



№4 (39)

2020

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАНКОВ

JOURNAL



22>

Артём СЫЧЁВ
Банк России

**Меняются критерии
оценки и формат
проверок**

26>

Константин МАРКЕЛОВ,
Валерий ШИПИЛОВ
Ассоциация российских банков

**ИИ стал средством
развития банкинга**

30>

Георгий ГАРБУЗОВ,
Алексей ТЕРЕНИН
Сбербанк

**Опыт Сбербанка
открывает перспективу**



38>

Вениамин ЛЕВЦОВ
Лаборатория Касперского

**Компании должны
стать владельцами
домашних офисов**

81>

Алексей ПЛЕШКОВ
Эксперт BIS Journal

Скам на барахолке

2020 ПОБЕДИЛА ЦИФРА





0	0	0	0	0	0	0
1	1	0	0	1	0	1
0	1	1	0	0	0	1
1	0	1	0	1	0	1
0	0	0	0	0	0	0

**Уникальные возможности
для вашего бизнеса**

ib-bank.ru



Алексей ЛУКАЦКИЙ
приглашённый редактор номера

Скоро год, как мир стал жить по новым правилам, называемым странным, не по-русски звучащим словосочетанием «новая нормальность». Пандемия изменила наши взгляды на происходящее вокруг нас и на то, как может функционировать бизнес. Оказалось, он вполне работоспособен и в удаленном режиме, что позволило пересмотреть многие процессы, обеспечивающие коммерческим компаниям доходы, а государственным — оказание госуслуг. Информационная безопасность впервые получила возможность продемонстрировать свою нужность и помочь ИТ организовать удаленную работу безопасным образом. Но переход на удаленку выявил и определенные сложности в обеспечении процессов ИБ, например, в рамках столь популярной сегодня темы, такой как центры мониторинга ИБ (SOC).

...Один аналитик SOC, когда его решили перевести на работу из дома, задал сакраментальный вопрос: «Я живу в однушке со своей девушкой и ее кошкой, на которую (кошку, а не девушку) у меня аллергия. При этом у нас всего один стол, за которым мы едим, а во внеурочное время, моя девушка на нем раскладывает чертежи, она модельер-конструктор одежды. И где мне прикажете разместить три монитора, которые мне разрешили временно забрать с работы?» И это только один из вопросов, на который стоит обратить внимание при организации удаленной работы в SOC. А вот еще несколько:

- ♦ Борьба со стрессом и снижением продуктивности (на удаленке такое снижение составляет до 15 %)
- ♦ Организация командной работы
- ♦ Резервирование каналов связи
- ♦ Менторство над аналитиками нижних уровней
- ♦ План коммуникаций (в рамках инцидентов и вне них)
- ♦ Инструменты общения (от war room в Webex Teams или Zoom до инструментов групповой работы над инцидентами)
- ♦ Удобство работы
- ♦ Удаленное подключение к SOC-платформам
- ♦ Удаленное расследование на удаленных ПК удаленных сотрудников
- ♦ Работа с аутсорсинговыми партнерами, которые также ушли на удаленку.

И это только небольшая часть вопросов, которые всплывают, если скрестить тему удаленной работы и SOC. А если попробовать увязать это с требованиями регуляторов, которые за год так и не удосужились выпустить никаких внятных рекомендаций по организации безопасной удаленной работы, то жизнь становится все чудеснее и чудеснее. Возможно, статьи в этом номере журнала помогут ответить на часть возникших вопросов? Если нет, то приглашаем вас на SOC-Форум Live, где можно будет обсудить то, что мы не успели выплеснуть на страницы журнала.

ОБЩЕСТВЕННЫЙ РЕДАКЦИОННЫЙ СОВЕТ

Емельянов Г. В. — член-корреспондент Академии криптографии РФ, действительный государственный советник РФ 3 класса
Сычев 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. — президент компании «Реальная безопасность», кандидат технических наук
Левиев Д. О. — председатель Совета НП «Партнерство специалистов по информационной безопасности»
Мельников С. Ю. — заместитель генерального директора ООО «Лингвистические и информационные технологии», кандидат физико-математических наук
Некрасов И. В. — главный редактор журнала
Одувалов М. В. — руководитель службы Управления по обеспечению ИБ Банка ВТБ (ПАО)
Окулесский В. А. — заместитель начальника службы ИБ банка «Возрождение», кандидат технических наук
Пазизин С. В. — заместитель начальника Управления по обеспечению ИБ Банка ВТБ (ПАО), кандидат физико-математических наук
Рачкова (Калашникова) 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 BI.ZONE

РЕДАКЦИЯ ЖУРНАЛА

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

УЧРЕДИТЕЛЬ-ИЗДАТЕЛЬ

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

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

Все права на материалы, опубликованные в номере, принадлежат журналу «BIS Journal — Информационная безопасность банков». Перепечатка и воспроизведение иными способами без разрешения редакции запрещаются.

При использовании материалов ссылка на журнал обязательна. Мнение редакции может не совпадать с мнением авторов. Присланные материалы не рецензируются и не возвращаются.

Подписан в печать 15.10.2020. Тираж 7000 экз.
 Заказ № 2322020. Цена договорная. Отпечатан в типографии «Московский Печатный Двор», 123298, г. Москва, 3-я Хорошевская 18, корп. 1, офис 201А

© BIS Journal, 2020



НОВОСТИ

- 5 **В России, законодательство, криминал**

ТЕМА НОМЕРА — SOC

- 8 Алексей Лукацкий (Cisco Systems)
SOC 2.0. 12 шагов, ведущих к пропасти
- 14 Алексей Плешков (Банк ГПБ)
Лайфхаки от Газпромбанка
- 16 Дмитрий Гадарь (Тинькофф)
Лайфхаки от Тинькофф
- 17 Александр Бодрик (thecyberdock.com)
CLOUD-ROBOT SOC
- 20 Иван Мелехин (Информзащита)
Почему вам нужен внешний SOC?



РЕГУЛЯТОРЫ

- 22 **Надзорная деятельность**
Артём Сычёв (Банк России)
Для чего вводятся риск-профиль и киберучения



БАНКИ

- 24 **Вредные советы**
Екатерина Рачкова (Калашникова)
(Банк ВТБ)
Залезь в ящик... Пандоры!
- 26 **Технологии**
Константин Маркелов, Валерий Шипилов
(Ассоциация российских банков)
Цифровая трансформация в банках как неизбежность
- 30 **Технологии**
Георгий Гарбузов, Алексей Теренин
(Сбербанк)
ИИ на страже банковских данных
- 35 **Блокчейн**
Анатолий Конкин, Илья Дружинин
(Ассоциация ФинТех)
ЗКР — блокчейн. Союз скорого будущего

УГРОЗЫ И РЕШЕНИЯ

- 38 Интервью**
Вениамин Левцов (Лаборатория Касперского)
«Лаборатория Касперского» для крупного бизнеса
- 41 SOC**
Тимур Зиннатуллин (ACRC)
Ступенью выше
- 44 Нормативная база**
Дмитрий Кандыбович (StaffCop)
На трёх китах
- 46 Комплексный подход**
Ольга Попова (Индид)
«Мы держим руку на пульсе времени»
- 50 Анализ уязвимостей**
Анастасия Харибина, Павел Семёнов (AKTIV.CONSULTING)
Держите уровень!
- 54 Сегментация**
Илья Кондратьев (АМТ-ГРУП)
Как защитить критичный сегмент: актуальные сценарии
- 56 Управление уязвимостями**
Владимир Бенгин (Positive Technologies)
Как грамотно выстроить управление уязвимостями
- 58 Импортозамещение**
Дмитрий Курашев (UserGate)
Сделано в России, сертифицировано ФСТЭК — 2



ИНФРАСТРУКТУРА

- 60 Деловые мероприятия**
PKI-Форум Россия 2020
- 64 Деловые мероприятия**
Никифор Ковалёв (BIS Journal)
Kaspersky Industrial CyberSecurity Conference
- 66 Деловые мероприятия**
Корней Ревт (BIS Journal)
CISO Форум 2020
- 68 Деловые мероприятия**
Павел Никифоров (BIS Journal)
ВБА-2020
- 69 Деловые мероприятия**
Марк Новоначный (BIS Journal)
MobiFinance-2020
- 70 Условия труда**
Сергей Вихорев (ИТ-Экспертиза)
Цирк уехал, клоуны остались

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

- 73** **Обучение персонала**
Ольга Лимонова, Андрей Жаркевич
(Антифишинг)
«Отделка щенка под капитана»
- 81** **Типология**
Алексей Плешков (эксперт BIS Journal)
Скам на барахолке

ОБРАЗОВАНИЕ И КАРЬЕРА

- 86** **Проекты**
Владимир Никонов (ФСРБИТ),
Борис Столпаков (историк криптографии)
Грань Победы
- 88** **Обзор**
Марина Бродская (BIS Journal)
**Вступительная кампания — 2020:
конкурс взлетел**
- 93** **Обзор**
Анна Катанкина (BIS Journal)
**Школы и университеты под прицелом
хакеров**



73



98

СУБЪЕКТЫ

- 98** **История**
Дмитрий Ларин (историк
криптографии)
**Большая тройка:
Тегеран — Ялта — Потсдам**
- 103** **История**
Борис Столпаков
(историк криптографии)
Первые лица отрасли
- 107** **Анонс**
**Будущее криптографии создаётся
уже сегодня**

«ЯНДЕКС» ОПУБЛИКОВАЛ ЗАКРЫТУЮ СТАТИСТИКУ

Впервые в истории ИБ «Яндекс» опубликовал статистику по выдаче данных пользователей властям. За первую половину этого года ИТ-гигант получил 15 300 запросов. По 12 900 обращений он предоставил информацию, а в 2400 случаев — отказал.

