бесплатные онлайн-ресурсы для обучения физике. Практические и лабораторные работы, которые проводятся в классе, в дистанционном варианте могут быть заменены роликами из YouTube.

Важный аспект школьной жизни — личное общение. Не только на уровне ученик — учитель, но и между педагогами. Образовательные платформы позволяют проводить собрания всего персонала школы, занятия по повышению квалификации, родительские собрания в классе или общешкольные собрания. Также рекомендованы групповые семинары, брифинги с использованием как упомянутых выше платформ, так и Zoom.

Главной целью дистанционного образования, помимо передачи знаний, является сохранение интереса к учёбе и поддержка мотивации учеников. Для этого школы должны контролировать участие учеников в дистанционном обучении, регистрировать уровень участия и мотивации, а также собирать отзывы родителей через регулярные отчёты. Для повышения мотивации школам предлагают выпускать еженедельный информационный бюллетень, в котором собраны примеры отличной работы, начислять баллы и награды за отличное взаимодействие или результаты.

ПОМОЩЬ МАЛОИМУЩИМ

Что делать с теми учениками, у кого нет интернета? Здесь в первую очередь на помощь пришли учебники, бумажные издания и простые телефонные звонки. Да, в Великобритании телефон

по-прежнему остаётся важным инструментом для контроля учеников, информирования родителей и осуществления образовательного процесса.

Также для поддержки качественного дистанционного образования с начала пандемии правительство Великобритании выделило школам и муниципальным образованиям более 560 тыс. устройств. С приходом новой волны карантина для учеников в первую неделю нового семестра выделено ещё более 100 тыс. компьютеров и гаджетов. Всего для помощи малоимущим учащимся запланировано выделить более 1 млн устройств и предоставить ученикам доступ в интернет, так как многим семьям пришлось из последних сил оплачивать счета за подключение во время первой волны. Почти четверть домохозяйств исключены из цифрового мира и не имеют доступа в интернет из дома. Согласно данным Ofcom 2020 Technology Tracker, 9 % домохозяйств получают доступ в интернет только через мобильную сеть с телефона, почти 40 % семей не имеют дома доступа к настольному компьютеру, ноутбуку или планшету.

Распространение такого количества ноутбуков и планшетов в школах стало возможным благодаря сотрудничеству государственных структур с различными организациями. Предоставление более 1 млн устройств учащимся делает образовательную программу Великобритании в своём роде одной из крупнейших в мире.

БЕЗОПАСНОСТЬ ПРЕЖДЕ ВСЕГО

Безопасность учеников и учителей во время уроков — важный элемент любого обучения и дистанционного в том числе. С одной стороны, учителя должны применять те же принципы, которые приняты при очном обучении, с другой — возникают специфические моменты, актуальные только для дистанционного онлайн-образования.

В первую очередь речь идёт о психологической защите детей: кто будет вести уроки, на каких ресурсах будут идти занятия, какие меры стоит принять для защиты ребёнка от нежелательного контента. Что должен знать малыш 4 лет, у которого начались первые уроки в глобальной сети, и как

поговорить с подростком 14 лет, который столкнулся с виртуальным сексуальным насилием во время онлайн-занятий или при общении в социальных сетях? Сайт Министерства образования содержит собственные рекомендации и ссылки на другие ресурсы для родителей и опекунов детей разных возрастов, советы, как поговорить с ребёнком об опасностях, поддельных личностях, личной информации, которой не стоит делиться с новыми виртуальными друзьями, о сайтах радикальных течений, чьи сторонники вербуют в сети свежие кадры, кибербуллинге и т.д. В случае любой угрозы личности детям советуют обратиться к взрослым, а тем рекомендовано обращаться в полицию, школу и Национальное криминалистическое агентство или звонить на горячую линию онлайн-безопасности в интернете.

Кроме защиты детей от моральных травм и влияния радикальных и деструктивных течений, даны советы и по традиционной информационной безопасности: от настроек образовательных платформ до установки антивирусов и родительского контроля на устройствах, с которых ребёнок выходит в интернет, настройке безопасности и конфиденциальности, фильтров для блокировки вредоносных веб-сайтов.

ОБЩАЯ СИТУАЦИЯ

По данным на начало января, школы в Великобритании будут работать в дистанционном режиме по ситуации, как минимум до третьей декады января (Уэльс), начала февраля (Шотландия, Ирландия) или середины февраля (Англия). Детские сады и школы смогут посещать дети, чьи родители работают в стратегических отраслях. А малоимущие семьи, имеющие право на бесплатное школьное питание, получают дополнительную поддержку правительства. С учётом развития ситуации дополнительно будет обсуждаться порядок сдачи летних экзаменов, так как традиционный подход в условиях онлайн-обучения будет несправедлив, считают в правительстве Великобритании.

Будут учиться дома и студенты колледжей и университетов, исключение сделано только для медицинских направлений.



Дмитрий ЛАРИН
кандидат технических наук,
АО «Лаборатория СКАТ»

СЕВЕР ПРОТИВ ЮГА

КРИПТОГРАФИЧЕСКАЯ ДЕЯТЕЛЬНОСТЬ В ПЕРИОД ВОЙНЫ В КОРЕЕ

70 лет назад, в июне 1950 года, началась война в Корее. К тому моменту ещё не отслужила свой срок техника времён Второй мировой, но стало массово применяться и новое вооружение. Например, именно тогда состоялся первый в истории воздушный бой между реактивными самолётами, закончившийся победой советских лётчиков. Американцы впервые массово использовали для

транспортировки личного состава и снабжения своих частей новый вид транспорта — вертолёты. Разумеется, противоборствующие стороны активно совершенствовали шифровальное дело, радиоразведку и криптоанализ.

РАССТАНОВКА СИЛ

В 1945 году Корейский полуостров был разделён надвое. Территорию севернее 38-й параллели заняли советские

войска, и вскоре там была образована Корейская Народно-Демократическая Республика (КНДР), а южнее разместились американцы, что, в свою очередь, привело к образованию Южной Кореи.

Начало войне положил руководитель КНДР Ким Ир Сен. 25 июня 1950 года северяне атаковали южан и быстро их разгромили. Но в войну вмешались США, и северокорейская армия была вынуждена отступить.



Hulton Archive/Archive Photos/Getty Images

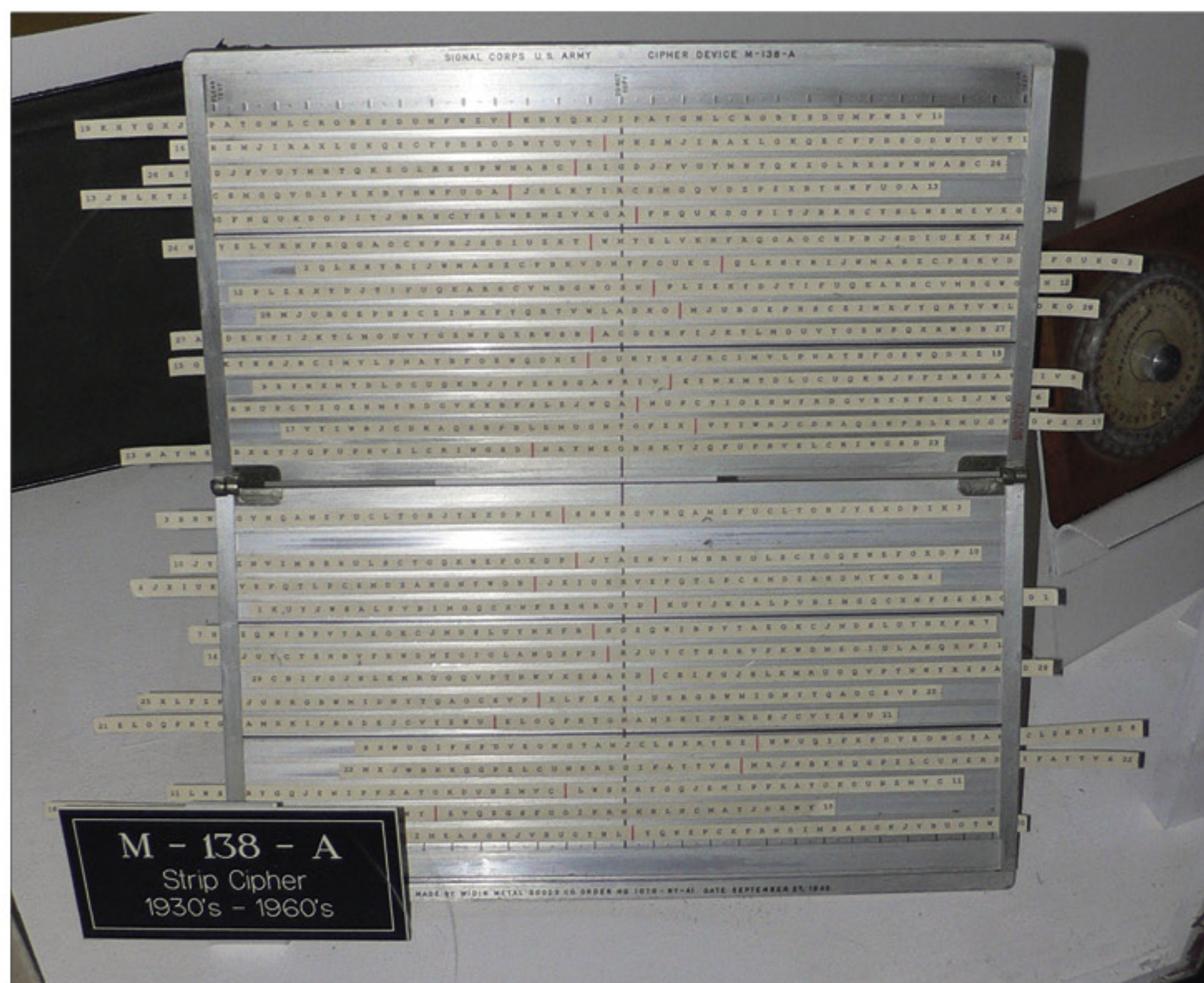
СССР направил в помощь КНДР 64-й истребительный авиакорпус (ИАК) в составе двух авиадивизий, подразделений зенитной артиллерии, прожекторных частей, радиолокационных станций, радиотехнических подразделений и т.д. Общее число советских военнослужащих, участвовавших в боевых действиях, составило примерно 26 000 человек. Кроме того, на стороне КНДР воевали подразделения китайской армии (так называемые китайские народные добровольцы) численностью более миллиона человек.

Коалиция южан включала 17 государств. Большую часть «войск ООН» представляли вооружённые силы США, а также подразделения из Австралии, Бельгии, Великобритании, Греции, Канады, Колумбии, Люксембурга, Нидерландов, Новой Зеландии, Таиланда, Турции, Филиппин, Франции, Южной Африки, Эфиопии.

СО СТОРОНЫ США

Американцы подошли к Корейской войне, имея большой опыт в области криптоанализа и радиоразведки. Напомним, что именно США стали

пионерами в области перехвата и дешифрования телеграфных сообщений во время гражданской войны 1861–1865 гг. Триумфом американских криптографов стала операция «Магия» — успешный криптоанализ японских шифров во время Второй мировой. Тогда американцы получили массу ценной информации, приблизившей победу союзников на Тихом океане. В 1949 году криптографические службы в армии, флоте и ВВС были объединены в Агентство безопасности связи ВС США (AFSA). В этой организации сосредоточилась вся криптографическая деятельность страны.



Полосковый шифратор M-138

Тем не менее нападение КНДР на Южную Корею стало неожиданностью. Одно из первых, если не первое перехваченное американцами сообщение, имеющее отношение к войне, датируется 27 июня, но оно не было переведено вплоть до октября. В этой радиограмме речь шла о передвижениях ряда северокорейских дивизий.