Больше всего запросов на выдачу данных касаются Яндекс.Почты и Яндекс.Паспорта — 8800 обращений от госорганов (7700 удовлетворено).

«Очень часто запросы к тому или иному сервису сводятся к предоставлению данных из Яндекс.Паспорта. Например, это может быть запрос о пользователе, который использовал один из сервисов Яндекса для мошенничества», — рассказал глава пресс-службы компании Илья Грабовский.

Он также заверил, что доступ к пользовательской переписке компания предоставляет только по судеб-

му решению, ограничивающему право человека на тайну переписки.

На втором месте по востребованности — Яндекс.Такси — 5200 запросов (4100 удовлетворено). Запросы касаются информации о водителях и о передвижениях пассажиров.

По остальным своим сервисам компания получила 1200 запросов.



НАСТОЯТЕЛЬНОЕ ИМПОРТОЗАМЕЩЕНИЕ

ИТ-компании предложили Минцифры устанавливать отечественные ОС и пакеты офисных программ на все компьютеры, которые будут продаваться в РФ. Эксперты считают, что это не должно повлиять на стабильность работы устройств, но увеличит их цену.

Инициатива содержится в предварительном списке мер поддержки ИТ-отрасли, который Минцифры готовит для курирующей отрасль вице-премьера Дмитрия Чернышенко. Список сформирован из предложений рынка, ИТ-ассоциаций и отдельных

экспертов. В нём — почти 100 мер по 11 направлениям: ИБ, здравоохранение, образование, ЦОДы, ИИ, офисное ПО, онлайн-кинотеатры, компьютерные игры, мессенджеры и др.

В настоящее время перечень находится на рассмотрении в министерстве, далее его отправят вице-премьеру. По плану, из списка отберут 20–30 предложений.

Ранее участники Евразийского экономического союза выступили против закона об обязательной предустановке российского ПО на устройства, продающиеся в России.

ЧЁРНАЯ МЕТКА ЦЕНТРОБАНКА

Банк России планирует публикацию списка компаний, предоставляющих нелегальные финансовые услуги, рассказал первый зампред ЦБ РФ Сергей Швецов на онлайн-брифинге в рамках Международной недели инвесторов.

Ранее он сообщал, что с января по сентябрь текущего года регулятор выявил и «прикрыл» 1 тыс. нелегальных поставщиков финуслуг, в том числе 140 финансовых пирамид, 600 «чёрных кредиторов» и 200 форекс-дилеров, осуществлявших свою деятельность нелегально.

«Сейчас мы обсуждаем вопрос публикации списка компаний, которые, как мы считаем, работают за пределами легальной плоскости, на своём сайте, чтобы гражданам было легче их идентифицировать», — сказал С. Швецов и добавил: «Мы активно информируем правоохранительные органы о выявленных компаниях, которые работают незаконно на российском рынке».

ВСПЛЕСК ПОКУПОК ЧЕРЕЗ QR-КОД

В октябре ЦБ РФ зафиксировал резкий рост числа операций по оплате с помощью Системы быстрых платежей (СБП). По сравнению с сентябрем показатель вырос на 214%.

В октябре россияне оплатили покупки таким способом 213 тыс. раз на общую сумму 765 млн руб., а всего с момента запуска СБП — почти 390 тыс. раз на сумму 1,67 млрд руб. То есть на октябрь пришлось 54% от общего числа операций и 45,8% от общей суммы в рублях.

Банки считают, что на скачок повлияло подключение к СБП крупных торговых сетей и брокеров с высоким средним чеком. Кроме того, начались интеграции оплаты по СБП с программами лояльности у крупного бизнеса, который начал предоставлять за неё бонусы. Ещё одна причина — отмена ЦБ РФ с 1 октября льготных комиссий за приём карт для e-commerce, что подстегнуло большинство площадок, откладывавших подключение к СБП.

ПОДМЕНЕ НОМЕРА — ЗАСЛОН!

Согласно постановлению от 29 сентября 2020 года № 1559 внесены поправки в Правила присоединения сетей электросвязи и их взаимодействия. Изменения позволят российским мобильным операторам корректно идентифицировать международные вызовы и сократить вероятность мошенничества с подменой номера.

Сегодня международные вызовы на российские номера могут маскироваться под местные звонки в целях экономии на пропуске трафика. Это почва для мошеннических действий.

Введение услуги завершения международного вызова позволит правильно определять и выявлять международный трафик и тарифицировать его. Операторы будут анализировать номер, с которого изначально поступил звонок. Это сделает неэффективной подмену номера для зарубежного трафика.

ПРО ЗАПРЕТ ПРОТОКОЛОВ ШИФРОВАНИЯ

Проект поправок к закону «Об информации» предполагает запрет ряда протоколов шифрования, среди которых TLS 1.3 с расширением ESNI, DoH (DNS поверх HTTPS) и DoT (DNS поверх TLS).

По мнению РСПП, если поправки примут в существующем виде, то формально использование компьютеров и гаджетов станет незаконным. Работа информационных систем остановится, что чревато «катастрофическими негативными последствиями». Операторам

информационных систем придётся отключать криптографические инструменты или модернизировать их.

Мнение РСПП разделяют директор «Интеллектуального резерва» Павел Мясоедов, партнёр Deloitte Денис Липов и исполнительный директор Artezio Павел Адылин. По их мнению, запрет протоколов выгоден только злоумышленникам. Также он усложнит процедуру использования зарубежных ресурсов, которые внедряют нововведения.



STAFFCOR

Программа для контроля информации, действий пользователей и событий системы на ПК

**МОНИТОРИНГ.
АНАЛИЗ. ОПОВЕЩЕНИЕ.
БЛОКИРОВКА**

опасной и непродуктивной деятельности сотрудников

WWW.STAFFCOR.RU



Единый реестр российских программ Минсвязи РФ №3337
Сертификат ФСТЭК №4234



ПОПРОБУЙТЕ БЕСПЛАТНО



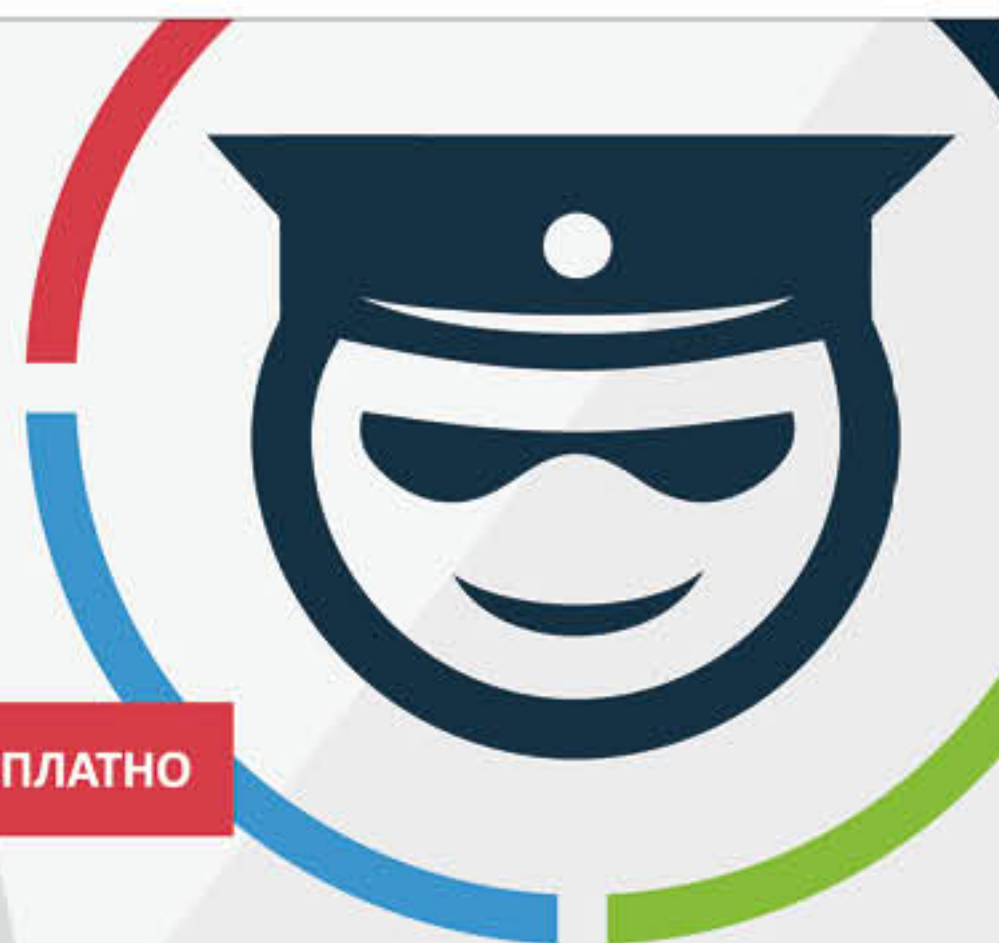
**ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ**



**КОНТРОЛЬ
ЭФФЕКТИВНОСТИ
СОТРУДНИКОВ**



**УДАЛЕННОЕ
АДМИНИСТРИРОВАНИЕ**



ПРЕДОТВРАЩЕНИЕ УТЕЧЕК

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ

УЧЕТ РАБОЧЕГО ВРЕМЕНИ

ПРОДУКТИВНОСТЬ И КРИ

УДАЛЕННЫЙ РАБОЧИЙ СТОЛ

МОНИТОРИНГ И БЛОКИРОВКИ
USB-ПОРТОВ, САЙТОВ И ПРИЛОЖЕНИЙ

КИБЕРГРУППИРОВКА РАСПРОСТРАНЯЛА ОТЕЧЕСТВЕННЫХ ЗЛОВРЕДОВ

Следственной частью Главного управления МВД России по Северо-Кавказскому федеральному округу завершено расследование уголовного дела по обвинению группы лиц в совершении преступления, предусмотренного ч. 2 ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ».