В июне 1950 года, до начала войны, американские военные имели всего двух специалистов, работавших на северокорейском направлении (криптоаналитика и переводчика). Однако к ноябрю их было уже 36 человек. В начале 1951 года число специалистов, работавших на корейском направлении, возросло до 49, а в марте 1953 года — до 87. В связи с активным участием в боевых действиях китайцев число специалистов AFSA также неуклонно возрастало. Если до начала войны в штате было 83 переводчика с китайского, то к ноябрю их число выросло до 131, а в феврале 1951 года — до 156.

Американцы и их союзники использовали различные средства шифрования. На низшем уровне управления войсками применялись ручные шифры, главным образом шифрблокноты с гаммой и кодовые таблицы. Также

применялись простейшие механические шифраторы — дисковые (M-94) и полосковые (M-138 и др.).

В звене батальон — дивизия основным средством был шифратор M-209 конструкции знаменитого шведского криптографа Б. Хагелина, выпускавшийся в США по лицензии. Массово применялся и английский шифратор Турех, основой для которого послужила немецкая «Энигма», и ограниченное применение нашли американские шифраторы, разработанные в период Второй мировой войны.

Первый американский криптоаналитик из AFSA, лейтенант Дэвид Мюррей, прибыл на полуостров 19 июля 1950 года. Для организации радиоперехвата он стал использовать оборудование частей американских ВВС, дислоцировавшихся в районе Токио. Таким образом обеспечивалась дешифровальная поддержка действовавшей над Кореей 5-й воздушной армии ВВС США (5 ВА).

Однако работы по перехвату и криптоанализу начались гораздо раньше благодаря Дональду Николсу, который жил в Сеуле, числился как майор вооружённых сил США и возглавлял небольшой нештатный разведотдел,



Дисковый шифратор M-94

работавший в интересах 5 ВА. По собственной инициативе он привлёк к работе двух корейцев — радиооператора и криптоаналитика. В начале войны северокорейские шифрсистемы были довольно слабыми и легко подвергались дешифрованию даже такой небольшой командой. К 14 июля большинство шифрсистем Северной Кореи было вскрыто, после чего группа Николса читала более 90% северокорейского трафика. Однако 31 июля было замечено, что стойкость северокорейских шифров значительно возросла.

Хотя работа по перехвату и криптоанализу северокорейских сообщений была организована, это не означало, что проблем не было. Среди всего трафика (львиную долю которого занимали советские и китайские радиогаммы) необходимо было найти корейские. Ещё одна проблема — не хватало линий связи. При этом специалисты AFSA были у связистов далеко не в приоритете.

Но всё же если ВВС и армия США сумели организовать радиоразведку на корейском ТВД, то ВМС не сумели. Уже готовое к командировке в Корею подразделение было отозвано из-за отсутствия необходимой техники.

КОНТРНАСТУПЛЕНИЕ

15 сентября началось контрнаступление южан. Командующий войсками ООН генерал Дуглас Макартур



Стратегические бомбардировщики В-29 — «Суперкрепости». Фото: Getty Images

проигнорировал ультиматум КНР о вступлении китайцев в войну при пересечении американцами и их союзниками 38-й параллели. Несмотря на доклады AFSA о скоплении китайских войск у границы, он до последнего не верил, что Китай сдержит обещание. 25 октября китайская армия перешла в наступление, и восьмая армия США поспешно отступила.

Главной задачей американских специалистов было заблаговременно предупреждать о наступательных действиях КНДР. А основной проблемой — нехватка переводчиков.

Вскоре появилась новая проблема — советские истребители, и понадобились переводчики с русского. Большое количество радиопереговоров советских пилотов было обусловлено тактикой. Воздушным боем управляли с земли, основываясь на данных РЛС (бортовых радаров ещё не было).

Для перехвата переговоров наших пилотов была установлена специальная станция, на которой работали восемь переводчиков с русского языка.

В октябре 1951 г. американская радиоразведка доложила о появлении в Северной Корее истребителей МиГ-15. 13 октября 307-я группа ВВС США (стратегические бомбардировщики В-29 — «Суперкрепости») нанесла удар по северокорейским аэродромам. Провал налёта признали даже американцы: из 278 сброшенных бомб в ВПП

попали только 24, корейцы быстро восстановили повреждения.

ПЕРСОНАЛИЗАЦИЯ

Американские радиоразведчики получили задачу обеспечивать действия стратегических бомбардировщиков В-29. Выдвинутые на передовую посты радиоразведки перехватывали и анализировали переговоры советских пилотов, что позволяло предупреждать экипажи В-29 об опасности и давало им возможность спастись бегством. Несмотря на некоторые успехи американцев, МиГи продолжали сбивать «Суперкрепости». При этом радиоперехват позволял персонализировать «обидчиков». Так, 3 июля над городом Синьчжу был сбит В-29, командир экипажа которого Норман Э. Эндерсон имел на счету 64 боевых вылета. По данным радиоперехвата американцев, его сбил лучший ночной ас корейского неба майор А. М. Карелин.

Понесла большие потери от советских истребителей и зенитной артиллерии КНДР, американцы стали использовать аппаратуру по постановке помех РЛС ПВО КНДР.

ВОСПОМИНАНИЯ КРАМЕРА

Весьма информативными оказались воспоминания командира 7-й роты связи Артура Крамера. Он писал, что шифровальщики его подразделения работали с большим напряжением, но



Советский ас А. М. Карелин

отлично справлялись со своими задачами. Вместе с тем он отметил серьёзные недостатки в организации шифровальной службы. Например, сообщения с высокой степенью секретности, на шифрование которых тратились большие усилия, параллельно передавались открытым текстом. Отмечал Крамер и небрежное хранение расшифрованных документов: «Я видел так много нарушений сохранности и сделал столько докладов, что в конце концов просто перестал обращать на это внимание».

Другой проблемой была неправильная расстановка приоритетов: многие сообщения с пометкой «срочно» на деле оказывались, например, пятидневной давности. Также в некоторых штабах не хватало квалифицированных шифровальщиков. Крамер вспоминает, что в одном из подразделений просто не могли вскрыть сообщение, закодированное в другом.

КАК ПОЯВИЛОСЬ АНБ

В годы Корейской войны американскими криптографическими службами была проделана колоссальная работа, однако американские историки, военные и политики оценили её как недостаточную. Но выводы американцы сделали. Главным криптографическим итогом этой войны стало создание в США единой криптографической службы — Агентства национальной безопасности (АНБ), одной из мощнейших криптослужб в мире. АНБ было создано директивой президента США 4 ноября 1952 года и сразу включилось в работу, но из-за организационных проблем



Советская радиостанция РБМ

с образованием новой спецслужбы до конца боевых действий основную нагрузку по-прежнему несли криптографы вооружённых сил США.

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА

Как уже отмечалось, в начале войны северокорейские шифрсистемы были слабыми и легко подвергались дешифрованию. Много трудностей в частях Корейской народной армии (КНА) было и с организацией связи. Подразделения связи были малочисленными и слабо подготовленными. Основным средством связи в дивизии и полку была радиосвязь. Использовались советские радиостанции РБМ, А7А и 13-Р.

Главной задачей советских подразделений связи и радиоразведки была организация связи истребителей авиакорпуса 64 ИАК с пунктами управления и между собой. Основными средствами были упомянутые выше советские радиостанции, а также техника, поставленная во время Второй мировой войны из США по программе ленд-лиза, которую использовали специально,

чтобы скрыть советское участие в боевых действиях.

Вот что вспоминает об организации связи в 64 ИАК командовавший им тогда генерал-майор Г. Лобов: «Мы располагали радиолокационной сетью обнаружения и наведения на цели, включавшей локаторы и радиостанции нескольких типов, шестиканальной УКВ-связью между самолётами и КП, артиллерийскими радиолокационными станциями кругового обзора и орудийной наводки (*речь о зенитной артиллерии — прим. автора*), а также радиоприёмниками с кварцевыми устройствами, позволявшими прослушивать радиопереговоры экипажей противника. Аэродромы были оборудованы радиосветотехническими системами, обеспечивавшими выполнение полётов в сложных метеорологических условиях и ночью, а также пеленгаторами».

Что касается криптографической защиты, Лобов отмечает: «Мы предполагали, что американцы прослушивают нашу радиосеть (точных сведений об этом не было), и передавали наиболее важные команды условным языком.

Коды часто менялись, поэтому на приборные доски МиГ-15 наклеивались таблички раскодирования приказов и запросов. Применялись и дезориентирующие сведения».

Телефонные шифраторы того времени и у нас, и на Западе были громоздкими и не могли быть поставлены на самолёт, поэтому и мы и американцы для управления истребительной авиацией использовали шифрование с помощью кодовых таблиц. К сожалению, в начале войны дошло до абсурда. Чтобы скрыть присутствие советских пилотов в небе Кореи, им предписывалось разговаривать на корейском языке.

Из воспоминаний командира 523-го авиаполка А. Сморгкова: «Эта строжайшая секретность и смешила, и изводила. По-корейски или по-китайски мы были ни бум-бум, а в бою предписывалось выходить на связь на корейском языке. К правому колену крепили планшеты со словарём — корейские слова в транскрипции. Вот и представляйте, как в бою на реактивных скоростях нужно умудриться скосить глаз на колено, отыскать нужное слово или фразу... Матерились. Лётчики не вытерпели,

и эту нелепицу всё-таки отменили. В Москве не стали спорить, дали добро».

После этого в корейском небе стала звучать русская кодированная речь, например: «Веду бой в районе «сосиски»» (небольшой полуостров в районе Анджу). «Всем «Трава!» — приказ всем самолётам идти на посадку. «Замок!» — сброс подвесных баков перед боем. «С «крестами» не связываться!» («кресты» — истребители F-84, сопровождавшие «суперкрепости»), главное — бомбардировщики» и т.д.

Иногда применялось радиомолчание. Из воспоминаний ещё одного аса Корейской войны П. Милаушкина: «В мае 1951 года... Приказ — радиосвязь не включать, действовать молча. Взлёт — по телефону, или в случае чего — ракета». И только в воздухе лётчикам разрешали пользоваться радиостанциями. Этот эпизод относится к разгрому 77-й эскадрильи ВВС Австралии, действовавших на английских истребителях «Метеор». Тогда из 16 «Метеоров» были сбиты 12 — без потерь с нашей стороны.

Что касается организации связи между наземными частями советского контингента, то здесь использовалась как проводная, так и радиосвязь. Для защиты информации применялись ручные шифры и коды, часто с перешифровкой — гаммированием. Обычно применялись ручные криптосистемы, хорошо зарекомендовавшие себя в ВОВ.

ХОРОШАЯ КОМПАНИЯ

Переход главного противника — бомбардировщиков B-29 — на ночные действия ещё более усилил роль радиоперехвата. Хотя поначалу были проблемы. Дело в том, что до лета 1952 года ночными истребителями у нас были поршневые самолёты Ла-11, которые не могли догнать «суперкрепости» даже днём. Поэтому было принято радикальное решение перевооружить авиаполк на реактивные МиГ-15.

Несмотря на отсутствие ночных радиолокационных прицелов, советские лётчики во взаимодействии с радиоперехватчиками, операторами РЛС, прожектористами и зенитчиками начали активно сбивать «суперкрепости» и по ночам. Радиоразведка отслеживала время вылета американцев и их цели,

дальше в дело вступали лоаторщики, а потом и прожектористы, обеспечивавшие истребителям комфортные условия для атаки.

Большую помощь радиоразведке оказывали и сами американцы, используя систему радиолокационного наведения SHORAN. В ночных условиях она позволяла точно отбомбиться по цели. Но наши специалисты научились перехватывать сигналы этих станций и определять место, а часто и время ударов бомбардировщиков. Соответственно, наши истребители оказывались в нужном месте в нужное время.

Вообще, наши специалисты использовали любую возможность исследовать вражеские системы связи. Так, в одном из воздушных боёв удалось заставить сесть F-86 «Сейбр» на северокорейской территории. Его, конечно, внимательно изучили. Наиболее ценным оказался оптико-радиолокационный прицел, обеспечивающий самолёту возможность успешно действовать как днём, так и ночью. Вскоре специалисты группы Лисиченко, оснащённые станциями радиотехнической разведки «Пирамида», стали уверенно засекать серии импульсов этих самых оптико-радиолокационных прицелов.