Оперативное сопровождение уголовного дела осуществлялось сотрудниками Управления «К» МВД России и окружного полицейского Главка.

Установлено: 20-летний уроженец Республики Северная Осетия — Алания три года назад создал вредоносное ПО, предназначенное для несанкционированных модификаций и копирования информации. К распространению зловредов он привлёк ещё шестерых соучастников, которые в период с ноября 2017 г. по март 2018 г. распространили на территории страны более 2100 экземпляров ПО. Группа получила доход в размере более 4,3 млн рублей.

Следственные действия и оперативные мероприятия проведены на территории Северной Осетии — Алании, Татарстана, Волгоградской, Рязанской, Тульской областей, а также на территории других субъектов РФ.

СЕМЬ ЛЕТ ЗА ВЫВОД ДЕНЕГ СО СЧЕТОВ КЛИЕНТОВ

По данным следствия, банковский служащий Энди Ли с 2015 по 2019 год выводил средства со счетов своих клиентов. Для этого — теперь уже бывший — сотрудник Bank of Melbourne предлагал людям оформить срочный вклад, а затем направлял деньги на другие счета — оформленные на подставных лиц.

Также Ли переводил средства своей девушке, а на свой личный счёт отправил не более 400 тыс. долларов.

Пара, у которой он украл около 1,5 млн долларов, даже присутствовала на его свадьбе. Похищенные деньги мошенник вкладывал в недвижимость и ресторанный бизнес, а также тратил на предметы роскоши: 26 дизайнерских наручных часов и два автомобиля Porsche (один — для своей девушки).

В сентябре фигуранта приговорили к тюремному заключению на срок семь лет и восемь месяцев.



КОЛОНИЯ-ПОСЕЛЕНИЕ ЗА КРАЖУ ДАННЫХ

Фигуранта, укравшего и опубликовавшего в даркнете персональные данные клиентов Сбербанка, приговорили к двум годам и десяти месяцам колонии-поселения. Суд также обязал его заплатить штраф в пользу кредитной организации в размере более чем 25 млн рублей.

В октябре прошлого года был задержан руководитель сектора в одном из бизнес-подразделений Сбербанка. За месяц до этого он попытался продать несколькими траншами 5000 учётных записей клиентов кредитной организации.



БЕЗ РАЗРЕШЕНИЯ СУДА

В Энгельсе возбуждено уголовное дело в отношении бывшего сотрудника мобильного оператора. Молодой человек обвиняется по ч. 2 ст. 138 УК РФ (нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений граждан, совершённое лицом с использованием своего служебного положения).

Подозреваемый работал специалистом офиса продаж в одной из компаний сотовой связи. Следователи считают, что молодой человек, воспользовавшись своим служебным положением, получил доступ к информации о входящих и исходящих звонках 698 абонентов компании. Сотрудник просматривал личные данные граждан без их согласия, а также без разрешения суда. Таким образом, молодой человек нарушил тайну переписки, телефонных переговоров и иных сообщений, пришли к выводу следователи.

SOC 2.0. 12 ШАГОВ, ВЕДУЩИХ К ПРОПАСТИ

И 12 СОВЕТОВ, КАК ИХ ИЗБЕЖАТЬ



**Алексей
ЛУКАЦКИЙ**
бизнес-консультант
по безопасности
Cisco Systems

Тема центров мониторинга ИБ (Security Operations Center, SOC) в России известна давно, и обычно её представляют в радужных тонах — там успех, здесь победа. Но не всё так красиво, как обычно это выглядит на презентациях SOC-Форума. Очень часто в деле построения SOC'ов совершаются ошибки, которые приводят к неоправданным тратам и несбывшимся ожиданиям. И хотя никто не застрахован от ошибок (и их надо совершать, чтобы уроки лучше запоминались), есть вещи, которые лучше сразу делать правильно. Да, безусловно. Есть ошибки, которые не привели

к краху и даже способствовали построению успешного центра мониторинга. В этом случае это не те ошибки, которых надо бояться. А есть истории успеха, которые, будучи повторёнными в других местах, не привели к тому же результату и, даже бывает так, привели к провалу. Поучаствовав в десятке проектов по построению или аудиту SOC'ов в разных странах постсоветского пространства, я собрал коллекцию наблюдений типичных ошибок, которыми я и хотел бы поделиться с читателями, чтобы они не наступали на те же грабли, что и их предшественники.



ЧТО ТАКОЕ SOC?

Одна из классических ошибок, которая возникает почти в любом проекте, — отсутствие согласия в терминологии, а именно в понимании того, что должен делать SOC. И вроде на пальцах все понимают, о чём идёт речь, но копни глубже, и всё, начинается рассинхронизация. Для кого-то SOC — это только центр мониторинга, кто-то добавляет в него и реагирование, третьи наделяют SOC ещё и возможностями по управлению всеми средствами защиты, а четвёртые, говоря «SOC», имеют в виду вообще всю службу ИБ. Но это ещё полбеды. Даже если сфокусироваться только на мониторинге,

то включать ли борьбу с DDoS в сферу внимания SOC? А поиск уязвимостей? А контроль утечек? А мониторинг репутации и Darknet? А мониторинг мошенничества в банках? У каждого специалиста по ИБ своё восприятие термина Security Operations Center, и каждый из них считает, что это восприятие настолько очевидно, что и тратить время на разъяснение не нужно.

Отсюда и стартует большинство проблем. По моим наблюдениям, до 50% провалов проектов по созданию SOC'a происходят именно из-за того, что стороны (служба ИБ, ИТ, руководства компании, подрядчик) не договорились о том, что же они хотят получить на выходе. Отсюда неоправданные ожидания, недовольство и признание проекта неудавшимся с вытекающими отсюда оргвыводами.

Совет № 1 Потратьте несколько часов или дней на мозговую штурм, в результате которого родится не только устраивающее всех понимание функций и задач SOC, но и его сервисная стратегия, которая и станет краеугольным камнем всех последующих шагов.

МАСШТАБИРУЕМОСТЬ

Ещё одна интересная особенность выплывает в крупных проектах, ориентированных на покрытие множества часовых поясов и работу во множестве регионов. Понятно, что пилотный проект, который обычно предшествует вводу SOC'a в промышленную эксплуатацию, является уменьшенной копией, разворачиваемой на одной-двух площадках. И так часто бывает, что для пилота выбирается решение без учёта итоговой архитектуры и масштаба. Например, в одном проекте пилот показал отличные результаты, но попытка масштабировать его на несколько регионов привела к неспособности выбранных технических решений обрабатывать такое количество данных и проводить в них поиск. И даже расширение лицензий на SIEM не решило проблему.

В другом проекте была схожая проблема, но там она возникла по другим причинам. Компания решила следовать «линии партии», взявшей курс на импортозамещение, и стояла задача построить SOC целиком на отечественных решениях. В процессе проектирования выяснилось, что один из отечественных SIEM'ов не способен «переварить» больше определённого количества событий в секунду (event per second, EPS) и надо использовать кластер из SIEM, между которыми распределялась нагрузка. Вместо одного условного Splunk, который в России больше не работает,

использовалось три копии одного российского SIEM'a, обрабатывающего тот же поток данных (и ещё один «мастер-SIEM» для управления ими). А так как проектируемый SOC был иерархическим и в разных странах присутствия компании строились свои региональные SOC'и, то число копий российского SIEM'a достигло двух десятков.

И дело даже не в том, что тот же Splunk «закрыл» бы задачу только одной своей инсталляцией. Просто такое потакание курсу на цифровой суверенитет привело к тому, что в проекте исчезла возможность оперативного поиска в едином массиве данных — каждый региональный центр мониторинга, по сути, был независимым от других и мог делиться только сводной информацией.

Правда, был в этом и положительный момент. Российский разработчик SIEM получил задание по доработке своего решения под разработанный проект, чтобы в будущем улучшить свои показатели масштабирования. А пока потребитель использует вместо одного SIEM двадцать и поддерживает тем самым отечественного производителя.

Совет № 2 Проектируя SOC, учитывайте его не только текущую, но и планируемую архитектуру.