РАДИОИГРЫ ПОД ШИФРОМ

Обе стороны активно занимались зафронтной деятельностью, забрасывая в тыл противника свою агентуру. Связь с такими группами обычно поддерживалась по радио. Имеющие немалый опыт советские специалисты предложили северным корейцам провести с южанами «радиоигры под шифром». На юг пошла серьёзная дезинформация.

Одна из успешных операций прошла в начале 1952 г. Северные корейцы захватили разведывательно-диверсионную группу, десантированную в район Пхеньяна. Любопытная деталь: сообщение о благополучном приземлении разведчики отправили не по радио, а с почтовым голубем. Группу перевербовали, и те под диктовку начали передавать в свой Центр шифрованную «информацию».

Была придумана легенда, что установлен контакт с якобы действующим партизанским отрядом, боровшимся

против Северокорейского режима. На юге эти сведения встретили с интересом, но и с недоверием. Предлагали сообщить подробные сведения о партизанах: биографию каждого из них, места дислокации и т.д. Дважды сбрасывались с парашютом фотоаппараты с запасом плёнки и давалось указание сфотографировать каждого бойца и передать снимки на юг. Одновременно «партизанам» перебрасывали по воздуху продукты питания, топографические карты, снаряжение.

Для усиления заинтересованности в американский разведцентр сообщили, что к «партизанам» попали несколько лётчиков со сбитого бомбардировщика B-29 (факт имел место, лётчиков взяли в плен). Приманка сработала. В помощь к южнокорейским агентам была направлена оперативная группа из четырёх человек во главе с представителем разведшколы южнокорейских спецслужб. Его удалось перевербовать, и он передал по радио подтверждение о «партизанах», американских лётчиках, а также информацию, в которой была заинтересована КНДР.

Завершилась игра после десантирования с юга один за другим двух вооружённых отрядов в количестве пятидесяти человек. Все они были обезврежены.

ВМЕСТО ЭПИЛОГА

Корейская война стала первым вооружённым конфликтом времён холодной войны, и её нередко рассматривают как опосредованное широкомасштабное вооружённое столкновение между США и их союзниками с одной стороны, и СССР, а также КНР — с другой. Характерная особенность этой войны в том, что за плечами основных противоборствующих сторон была Вторая мировая. Однако Корея стала не только «полигоном» для шлифовки горьких, но вместе с тем и ценных уроков совсем близкой Большой войны. Завершившись вничью, Корейская война сопровождалась чередованием успехов и провалов всех противоборствующих сторон и бросила новые вызовы, в том числе в области криптоанализа и радиоразведки. Поиск ответов на эти вызовы активно шёл в последующие годы и во многом сформировал наш сегодняшний мир.



Борис СТОЛПАКОВ
историк криптографии,
кандидат физико-математических наук

ПЕРЕД ЗАКАТОМ ИМПЕРИИ

РОССИЙСКИЕ КРИПТОГРАФЫ В НАЧАЛЕ XX ВЕКА

В преддверии столетнего юбилея Криптографической службы Российской Федерации уместно обратиться взором к событиям вековой давности. История распорядилась так, что начало прошлого века оказалось временем подведения итогов криптографической деятельности в Российской империи.

В первые годы XX столетия российские криптографы были сосредоточены главным образом в МИД: в двух отделениях, именовавшихся экспедициями, при канцелярии министерства. Первая экспедиция занималась разработкой собственных шифров,

вторая — дешифрованием перехваченной, в основном телеграфной, иностранной переписки. Координировать их деятельность был призван Цифирный комитет, административно-финансовый орган, составленный из ведущих специалистов, а также руководителей министерства. Постепенно росли шифровальные службы Военного министерства, МВД и других ведомств, созданные ещё в XIX столетии.

СЛОВАРИ И КОДЫ

Первой экспедицией до лета 1917 г. руководил К. Ф. фон Таубе. Руководителей второй экспедиции было

двое: В. В. Сабанин (до мая 1907 г.) и А. А. Долматов (2 июня 1907 г. — 1917 г.).

Конец XIX — начало XX века — это время широкого использования кодов. Объём некоторых из них уже достигал 10 000 словарных величин. Т. А. Соболева отметила, что к 1917 г. наибольшее распространение имели коды именно такого объёма. Составление кодов потребовало весьма глубокого и кропотливого труда российских криптографов. Прежде всего, необходимо было выделить для помещения в словари кодов слова и словосочетания, отражающие специфику переписки. Понятно, что словари

Иллюстрация 1. Телеграмма императора Николая II П. А. Столыпину (РГИА)

военных кодов должны отличаться от словарей кодов дипломатических или кодов, используемых в финансовом ведомстве. Значительная часть словарных величин в кодах отводилась под специальные термины, включая календарь, имена собственные и географические наименования. При этом криптографы стремились достичь относительного выравнивания частот в шифртекстах искусным выбором кодовых обозначений.

ПЕРЕШИФРОВАНИЕ СТАЛО ПОЧТИ ОБЯЗАТЕЛЬНЫМ

С конца XIX века повсеместно начинают использоваться коды с перешифровкой. Для одних кодов перешифрование было обязательным, для других — лишь

в случаях передачи особо секретных сообщений.

Содержание кодовых и перешифровальных инструкций свидетельствует о глубокой проработке криптографических методов анализа предлагаемых шифров. С их учётом создавались средства, имевшие целью сделать неэффективными возможные подходы к дешифрованию. Например, в «Руководстве» к «Передвижному условно-словарному ключу № 437» 1910 г. сказано, что он «предназначен для шифрования приведённых в секретных сообщениях выражений общего характера и ссылок, независимо от набора любым секретным ключом (или сочетанием ключей) открытого текста шифруемого сообщения».



Иллюстрация 2. Один из шифров императора Николая II

ВОЕННЫЕ И ПРОЧИЕ КОДЫ

Уже с конца 40-х гг. XIX века в Главном штабе Военного министерства налаживается работа собственной шифровальной экспедиции. Создававшиеся здесь шифры утверждались военным министром. Экземплярами военных шифров снабжали и императора.

Большинство шифров военного министерства в начале XX столетия представляли собой коды малого (до 1000 словарных величин) объёма. Кодовыми обозначениями являлись трёх- и четырёхзначные числа. В шифрах были предусмотрены маскировка (перестановка двух цифр в пятиграммах шифртекста) либо перешифрование кода.

Шифры Департамента полиции, жандармерии, гражданских ведомств существенно уступали шифрам МИД и Военного министерства по своим криптографическим качествам. Так, типичный шифр жандармерии — это цифровой код на 100 величин, одно- и двузначный.

ИМПЕРАТОРСКИЕ КОДЫ

Специальные шифры императора Николая II — это коды объёмом до 10000 словарных величин. Один из них, шифр 1911 г., был оформлен как небольшая книжечка, размером 14,5x21 см. На обложке золотом вытиснен герб России — двуглавый орёл — и надпись золотыми буквами: «Ключ Военного министерства. Лит. М». Ещё один императорский код представлен на илл. 2.

ДЕШИФРОВАЛЬНАЯ СТАТИСТИКА

Обратимся теперь ко второй, дешифровальной экспедиции МИД. В основном зашифрованные депеши поступали туда в виде телеграмм. Показатели дешифровального отделения по работе с телеграммами за 1893–1902 гг. приведены в табл. 1. Также для сравнения указаны данные за предыдущее десятилетие.

Заметим, что здесь среднее число разобранных телеграмм лишь условно характеризует успех деятельности отдельных дешифровальщиков за более короткий срок. К примеру, по данным В. С. Измозика, за 1899–1902 гг. В. В. Сабанин расшифровал 3175 телеграмм, Е. К. Напьерский — 2164, Е. Ф. Маттей — 1594, Э. К. Феттерлейн — 1195, К. В. Циглер — 784, А. А. Долматов — 391 телеграмму.

СОЦИАЛЬНЫЙ ПОРТРЕТ КРИПТОГРАФА

Послужные списки позволяют уточнить социальный портрет криптографа МИД: это, как правило, выпускник университета по юридической либо по языковой специальности. Так, один из самых успешных дешифровальщиков Э. К. Феттерлейн перед началом своей службы окончил факультет восточных языков Императорского Санкт-Петербургского университета как арабист. Несомненна связь между подбором лингвистически образованных кадров для криптографической службы и всё более широким и глубоким внедрением кодов в шифровальную практику конца XIX — начала XX столетий. Тогда считалось, что для успешных занятий с шифрами требуются знание иностранных языков, общекультурный кругозор и способности к логическому

рассуждению. И такой взгляд был вполне справедлив. Ещё продолжался, как известно, хотя и близился к концу, домашний период криптографии. А потому математика, физика, информатика в ней пока ярко себя не проявляли. Тем не менее в начале XX столетия работа дешифровальщиков заметно усложнилась.

«ШИФРЫ СТАНОВЯТСЯ БОЛЕЕ СЛОЖНЫМИ И ОБЪЁМИСТЫМИ»

В отчёте за 1909–1910 гг. А. А. Долматов указывал, что «за последние годы иностранные правительства... уделяют всё большее внимание своим дипломатическим шифрам, которые становятся более сложными и объёмистыми и значительно чаще заменяются новыми. Английский посол, который раньше сообщал тексты полученных им телеграмм дословно, теперь передаёт их нашему министерству в совершенно изменённой редакции. Французский посол недавно телеграфировал в Париж, прося не пользоваться больше одним из ключей, потому что в нём уже второй раз передаётся текст, известный русскому правительству. Германское правительство, ранее менявшее ключи только один раз в год, совершенно неожиданно ввело ещё один новый ключ. Японское правительство заменило свои маленькие ключи чрезвычайно объёмистыми и, следовательно, весьма трудными для разбора новыми кодами на японском языке. Новые ключи введены и австрийским, греческим, сербским и другими правительствами».

Постепенно сложилась некоторая специализация чиновников отделения. Например, А. А. Долматов занимался шифрами Бельгии и Испании;

Е. Ф. Маттей — Франции и Японии; Е. К. Напьерский — Германии, Италии и Турции; К. В. Циглер — Баварии, Франции, Греции; Э. К. Феттерлейн — Баварии, Болгарии, Дании, Франции, Персии и Турции, а в конце 1904 г. он наконец «нашёл теорию австрийских ключей».

«НАХОЖУ НЕОБХОДИМЫМ ПРИБРЕТАТЬ... КОПИИ ТЕЛЕГРАММ»

Российские посольства, активно добывавшие через свои источники важную дипломатическую переписку, пересылали её во вторую экспедицию для расшифровки. Так, российский посол в Турции И. А. Зиновьев писал в ноябре 1901 г. министру В. Н. Ламздорфу: «Нахожу необходимым приобретать по временам копии как с отправляемых [германским] посольством... в Берлин, так и с получаемых оттуда... телеграмм». К письму были приложены две серии телеграмм. Вскоре от Зиновьева поступили две новые серии.

«ОТСУТСТВИЕ ЭТОГО МАТЕРИАЛА ЗНАЧИТЕЛЬНО ЗАТРУДНИЛО РАЗБОР КЛЮЧЕЙ»

Шифрованные телеграммы, как правило, поступали с телеграфа. Очень кстати оказалось прохождение через территорию России международных линий связи Европы с Южной Азией и Дальним Востоком. В этом отношении показательна записка Сабанина директору канцелярии МИД Савинскому от 10 мая 1905 г.: «Доставка английских телеграмм из Тегерана крайне желательна. Мы прежде ежедневно получали их через Одессу и имели таким образом всю переписку между Лондоном и Тегераном. Телеграммы эти имели для нас большое значение... и по своей технике, так как Лондон употреблял для Тегерана те же ключи, как и для Петербурга... С 1903 года эти телеграммы больше не доставляются».