ПОКРЫТИЕ И ТЕЛЕМЕТРИЯ

«У нас есть SOC!» или «Мы построили SOC!». Такие высказывания часто слышишь от коллег на различных конференциях по ИБ, где все делятся опытом и успехами. Но стоит копнуть глубже, и выясняется, что уровень покрытия SOC'ом существующей инфраструктуры достаточно низкий и ограничивается преимущественно периметром. На SOC не заведены не только облачные среды (а многие сегодня переносят часть ресурсов в публичные облака) или мобильные устройства, не только промышленные площадки (если они есть в организации), но даже кампусная, внутренняя сеть остаётся вне сферы влияния центра мониторинга, который не умеет или не знает, как мониторить Netflow или иные flow-протоколы

и как собирать телеметрию с коммутаторов, маршрутизаторов и точек доступа (включая и виртуальные), через которые проходит весь внутренний трафик и которые также должны мониториться в целях обнаружения инцидентов, начавшихся с обхода периметровых средств защиты или с инсайдеров, которые начинают сливать данные.

Помимо Netflow, внутренняя сеть может и должна отдавать в SOC данные с хостов и приложений, которые будут коррелироваться с сетевыми событиями. Без этого SOC является красивой и дорогостоящей, но всё-таки игрушкой, не приносящей почти никакого выгоды.

Совет № 3 Чем больше источников телеметрии с разных участков инфраструктуры попадает в SOC, тем оперативнее он может выявлять инциденты. Составьте план расширения уровня покрытия SOC от периметра внутрь кампусной сети, а также наружу — в облака и мобильные устройства.

УРОВНИ L1-L3

Ох уж эти три уровня аналитиков SOC, обсуждение которых идёт уже не первый год. Кто-то считает, что наличие этих уровней говорит о зрелости SOC, и по-другому и быть не может. Первая линия отсекает явные ложные срабатывания и проводит вторичную обработку событий (после SIEM) и заводит соответствующие тикеты в IRP или SOAR системе (вот тоже большая тема для дискуссии — чем отличается IRP от SOAR и SGRC?). Вторая линия разбирается с более сложными случаями, а третья — это такая швейцарская гвардия, которая призывается только в особых случаях и самых сложных инцидентах, требующих, например, реверс-инжиниринга вредоносного кода.

Но есть и другая точка зрения, которая предполагает отказ не только от L1, которую можно заменить технологиями, справляющимися с приоритизацией, ложными срабатываниями, заведением тикетов лучше и быстрее, но и вообще от концепции уровней L1-L3 в SOC. В таких SOC'ах гораздо лучше выстроена ротация аналитиков, и они могут попробовать себя в разных ролях, получая новые знания и навыки и повышая свою эффективность. Больше возможностей по взаимодействию, менторству и обмену знаниями — это ключевая характеристика SOC'ов, которые отказались от модели L1-L3. Правда, есть и ряд условий, которые обязательны для существования такого SOC. Речь

Больше возможностей по взаимодействию, менторству и обмену знаниями — это ключевая характеристика SOC'ов, которые отказались от модели L1-L3

в первую очередь идёт об определённом уровне корпоративной культуры, которая в отечественных условиях сформирована далеко не везде и не всегда.

Совет № 4 Не гонитесь за модой и не стройте SOC по принципу «все так делают». Возможно, в вашем случае аналитики могут работать и без чёткого деления на уровни L1-L3.

ИНТЕГРАЦИЯ С ИТ

Ещё одна боль многих SOC'ов — их неумение выстраивать работу с другими подразделениями и, в частности, с ИТ. Например, на одном из серверов выявлена критическая уязвимость, и SOC, недолго думая, открывает соответствующий тикет и отправляет заявку на устранение уязвимости в ИТ-службу. И... А дальше всё — никакого контроля исполнения заявки внешними подразделениями. Через месяц выясняется, что... Да много может быть причин. Ложное срабатывание сканера уязвимостей, уязвимость не может быть проэксплуатирована в конкретной инфраструктуре, сервер не критичный, вендор не выпустил патч... Центр мониторинга эскалирует проблему вышестоящему руководству, где и выясняется, что SOC — это скорее вещь в себе, чем интегрированное в компанию подразделение. Так ещё и конфликтная ситуация возникла, которая ни к чему хорошему не приведёт, так SOC не может эффективно работать без поддержки со стороны ИТ. Та же реконфигурация средств защиты, которые могут находиться в эксплуатации у ИТ...

Отсутствие регламентов взаимодействия SOC'а с другими подразделениями — это распространённая проблема многих российских центров мониторинга ИБ, что в случае серьёзных инцидентов выливается в лишнюю трату времени и большие потери.

Совет № 5 Помните, что SOC не может работать сам по себе, изолированно от других. Как минимум наладьте и регламентируйте взаимодействие с ИТ-подразделением (даже если SOC аутсорсинговый), а также с иными, чья помощь может понадобиться, — HR, юристы, экономическая безопасность и т.п.

СЦЕНАРИИ ИЛИ USE CASE

В уже функционирующих SOC'ах такого уже не встречается, но для тех, кто только подступает к теме, это неоправданное ожидание звучит постоянно. На вопрос «Какие сценарии мониторинга для вашего SOC являются

На вопрос «Какие сценарии мониторинга для вашего SOC являются приоритетными?» ответ часто звучит так: «Мы хотим мониторить всё!»

приоритетными?» ответ часто звучит так: «Мы хотим мониторить всё!». Это как с системами обнаружения вторжений, в которых нередко включают абсолютно все сигнатуры, которые есть в системе, в надежде на то, что это позволит увидеть больше атак. Не позволит. Только ухудшит ситуацию, так как система будет либо жутко «фолсить» (то есть генерить ложные срабатывания), либо излишне нагружать себя обработкой событий, которые никогда не встретятся в месте установки системы мониторинга. Так и с SOC'ами — они не мониторят всё и вся — у них есть вполне конкретный набор сценариев, которые наиболее актуальны для предприятия, в котором функционирует SOC. Эти сценарии зависят от модели угроз, ожиданий руководства, требований законодательства, ИТ-ландшафта и ряда других параметров, но список их всё равно конечен. У кого-то их несколько десятков; у кого-то 2–3 сотни. Но уж точно не тысячи возможных сценариев (use case). Безусловно, есть набор стандартных для многих сценариев (типа контроля привилегированного доступа, неудачные попытки аутентификации, аномалии доступа, утечки данных, использование уязвимостей, отказ средств защиты и сервисов и т.п.), но их не так уж и много.

Совет № 6 Начните настройку инструментов мониторинга в своём SOC'е с формирования перечня сценариев (use case), которые для вас являются наиболее актуальными, постепенно расширяя их число не столь популярными, но всё-таки встречающимися ситуациями. И не забывайте регулярно пересматривать этот перечень, опираясь на происходящие вокруг SOC'а изменения.

АВТОМАТИЗАЦИЯ И ОРКЕСТРАЦИЯ

Это интересная история. Во многих SOC'ах есть SIEM'ы, есть TIP-платформы, есть системы тикетинга. На бумаге или в формате вики хранятся сборники дежурных процедур (playbook). То есть мониторинг худо-бедно, но выстроен. Проблемы начинаются, когда мы фиксируем инцидент и необходимо на него среагировать. Вроде как эту задачу решают системы класса SOAR (Security Orchestration, Automation and Response), которые давно уже стали

неотъемлемой частью современного SOC'a. И не так важно, речь идёт о платном решении типа Splunk Phantom, бесплатном Cisco SecureX или решении open source TheHive.

Проблема в том, что каждая из трёх букв O, A и R работают не очень хорошо. Во-первых, далеко не у всех компаний есть чёткое понимание термина «инцидент», иначе как можно объяснить, что многие компании заявляют о том, что они сталкиваются ежедневно с тысячами (!) инцидентов (даже не атак). К слову, служба ИБ Cisco, ежедневно получая с инфраструктуры около 1,2 триллиона событий безопасности, трансформирует их всего в 22 инцидента. Говоря о тысячах инцидентов, надо понимать, что управлять ими будет некому. Даже после внедрения SOAR время локализации инцидента может составлять от полутора десятков минут до нескольких часов (зависит от инцидента). Даже при 12-часовой смене аналитика SOC отработать ему более 50 инцидентов не получится (и то в идеальной ситуации). Откуда берутся тысячи инцидентов, непонятно.

Во-вторых, у трети компаний вообще отсутствует формализованный процесс реагирования на инциденты, без которого SOAR не работает.

В-третьих, оркестрация подразумевает возможность подключаться к управляемым средствам защиты. Но если они не имеют API (например, отечественные решения, насквозь сертифицированные и обвешанные печатями регуляторов) или к ним запрещён формуляром на средство защиты удалённый доступ, то полностью задачу оркестрации решить невозможно. А тут ещё и неочевидная ситуация с вмешательством SOAR своими скриптами в регламенты работы средств защиты. Кто будет нести ответственность, если реагирование пойдёт не так и что-то важное будет заблокировано?

Поэтому SOAR далеко не всегда запускается в полностью автоматическом режиме, превращаясь в дорогостоящую экспертную систему.

Совет № 7 Попробуйте начать с SOAR-функциональности в вашем SIEM'e (если она там есть) или с бесплатного или open-source-решения, пилотирование которого позволит не только понять зрелость вашего процесса реагирования, но и сформулировать требования к SOAR-решению. Также можно начать работу с SOAR с реализации каких-то типовых playbook'ов, попутно не только готовя новые сборники дежурных процедур, но и создавая варианты сопряжения SOAR с имеющимися средствами защиты; если не напрямую, то через промежуточный шлюз.



ОТСУТСТВИЕ ПРОДВИНУТЫХ СРЕДСТВ АНАЛИТИКИ

Несмотря на то что в России тема SOC активно продвигается уже лет пять, для многих технологическим ядром SOC по-прежнему является SIEM, оперирующий одними логами, получаемыми от средств защиты, сетевого оборудования, прикладного и системного ПО. А что с Netflow или поведенческими характеристиками пользователей? А что с мониторингом DNS-активности? А применяется ли машинное обучение или хотя бы цепочки правил для SIEM, позволяющие выявлять достаточно сложные события безопасности? Нередко бывает так, что даже купленное и достаточно дорогостоящее



решение по мониторингу используется от силы на треть своих возможностей, а технологии, которые, по версии Gartner, составляют ядро SOC следующего поколения (речь идёт о NTA, мониторинге сетевых аномалий, EDR, мониторинге персональных и мобильных устройств, а также CASB, мониторинге SaaS-платформ), не используются вовсе, оставляя немалое количество инцидентов за пределами внимания аналитиков SOC.

Совет № 8 Начиная с мониторинга логов, не забудьте и про другие источники телеметрии, а также продвинутые методы анализа этих источников.

МЕТРИКИ

С показателями эффективности ситуация обстоит хуже всего, так как это последнее, до чего доходят руки у руководства SOC. Инциденты обнаруживаются? Да. Чего ещё надо? Наверх, на стол руководству компании, уходят цифры отражённых ежемесячно атак и локализованных инцидентов, а на уровне SOC к этим метрикам добавляются более привычное время реагирования или локализации инцидента, загрузка аналитиков SOC, число незакрытых тикетов и инцидентов. А что насчёт других, не менее показательных метрик — уровень автоматизации SOC, число инцидентов, обнаруженных с помощью данных Threat Intelligence,

процент эскалации инцидентов на уровень L2, число ложных срабатываний, уровень прохождения аналитиками тренингов и курсов повышения квалификации, число инцидентов, не имеющих use case, уровень покрытия SOC, число инцидентов из-за известных уязвимостей и др.? Не измеряя ключевые и не очень показатели деятельности SOC, включая и время перехода от одного элемента дежурной процедуры (playbook) в SOAR к другому (это позволяет оценивать не просто время расследования и локализации конкретного инцидента, но и выявлять конкретные шаги рабочей процедуры, из-за которых инцидент расследуется слишком долго и неэффективно), мы не в состоянии улучшать процессы мониторинга и реагирования. Без этого нельзя также и руководству компании донести эффективность инвестиций в центр мониторинга ИБ и показать результаты его деятельности, понятные именно на бизнес-уровне.

Совет № 9 Выстраивая технологический стек, описывая процессы и набирая и тренируя людей, ни в коем случае нельзя забывать про процесс измерения эффективности своего SOC. Из каталога из нескольких десятков и даже сотен метрик со временем остаются только ключевые, отслеживание которых и

позволяет следить за успехами и провалами в SOC и выстраивать планы его улучшения и развития.

ОТСУТСТВИЕ ПЛАНОВ РАЗВИТИЯ

Отсутствие планов развития — это ещё один, казалось бы, не так уж и заметно влияющий на работы SOC'а фактор, но при этом он является достаточно важным. Не имея на руках утверждённого плана развития, мы не можем выстроить план обучения аналитиков, инвестиций в новые технологии и аналитические возможности, подготовки новых сборников дежурных процедур, визуализации новых дашбордов и отчётов и т.п. Не имея плана развития, SOC часто топчется на месте, хаотически берясь то за одно, то за другое, в зависимости от того, какая вожака попала под хвост руководителю SOC или службы ИБ, в рамках которых и действует центр мониторинга.

Совет № 10 Имея в голове некую идеальную картину своего SOC (может, вы хотите построить не Security Operations, а уже Fusion Center), попробуйте выплеснуть её на бумагу и зафиксировать ключевые атрибуты будущего центра. Затем, опираясь на имеющиеся ресурсы и временные рамки, можно выстроить стратегию достижения идеального SOC'а, стартуя с текущей точки.



Алексей ПЛЕШКОВ
заместитель
начальника
Департамента
защиты
информации
Банка ГПБ (АО)

ЛАЙФХАКИ ОТ ГАЗПРОМБАНКА

Если перефразировать (от обратного) основную аксиому планиметрии, то допустимо утверждать, что помимо кратчайшего расстояния между двумя точками в пространстве существует бесконечное множество других, отличающихся друг от друга, путей. Эту метафору объективно можно применить и в жизни, в отношении последовательных сценариев создания и развития центров мониторинга информационной безопасности. При прочих равных условиях не существует двух одинаковых SOC. За каждым SOC в РФ стоит своя история, свой сценарий развития, свой путь между двумя точками на временном отрезке существования.

Что касается пути становления SOC Газпромбанка с 2009 года по настоящее время, то

назвать его кратчайшим и оптимальным просто язык не поворачивается. За более чем десять лет мы смогли превратить дежурную смену с базовым opensource-инструментарием для мониторинга доступности и работоспособности технических средств защиты информации в один из лидирующих ситуационных центров по информационной безопасности в финансовой отрасли России. Постараюсь не пересекаться с автором сборника лучших практик по SOC-строению от CISCO и приведу лишь несколько лайфхаков, которые реально помогли нам достичь нужного эффекта при создании SOC в Газпромбанке.

◆ Не бойтесь пилотировать, пробовать и внедрять новые инструменты сбора и мониторинга событий: часто синергетический эффект от

НИЗКИЙ КОНТРОЛЬ КАЧЕСТВА

Отсутствие планов развития имеет и другую сторону — отсутствие контроля качества в SOC, который реализуется отдельным человеком или подразделением, независимым от других отделов (мониторинга, реагирования, threat intelligence, расследования, threat hunting и т.п.), который, по сути, является таким аудитором или внутренним контролем, который, невзирая на регалии участников процесса и их близость к руководству, фиксирует все слабые места и недостатки SOC'а, его технологий, процессов, персонала и, не стесняясь, выносит их на обсуждение с последующим устранением. По сути, можно говорить об этом мини-плане развития в краткосрочной перспективе.

Совет № 11 Выделите сотрудника (как минимум), который был бы наделён полномочиями и был достаточно подкованным во всех вопросах построения и эксплуатации SOC'а, чтобы он мог выступать в качестве «ревизора» и готовить предложения по улучшению. Тем же, кому сложно добиться создания ещё одной штатной единицы, а свободных людей в SOC'е нет, стоит задуматься о внешнем аудите своего центра мониторинга.

Отсутствие планов развития имеет и другую сторону — отсутствие контроля качества в SOC, который реализуется отдельным человеком или подразделением, независимым от других отделов

ОТЧЁТЫ И ДАШБОРДЫ

Думаю, что завершить дюжину наблюдений по SOC'ам стоит ещё одним, неразрывно связанным с уже описанной проблемой под номером 9, а именно речь пойдёт о дашбордах и отчётах, демонстрирующих работу центра мониторинга. При этом я не говорю о видеостенах, на которых показывают экраны SIEM, UEBA, NTA или SOAR/IRP. Речь идёт о способе визуализации, который позволяет, увидев ключевые показатели эффективности, добиться инсайта или озарения и увидеть что-то, что нельзя увидеть в обычном отчёте или панели средств мониторинга. Для этого, правда, необходимо понимать, не только что делает SOC, но и зачем он это делает, и как это соотносится с требованиями всего бизнеса или его отдельных направлений. А это, увы, большая редкость. Для многих задача SOC — это снижение числа инцидентов и не более. А так как

использования той или иной подсистемы наступает намного позже, чем вы ожидаете при планировании, но это не повод забывать про обновление и развитие источников атомарных событий и алгоритмов обработки цепочек.

♦ Наличие двух и более альтернативных центров компетенций внутри SOC не только вредно, но и полезно: в аргументированном диалоге (не путать с конфликтом) между участниками с различными точками зрения часто рождается именно то решение (как в организационном, так и в техническом плане), которое станет стратегически верным в данных обстоятельствах.

♦ Бесполезность организационных каналов поступления в SOC информации о событиях с признаками инцидентов (по телефону, электронной почте, в диалоге с коллегой) сильно преувеличена: по опыту, именно полученные без использования технических средств данные об инцидентах в целевых системах становятся бесценной базой для формирования наиболее эффективных правил и цепочек для SIEM (в силу своей очевидности для обывателей).

♦ С самого начала создания SOC важно учесть и иметь организационную и штатную возможность разделить процессы выявления, обработки, учёта и расследования инцидентов: объединение в одних руках (в силу ограничения штатного расписания) этих процессов негативно сказывается на общей эффективности работы SOC и не позволит быстро (в терминах проектного управления) запустить потоковую обработку инцидентов.