В январе 1906 года последовал новый рапорт Сабанина по аналогичному поводу: «С 5/18 мая 1905 г. прекратилась доставка телеграфной переписки между великобританским послом в Константинополе и Лондонским

	1893–1902 гг.	1883–1892 гг.
Количество входящих телеграмм	65 450	39 524
Количество разобранных телеграмм	23 643	12 431
Процент разобранных телеграмм	36	31
Среднее число служащих	5,7	4
Среднее число разобранных телеграмм на одного служащего	4146	3107

Таблица 1. Показатели дешифровального отделения МИД

кабинетом... Отсутствие этого материала значительно затруднило разбор английских ключей... Ранее уже утратили доставлявшуюся из Одессы телеграфную переписку между английской миссией в Тегеране и лондонским кабинетом, между индийским вице-королём и статс-секретарём по делам Индии». Руководство МИД вновь обратилось в Главное управление почт и телеграфов с просьбой о присылке копий телеграфных сообщений, проходящих через Одессу.

Эти просьбы и труды криптографов оказались не напрасными. Судя по донесениям А.А. Долматова, к 1908 году удалось справиться с английским шифром для дипломатической переписки Лондона с Константинополем и Тегераном. Заслуга в этом принадлежала прежде всего К.В. Циглеру. В течение 1908 года было расшифровано 180 телеграмм, включавших переписку британского руководства с послами в Турции и Персии.

С ЯПОНСКИМИ ТЕЛЕГРАММАМИ БЫЛО СЛОЖНЕЕ

Та же самая проблема — необходимость большого количества телеграмм для расшифровки, только уже относительно турецкого и японского шифров, обсуждалась в 1911 г. Русский посол в Турции Н.В. Чарыков сообщил товарищу министра А.А. Нератову о возможности получения в Стамбуле подлинных зашифрованных телеграмм военного министра и великого визиря. К донесению он приложил четыре телеграммы на турецком языке, прося в случае расшифровки сообщить об их содержании, «чтобы судить о политическом значении нового источника». Через несколько дней от него поступило ещё пять телеграмм.

С японскими телеграммами дело обстояло сложнее. Ситуация усугубилась большим количеством ошибок в копиях зашифрованных телеграмм, присланных из отделений связи. Причём часть важных телеграмм была пропущена без копирования и, таким образом, потеряна для дешифрования. По этой причине из МИД было направлено отношение начальнику Управления городских телеграфов в Санкт-Петербурге.

В целом же, судя по отчёту Долматова за 1912 год, на вскрытие иностранных дипломатических шифров требовалось примерно от полугода до двух с половиной лет.

«НЕ СЛИШКОМ ЛИ ВЕЛИКО ВОЗНАГРАЖДЕНИЕ?»

В начале XX столетия дешифровальные подразделения имелись уже не только в МИД, но и в Военном и Морском ведомствах, а также в МВД.

Ещё в 1860-е гг., когда значительно увеличилась переписка с заграницей и в «чёрных кабинетах» при перлюстрации стали обнаруживать зашифрованные письма, III Отделение императорской Канцелярии обратилось за помощью в МИД. Тогда к сотрудничеству привлекли Л.П. Иессена, руководителя дешифровальной службы министерства. С 1869 г. по май 1872 г. он разобрал четырнадцать шифров, за что получил 2500 руб. наградных. В 1874–1878 гг. — ещё 2300 руб. В частности, он разобрал две записки, найденные при аресте у П.А. Кропоткина в 1874 г. За расшифровку этих записок Иессен получил 800 руб., хотя начальник III Отделения и шеф жандармов П.А. Шувалов первоначально запрашивал своих подчинённых, не слишком ли велико будет вознаграждение за разбор двух кратких записок.

КОЛИЧЕСТВО ЗАШИФРОВАННЫХ ПИСЕМ СТАЛО ОГРОМНЫМ

После создания в 1880 г. в МВД Департамента государственной полиции (ДП) и его дешифровальной службы письма с шифрами из «чёрных кабинетов» стали направлять собственным специалистам-криптографам. В начале XX века наибольшей известностью в качестве такого специалиста пользовался Иван Александрович Зыбин.

Самой дешифровальной работой тогда занимались всего двое — И.А. Зыбин и его ученик С.И. Жабчинский, выпускник Санкт-Петербургского университета. Между тем объём работы стремительно возрастал. Если в конце XIX века «чёрные кабинеты» по всей России перехватывали по 150–200 конспиративных писем в год, то начиная с 1901 г. их число выросло до

2,5 тысяч. А к 1910 г. ежегодный перехват достиг 4–5 тысяч (по данным А.В. Синельникова). Столько попадало в полицию писем, где зашифрованный текст был скрыт химическим путём. Уже в 1903 г. Зыбин писал директору ДП Лопухину, что разрабатывать зашифрованные письма с каждым годом становится всё труднее. Их количество стало огромным, но главное, сравнительно лёгкие приёмы шифрования текста уже редки и «более опытные революционные деятели пользуются для переписки в настоящее время или двойными ключами, или страницами малоизвестных книг и брошюр... что крайне осложняет работу». Для успешного разбора криптограмм нередко требовалось наличие не менее 3–5 писем, зашифрованных единым ключом.

ЗА ПОМОЩЬЮ В ДЕПАРТАМЕНТ ПОЛИЦИИ

Пришло время и дешифровальщикам МИД воспользоваться помощью ДП. С началом Русско-японской войны выявились существенные трудности дешифрования японской дипломатической почты. На рубеже XIX–XX столетий в «недвижном Китае» и в Японии произошли такие значительные перемены, что кадровое обеспечение МИД оказалось не готово к необходимому усилению этих направлений. Так, 15 ноября 1904 г. Сабанин сообщал товарищу министра внутренних дел, что русский посланник прислал из Пекина девятнадцать нелегально добытых копий телеграмм, отправленных японскими властями из Тяньцзиня, крупного портового города в Китае. Тринадцать из этих телеграмм были зашифрованы. Сабанин объяснял, что у него «не имеется сотрудников, знакомых с этими языками: японским и китайским». А потому он просил передать указанные тринадцать копий в ДП для расшифровки и перевода. И позже Сабанин неоднократно докладывал, что «все зашифрованные телеграммы не могут быть разобраны». Ещё 26 января 1905 г. он сообщал о возвращении по этой причине тридцати девяти телеграмм, доставленных из Пекина. Только в сентябре в отделении официально утвердился младший чиновник С.В. Литвин, специально занимавшийся японскими шифрами.