♦ Качество визуализации в дашбордах для первой линии и наличие мультиканальной системы уведомлений так же важны, как и чёткая логика сбора и обработки событий с признаками инцидентов: можно накапливать бесконечное количество атомарных событий с высокой степенью детализации, но без понятной дежурным инженерам подсистемы визуализации и своевременных уведомлений эти события не будут иметь никакой превентивной ценности для организации в целом до момента фактического поступления в SOC сообщения об инциденте по альтернативным каналам.

«продать» это бизнесу достаточно сложно (в отличие от, например, снижения объёма мошенничества или ущерба от инцидентов или снижения стоимости клиентской записи в Darknet), то рождаются многостраничные отчёты, размалёванные всеми цветами радуги, или такие же статические, но дашборды во всю стену, которые что-то показывают, но насколько это важно, никто не понимает (даже их авторы). Руководство тоже не понимает, но по количеству страниц или частоте мигания дашборда делает вывод, что «да, люди работают, значит, всё хорошо».

Совет № 12 Отчёт или дашборд — это способ визуализации наиболее важной для целевой аудитории информации, сгруппированной по смыслу так, чтобы её было легко понять и принять какие-то управленческие решения (получить деньги, полномочия, людей, одобрение...). Просто показать число инцидентов — это не цель, и ни к какому решению это число не приведёт. Поэтому важно уделять внимание не только «понятным» вещам, таким как количество EPS / FPS у SIEM

или выбор способа анализа журналов регистрации Windows, но и тому, как воспринимается информация людьми и как правильно доносить до них имеющиеся показатели деятельности.

* * *

Мы плавно подошли к финалу нашего движения к SOC 2.0. Кто-то успешно сделал все 12 шагов и смог пересечь пропасть, запустив SOC нового поколения, в котором все его элементы — и люди, и процессы, и технологии, и сервисная стратегия — подчинены единому замыслу и увязаны с бизнес-потребностями компании, которая раскошелилась на этот центр. Кто-то ещё только делает эти шаги в надежде построить SOC 2.0. Главное, не ошибиться и для описанных в статье 12 наблюдений (а на самом деле у меня их больше) реализовать приведённые советы, чтобы движение к центру мониторинга будущего не превратилось в падение в пропасть. Удачи вам на этом пути!



Дмитрий ГАДАРЬ
директор
Департамента
информационной
безопасности,
Тинькофф

ЛАЙФХАКИ ОТ ТИНЬКОФФ

Поддерживаю Алексея! Все советы по делу! Я бы дополнил еще несколькими идеями.

1. Не изобретайте велосипед. Не нужно разрабатывать все правила и сценарии с нуля — в условиях «гитхабизации» огромное количество готовых правил корреляции доступны аналитикам. Умейте использовать чужой опыт — iOs, техники поведения злодеев и т.д. Много из этого открыто и доступно в интернет, например, в каналах twitter.

2. Переиспользуйте. Выясните, что уже реализовано — в мониторинге ИТ, клиентском антифроде, сверках платежей ОПЕРу. Это не только инфраструктура, это могут и должны быть критичные прикладные системы, DLP, антифрод.

3. SOC — это в первую очередь набор процессов и людей, структурированных под вашу организацию. SIEM не всегда главный компонент, а возможно, что он в вашем SOC и не нужен. Не обязательно стараться все затянуть в SIEM — вполне нормальный вариант делать прекоорреляцию на sysmon на конечных хостах.

4. Интегрируйте проактивные техники threat intelligence/threat hunting в процессы SOC.

5. Тестируйте каждое правило SOC. Постоянно. Автоматизировано. На практике без этого вы рискуете узнать, что из источника пропали события или уже после инцидента не работает правило. Считаете что закрыли мониторингом какую либо технику хакерской группы? Протестируйте это руками red team и поставьте на мониторинг. Нет red team? Найдите способы тестирования и автоматизируйте их. Иначе не считается.

6. Внедрение средства защиты не считается, если SOC не принимал в нем участие и не реагирует на него.

7. Автоматизируйте все, что можно автоматизировать. Задать вопрос пользователю в мессенджер и обработать его ответ вполне может и робот.

8. Профилируйте! Планируйте как развивать направление поиска отклонений от «стандартного» поведения. Думаю, мы все уйдем в machine learning рано или поздно, но уже и сейчас можно на простых выборках выявлять отклонения, а также фильтровать фолс.

CLOUD-ROBOT SOC

ЭКСПРЕСС-АНАЛИЗ «ГОТОВ ЛИ ВАШ SOC ОБЕСПЕЧИВАТЬ БЕЗОПАСНОСТЬ В ЦИФРОВОЙ ЭРЕ?»

Мой новый знакомый Cloud DevOps Василий каждый день до обеда готовит Cloud Formation скрипт, который после обеда сам создаёт в AWS десятки, а иногда и сотни серверов. Василий делает это не первый год, что наводит на мысль: кажется, мы не заметили революции, которая давно и как-то незаметно свершилась.

Мы привыкли мыслить скоростью изменений порядка 5–10 новых активов в сети в день, а их сегодня — десятки, сотни, а иногда и тысячи. Мы едва успели понять, что такое Cloud и DevOps по отдельности, а уже появились Cloud DevOps (Infrastructure as a Code), и теперь большинство традиционных SOC-практик резко устарели.

Но не так уж всё и плохо. Именно в России изменения ещё не очень заметны, поэтому

вполне есть несколько лет, чтобы подготовиться. Например, для начала оценить готовность своего SOC к новой цифровой эре. Для этого автор подготовил чек-лист, использующий наиболее популярные среди крупных мировых компаний практики и технологии (таблица 1).

Баллы начисляются следующим образом. За каждый ответ ① баллы не набавляем (0 баллов), за ответ ② — 2 балла, ответ ③ — 3 балла, ответ ④ — 4 балла, за ответ ⑤ — тоже 4 балла. После сложения полученных баллов ваш SOC можно отнести к одной из следующих категорий.

36–48 баллов — уровень Альфа — идёт в ногу со временем, иногда опережает. Автор подозревает, что это SOC Yandex или крупной мировой ИТ-компанияи.



Александр БОДРИК
Business Development Director
thecyberdock.com (Kubernetes security),
Managing Director
cyberlands.io (API pentest)

SOC Delivery

1 Сервисы SOC работают на основе	① Appliance ② VM ③ On-prem containers ④ Cloud (EC 2 etc) ⑤ Serverless
2 SOC применяет подход к сбору данных	① Собираем, что нужно для проверки политики ИБ ② + что нужно для комплаенса ③ + что нужно для антифрода ④ + что нужно для выявления кибератак ⑤ Всё собираем (data lake)
3 Наша 1-я линия	① Студенты ② Студенты, но есть структурированный курс обучения ③ Бывшие сисадмины ④ Бывшие сисадмины с курсом обучения ⑤ Робот «X», и ещё есть фоллоу-ап-робот «Маша»

SOC Cloud Control

4 SOC собирает логи	① Не собираем, смотрим Security Hub ② CloudTrail ③ Правильно настроенный CloudTrail ④ + VPC Flow / CloudWatch ⑤ + DNS/GuardDuty
5 SOC подключается к клиенту	① Даём инструкцию и образ виртуальной машины ② + авто поднимается VPN ③ + VPN встроен криптобиблиотекой ④ + инструкцию, как к нам открыть доступ внутри AWS ⑤ Саморегистрация через клиентский портал
6 SOC мониторит	① Смотрим Security Hub «глазами» по расписанию ② + UNIX, Windows — смотрим внутри EC 2 ③ + изменения конфигурации (политики логирования, AWS IAM) ④ + сетевые соединения и ищем аномалии ⑤ + редкие сервисы, как AWS Lambda

Таблица 1. Чек-лист от Александра Бодрика

25–35 баллов — уровень Бета — хороший задел, если год-два продолжать в том же темпе, то SOC будет готов к новым вызовам.

13–24 балла — уровень Гамма — классический on-premise SOC. Пора подумать о модернизации: поговорить с коллегами, куда будет двигаться компания, прикинуть, где брать людей, оценить готовность ранее приобретённых технологий к новой реальности.

До 12 баллов — уровень Дельта — поставленный в 2007 году под PCI DSS SIEM сложно назвать SOC. Может, пока использовать услуги внешнего SOC? Самостоятельный путь может занять 5–7 лет.

Что дальше? Допустим, решение о модернизации SOC принято. Вот что может сделать для повышения зрелости своего SOC представитель каждого из уровней.

Уровень Альфа. Вступить в клуб по интересам, обмениваться лучшими практиками. Например, вступить в telegram-группу cloud-robotsoc, подписаться на AWS Security Blog (<https://aws.amazon.com/blogs/security>).

Уровень Бета. Убедитесь, что у вас есть доступ к экспертизе Cloud DevOps, что ваш SOC в состоянии поспевать за auto-scaling-алгоритмами, что SOC плотно интегрирован со staging-средой и готовится к cloud remediation.

Уровень Гамма. Нужно выровнять стратегию развития SOC с планами как самой стратегии, так и конкретных заинтересованных сторон. Желательно выделить инновационную «песочницу» и начать отрабатывать в ней современные подходы к контролю цифровой среды и обнаружению атак.

Уровень Дельта. Выберите сервис-провайдера, который станет вашим гидом в мире CLOUD-ROBOT SOC, определите «низко висящие фрукты» с точки зрения их реализации и ценности для организации и последовательно меняйте способности своего SOC в лучшую сторону.

Путешествие в цифровую страну закончится хорошо не для всех. Тот, кто будет пассажиром, может оказаться высаженным по дороге, кто станет паровозом — получит много новых возможностей для познания, совершенствования и карьеры.

SOC DevOps Control

7 SOC узнаёт о новых активах	① Когда произошёл инцидент (при расследовании) ② + когда ИТ учло актив в CMDB ③ + прошёлся сканер ④ + актив создал сетевое соединение ⑤ Сразу, через AWS API
8 SOC умеет реагировать на инциденты	① Посылая письма контактному лицу ② + посылая краткие выдержки из инцидентов в Slack etc ③ + добавляя тикет в Jira ④ + генерируя CloudFormation template ⑤ + напрямую через AWS Lambda
9 SOC интегрирован в разработку	① Письмами при инцидентах ② + направляет предложения по совершенствованию процессов ③ + согласовывает действия по восстановлению по процедуре ④ + получает информацию о действиях во всех средах (staging) через AWS API ⑤ + автоматически восстанавливает безопасность сред разработки по заранее согласованным параметрам через AWS API

SOC Audit & Self-improvement

10 SOC проверяет свою эффективность (внутренне)	① Выполнение планов ② + выполнение метрик (MTTD/MTTR) ③ + Atomic Testing ④ + Purple Team ⑤ + сравнение своего времени реагирования и времени реагирования DevOps на инциденты доступности (SRE)
11 SOC проверяет свою эффективность (внешне)	① Не проверяет ② + аудит на соответствие общим стандартам 27к/SOC 2 Type II ③ + участие в киберучениях (например, PHD) ④ + аудит зрелости SOC ⑤ + RedTeam
12 SOC обучает персонал	① Практикой ② + есть модель компетенций, на основе которой происходит набор новых людей ③ + есть планы по развитию (книжки и курсы) ④ + есть собственные структурированные курсы и практические занятия ⑤ + есть киберполигон

Таблица 1. Чек-лист от Александра Бодрика (продолжение)



**Денис
БАТРАНКОВ**
эксперт
BIS Journal

Зрелость SOC принято оценивать по его трём основным составляющим: технологиям, процессам и людям. Александр привёл интересный чек-лист самооценки для SOC, использующего облачные технологии компании Amazon. Действительно, Amazon задаёт ориентир для всего ИТ-рынка. Например, вычисления без выделения серверов и управления ими на основе AWS Lambda для многих пока остаются проектами из будущего. При этом новые технологии как улучшают KPI, по которым бизнес оценивает эффективность SOC, так и приносят новые трудности. Например, сейчас контейнеризация — это основная головная боль у служб безопасности.

На самом деле зрелость SOC оценивают по паре сотен различных параметров, и лучше всего это делают профессиональные аудиторы, которые сами занимаются построением SOC. Готовый анализ покажет, на каком уровне развития находятся процессы, люди и технологии, и даже прольёт свет на слепые пятна, которые мы не замечаем, увлекшись текущими задачами. И это очень ценно. Возможно, вам нужно запустить новый процесс, например, кадровый, чтобы постоянно мониторить выгорание аналитиков и готовить им смену к тому моменту, как они захотят перейти на новую должность.

Ниже проиллюстрирую список процессов и процедур, которые должны быть в SOC (рис. 1). Их число превышает сотню; они относятся и к работе с технологиями и бизнес-процессами, и к архитектуре, и к методам аналитики, и к операционной деятельности.

Например, для повышения эффективности каких-то SOC придётся переделывать организационные процессы и нанять людей, живущих в другом часовом поясе, чтобы передавать вечернюю смену им, потому что они выспались и у них уже настало утро.

Если оценивать зрелость процессов по метрике CMMI, которая гласит: 1 — это хаотичное исполнение задач, причём всегда по-разному, а 5 — это

самооптимизирующийся процесс, — реальная оценка многих SOC будет находиться в районе 2–3: задачи определены, а новичок знает, где прочитать описание процесса, и может повторить его за лучшим экспертом компании. Например, результат аудита зрелости SOC может выглядеть как на рис. 2.

Имея такую оценку по каждому компоненту вашего SOC, вы понимаете, что нужно улучшать.



Рисунок 1. Процессы и процедуры, которые должны быть в SOC

Направления развития	Оценка	Комментарий
Люди	1,23	
Основные	1,55	Создание команды еще ведется и не закончено
Обучение	1,00	Обучение аналитиков начато, нужно больше документации
Оценка навыков	1,00	Нехватка кадров
Карьерный рост	1,00	Нехватка кадров
Лидерство	1,60	Нужно четкое определение полномочий и зон ответственности
Процессы	1,90	
Основные	2,00	Хорошо документировано, но сфокусировано на работе с событиями, а не атаках
Операционные	1,94	Документация разрознена, ее трудно найти
Аналитические	1,83	Нужна более полная база Threat Intelligence
Бизнес	1,84	Релизовать процесс общего взаимодействия через wiki
Технологии	2,08	
SIEM	2,08	Зрелый ИТ процесс и процедура поддерживающая развертывание
Архитектура	2,83	Самый зрелый процесс SOC
Корреляция	1,30	Еще происходит наработка контента
Технологии безопасности	1,94	Анализ поведения сотрудников еще не включен и срочно требуется
Управление жизненным циклом информации	2,23	Архивирование информации работает и хорошо документировано
Общий уровень зрелости	1,74	

Пример оценки зрелости SOC

Рисунок 2. Пример оценки зрелости SOC

ПОЧЕМУ ВАМ НУЖЕН ВНЕШНИЙ SOC?

НАБОР АРГУМЕНТОВ ОТ «ИНФОРМЗАЩИТЫ»



Иван МЕЛЕХИН
директор Центра
мониторинга
и реагирования
на киберугрозы
IZ: SOC компании
«Информзащита»

В нашем технологически ориентированном мире каждый бизнес, независимо от его размера, прилагает особые усилия для защиты своих конфиденциальных данных. Эти данные могут касаться персонала, клиентов, деловых партнеров, внутренних операций и многого другого. Но с ростом числа изолированных и целенаправленных кибератак стало сложно обеспечить безопасность инфраструктуры. Даже вероятность стать жертвой нападения возросла за последние несколько лет.

СОГЛАСНО СТАТИСТИКЕ

Согласно статистике нашего Центра мониторинга и реагирования на киберугрозы IZ: SOC, количество регистрируемых инцидентов возросло на 36% по отношению к началу 2020 года. Современным компаниям постоянно приходится работать над поиском надежных защитных стратегий от кибератак. Некоторые полагаются на себя и внедренные продукты, в то время как другие передают услуги по кибербезопасности на аутсорсинг в коммерческие SOCи.

БУДНИ

Типичные будни коммерческого Центра мониторинга и реагирования на киберугрозы (SOC) выглядят примерно так: часов в десять вечера, в бесконечном потоке легитимных DNS запросов движок TI отлавливает обращение на C&C сервер какого-нибудь очередного клона WannaCry. Аналитик, сделав дежурную проверку на false positive и увидев некоторые странности в логах, эскалирует инцидент на уровень выше. Аналитик второй линии подтверждает высокую вероятность угрозы и сообщает об

инциденте заказчику. Заказчик не реагирует. Во-первых, потому что в десять вечера у него просто некому реагировать. Во-вторых, потому что WannaCry — это что-то из аналитических обзоров и презентаций и никак не может случиться в реальной жизни.

В лучшем случае, утром следующего дня команда внешнего SOCа получит от клиента сообщение, что подозрительный компьютер выключен и отправлен на переустановку. Только профессионализм и настойчивость специалистов центра реагирования, подключивших все возможные ресурсы, от сервис-менеджера до руководителя, не позволит спустить историю на тормозах. Заказчик, пройдя через стадию отрицания и сомнения до принятия факта и уровня опасности, согласится на предложенный план реагирования и проведет необходимые действия, чтобы предотвратить эпидемию в самом начале, еще до закрепления вредоносных программ в инфраструктуре компании.

SOC НУЖЕН

Возможен ли такой сценарий со своим SOCом? Конечно, если вы большая богатая компания. Таких компаний, где масштаб проблемы соотносится с возможностями их решения, не так много.

Я как директор Центра мониторинга и реагирования на киберугрозы IZ: SOC общаюсь с большим количеством представителей служб информационной безопасности компаний разного размера и разных секторов экономики. Существенная часть из них (согласно нашему исследованию 43%) считает, что SOC должен быть своим. 23% рассматривают вариант с внешним SOCом, и у 14% он уже есть. То есть, больше 80% компаний к настоящему времени не сомневаются в том, что SOC нужен.

Разногласия начинаются в вопросах: «зачем?» и «какой?».