Иллюстрация 3. Группа сотрудников Департамента полиции за работой

«СОВЕРШЕННО ДОВЕРИТЕЛЬНО» ОТ МВД

Руководители МВД в начале XX века регулярно направляли министру иностранных дел с пометкой «совершенно доверительно» расшифрованные телеграммы или добытые агентурным путём копии писем и донесений иностранных дипломатов. В июне 1905 г. директору ДП С. Г. Коваленскому представили переводы писем британского посольства. Их копии были доложены государю и министру иностранных дел В. Н. Ламздорфу. В октябре 1905 г. в МИД были направлены копии шести телеграмм из американского посольства, трёх — из китайского, два донесения из греческого посольства и одно — из румынского.

В ноябре 1904 г. из Департамента полиции во второе отделение поступили три японских кода, добытые в Париже агентами ДП.

УСПЕХ ДОСТИГАЛСЯ ОБЩИМИ УСИЛИЯМИ

В зоне боевых действий русско-японской войны военных выручали тогда студенты Восточного института во Владивостоке. Среди различных документов, захваченных русскими моряками на японских судах, оказался телеграфный код. «Разбор и перевод документа оперативно выполнил А. Занковский, снабдив его весьма толковыми для студента 2-го курса комментариями. Кроме того, на пароходе „Хагинура Мару“ была обнаружена зашифрованная телеграмма с исходным текстом». Эти

документы пересылали из одного штаба в другой и наконец передали в дешифровальную службу МИД.

В отчёте за 1907 г. А. А. Долматов сообщал о сотрудничестве с сухопутным и морским генеральными штабами: «Нам доставляются случайно добытые дипломатические депеши разного рода, из которых многие оказались весьма интересными и полезными. Те из этих депеш, разбор которых удаётся, в русском переводе возвращаются агенту Генерального Морского штаба г. Кривошу, который доставляет нам оригиналы».

Так, развивая контакты между подразделениями криптографической службы различной ведомственной принадлежности, российские дешифровальщики в целом успешно справлялись со своими обязанностями. Они предоставляли политическому руководству страны необходимый фактический материал для анализа действительного положения и выработки дальнейших шагов. В годы Первой мировой войны такой опыт был востребован и пригодился на театре военных действий.

ВРЕМЯ ПЕРЕМЕН ДЛЯ КРИПТОГРАФОВ МИД

Перед самым началом войны при реорганизации МИД в нём появилось цифирное отделение. Ему поручили создание новых шифров и оснащение ими представительств и подразделений министерства. Там же состояли чиновники, занятые дешифрованием. Текущую шифровальную деятельность

обеспечивало шифровальное отделение при канцелярии. В основном силами молодых чиновников политических отделов. Это, по замыслу руководства, готовило их к занятию дипломатических и консульских постов за границей.

В феврале 1917 г. в МИД вновь встал вопрос о реорганизации шифровальной службы. Руководители МИД решили, что необходимо поручить всю деятельность шифровального отделения профессионалам. Новая система должна была обеспечить «первое основное требование шифровального дела, его срочность». В качестве профессиональных шифровальщиков предполагалось использовать офицеров, увольняемых по ранению из армии.

Согласно материалам Историко-документального департамента МИД, шифровальное отделение планировали оставить при канцелярии, включив в его состав не менее 32 человек и распределив их на четыре 8-часовые смены. Поскольку у чиновников шифровального отделения не было перспектив продвижения по службе, проект предусматривал им особые надбавки к жалованью, а также возможность по истечении определённого срока службы замещать заграничные должности вице-консулов. Февральская революция внесла в эти планы свои коррективы. И в сентябре 1917 г. новое шифровальное отделение, занятое «шифрованием и расшифровкой секретной переписки», вместе с цифирным отделением были объединены в Шифровальную часть. Шифровальная часть стала самостоятельным подразделением МИД.

Такой окончательный вид приняла криптографическая служба МИД, главная из нескольких разноместных частей, чьё неформальное единство позволяло видеть в них Криптографическую службу России имперского времени. Это единство в значительной степени определялось подчинением воле императора. Новое государство — Советская Россия — стало создавать свою криптографическую службу уже в иных условиях и с другими людьми.



АССОЦИАЦИЯ
БАНКОВ
РОССИИ

30 ЛЕТ ВМЕСТЕ

Ежегодная встреча кредитных организаций с руководством Банка России

«Регулирование Банком России деятельности коммерческих банков»

Во встрече традиционно принимают участие Председатель Банка России, заместители Председателя Банка России, руководители департаментов и служб мегарегулятора, а также представители Госдумы, Совета Федерации, АСВ, Минфина России, Минэкономразвития России, Росфинмониторинга, Службы финансового уполномоченного в России.

Целью ежегодно проводимых встреч, собирающих более 500 участников, является обсуждение в прямом диалоге с регулятором актуальных проблем, стоящих перед банковским сообществом, новых законодательных и нормативных документов.

Организатор мероприятия - Ассоциация банков России.

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



18-19 февраля 2021 года

Онлайн



КИБЕРБЕЗОПАСНОСТЬ НАШИ ДНИ

Промышленные технологии

ДЦ «Юбилейный», г. Магнитогорск

ib-bank.ru/uralcyber

17-19 февраля

НОВЫЙ УРОВЕНЬ ПРОМЫШЛЕННОЙ КИБЕРБЕЗОПАСНОСТИ!

КИБЕРУЧЕНИЯ | МАСТЕР-КЛАССЫ | ПИТЧ-СЕССИИ

НА ФОРУМЕ

- ✓ Признанные эксперты отрасли ИБ
- ✓ Интенсивное обучение лучшим практикам
- ✓ Обмен передовым опытом
- ✓ Эффективные технологии для решения ваших задач



CYBER

#URALCYBER

#URALCYBER

#URALCYBER

#URA

Узнать
больше