РАЗ, ДВА, ТРИ

Во-первых, сейчас мы наблюдаем результаты волны маркетинговой популярности SIEM — систем сбора, обработки и хранения событий информационной безопасности. В свое время

Согласно статистике нашего Центра мониторинга и реагирования на киберугрозы IZ: SOC, количество регистрируемых инцидентов возросло на 36% по отношению к началу 2020 года

считалось, что SIEM чуть ли не серебряная пуля, обладать которой должна любая уважающая себя служба ИБ, после установки которой все хакеры разбегаются, только услышав название того или иного именитого вендора. Это не соответствует действительности. После полутора — двух лет эксплуатации приходит понимание, что SIEM всего лишь инструмент, причем крайне сложный и затратный в содержании и использовании.

Во-вторых, многие заказчики, которые находятся на начальной стадии строительства своих центров мониторинга, недооценивают сложность, бюджет и сроки, необходимые для достижения такого уровня зрелости ИБ, при котором сценарий реагирования внешнего SOCa, описанный в начале статьи, будет будничной рутиной внутреннего центра.

В-третьих, нет, к сожалению, четкого универсального определения, что, собственно говоря, есть SOC, какой функционал он может и что от него ожидать.

БАЛАНС

На самом деле, и поставщики услуг, и заказчики прекрасно понимают, что нужно делать для выявления и предотвращения атак и киберинцидентов. Вопрос заключается в балансе между реализацией функционала своими и внешними силами и финансовыми затратами на поддержания этого баланса. При этом, хочу отметить, что точка нахождения этого баланса не обязательно должна быть фиксирована. Скорее наоборот: с ростом зрелости информационной безопасности компании силы могут плавно смещаться в то или иную сторону. Например, выбирая стратегическое направление на строительство своего внутреннего SOCa и трезво отдавая себе отчет, что срок реализации такого проекта может доходить до двух лет, можно на это время часть функций отдать внешнему поставщику услуг, договорившись постепенно переводить функционал в службу ИБ компании, не теряя уровня сервиса.

ПРИДЕТСЯ ПЛАТИТЬ

Так, начав с полноценного внешнего SOCa, который реализует всё, начиная с мониторинга событий безопасности первой линией и заканчивая проведением расследований киберинцидентов третьей линией, вы можете по мере готовности переводить обработку инцидентов на вашу SOAR\IRP систему, забирать на себя часть функционала 1–2–3 линий аналитиков, постепенно внедрять свой конвейер

Даже бесплатные пилоты SOCa длительностью не больше месяца могут вскрыть огромный пласт задач и проблем в части реализации функций ИБ, взаимодействия с ИТ и внешними подрядчиками

сбора, обработки и хранения логов. Нельзя забывать и о том, что внешний MSSP SOC, придя к вам в инфраструктуру, автоматом принесет с собой политики настройки источников событий и аудита, рекомендации по составу источников данных, методы по централизованному сбору событий и огромный пул сценариев и правил корреляции. За все это вы будете вынуждены платить ресурсами или деньгами во время строительства внутреннего SOCa, а оценить качество и эффективность получится только через 2–3 года после начала эксплуатации.

ПОХОЖЕ НА ТЕСТ-ДРАЙВ

На рынке информационной безопасности присутствует множество поставщиков MSSP услуг, и вы, как при покупке автомобиля, можете попробовать разные машины, причем в режиме не часового тест-драйва, а реальной эксплуатации перед тем, как купите свою. Возможно, что в процессе вы поймете, что в условиях современного мира внешний сервис сравним по затратам и существенно эффективнее по качеству, чем свое собственное решение.

* * *

Итак, строите ли вы свой SOC, являетесь ли сторонником внешних сервисов или гибридной модели — взаимодействие с внешним центром мониторинга и реагирования на киберугрозы будет для вас полезным. Даже простое пилотирование одного или двух внешних SOCs уже даст понимание не только в различиях подходов, но и в том, что, собственно, вы хотите получить. Даже бесплатные пилоты SOCa длительностью не больше месяца могут вскрыть огромный пласт задач и проблем в части реализации функций ИБ, взаимодействия с ИТ и внешними подрядчиками, а также открыть ландшафт угроз и рисков в новой перспективе. Всё это само по себе дает отличный толчок к развитию информационной безопасности в компании на много лет вперед.

**Артём СЫЧЁВ**

первый заместитель
директора Департамента
информационной
безопасности Банка России

ДЛЯ ЧЕГО ВВОДЯТСЯ РИСК-ПРОФИЛЬ И КИБЕРУЧЕНИЯ

МЕНЯЮТСЯ КРИТЕРИИ ОЦЕНКИ, ФОРМАТ ПРОВЕРОК И ФОРМЫ ОТЧЁТНОСТИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Банк России совершенствует обеспечение информационной безопасности финансовой сферы по нескольким направлениям. Среди ближайших нововведений — новые форматы оценки и проверки подведомственных организаций: риск-профиль и киберучения. Новшества будут отражены в изменении системы подготовки кадрового обеспечения отрасли.

НАПРАВЛЕНИЯ УЛУЧШЕНИЙ

Банк России, государственный регулятор информационной безопасности финансовой сферы, нацелен на совершенствование отрасли по трём направлениям:

- ♦ совершенствование корпоративного управления вопросами информационной безопасности;
- ♦ осознание и оценка того, насколько финансовая организация может обеспечивать свою операционную надёжность;
- ♦ улучшение кадрового потенциала, подготовки и переподготовки специалистов служб информационной безопасности.

Таковы ближайшие планы, работа по их осуществлению ведётся. Внесены некоторые коррективы в базовый документ Положение Банка России № 382-П от 9 июня 2012 г. Дорабатываются новые инструменты надзорной деятельности: риск-профиль и киберучения.

ФОРМАТ ОЦЕНКИ — РИСК-ПРОФИЛЬ

Риск-профиль — новый важный формат для оценки уровня обеспечения информационной безопасности финансовых организаций. Много о нём уже хорошо известно. Эта тема предварительно обсуждалась на XII Уральском форуме «Информационная безопасность финансовой сферы» в феврале 2020 года.

Остановиться следует на том, на что влияет риск-профиль и как в ближайшем будущем будет складываться надзорная деятельность в сфере информационной безопасности. Учитывая, что риск-профиль уже рассчитывается не только

для кредитных, но и для некредитных организаций: пенсионных фондов, страховых компаний, других крупных инфраструктурных участников финансового рынка и т.д.

Основой для формирования риск-профиля является информация, поступающая в Банк России по нескольким каналам.

Это, во-первых, отчётность по 203-й форме об операциях, совершаемых без согласия клиентов в рамках Национальной платёжной системы.

Во-вторых, информация об инцидентах, приходящая от банков и нефинансовых организаций по линии АСОИ ФинЦЕРТ.

Эта база будет развиваться — расширяться и усложняться. Новых форм отчётности для банков не появится. Поступающая в АСОИ информация будет рассматриваться с точки зрения дата-центричности, чтобы автоматически обрабатываться. Отчётность будет рассматриваться с точки зрения не только технической, но и экономической составляющей и перепроверяться.

На сегодняшний день финансовые организации обязаны сообщать в Банк России обо всех инцидентах информационной безопасности. До сих пор соответствующей формы отчётности не существовало. Предстоит сделать этот поток сообщений о событиях информационной безопасности обязательным, утвердив форму отчётности.

В основе риск-профиля лежит необходимость для Банка России понимать, насколько финансовая организация готова противостоять инцидентам в сфере ИБ, а также учитывать, в какой степени у неё достаточно ресурсов для покрытия возможного ущерба.

ОТ ТЕХНИКИ К УПРАВЛЕНИЮ

Это путь постепенного отхода от сосредоточения на чисто технических вопросах обеспечения информационной безопасности поднадзорными организациями. Наши коллеги, приходя с проверками в финансовые организации, иногда углубляются

в такие вопросы: какие антивирусы стоят, как настроены, в работу со средствами криптографической защиты.

Чрезмерно погружаясь в технические детали, можно не заметить принципиальных проблем, которые способны возникнуть у финансовой организации, но находятся не в зоне технических специалистов, а на уровне руководства.

Одна из главных задач, решаемых государственным регулятором при формировании риск-профиля, — перенос акцента с технических моментов обеспечения информационной безопасности на управленческие вопросы. В центре оказывается качество корпоративного управления, а также наличие у финансовой организации достаточных ресурсов, чтобы преодолеть кризисную ситуацию в случае возникновения проблемы.

Проблемы могут быть разными: хищение денежных средств, нарушение устойчивости работы информационной инфраструктуры, непредоставление важного и нужного сервиса клиентам. Предметом оценки является способность финансовой организации обеспечить непрерывность, бесперебойность и операционную надёжность своего функционирования.

Со стороны Банка России надзорный процесс перестанет быть привязан к оценке чисто технических составляющих. В центре внимания оказывается готовность финансовой организации противостоять угрозам, её реальная защищённость.

МЕТОДОЛОГИЯ ПРОВЕРОК — КИБЕРУЧЕНИЯ

Готовится новая методология проверки, идущая на смену обычным проверкам. Это киберучения. Первое в пробном режиме начнётся в октябре, несколько запланировано до конца 2020 года. В дальнейшем эта практика будет расширена.

Методология киберучений прорабатывалась с несколькими участниками финансового рынка и отражает коллективную позицию, а не только точку зрения Банка России. Документ станет доступным для всех участников финансового рынка. Процесс внедрения киберучений будет не закрытым, а публичным.

Первая задача киберучений — оценить защитные возможности, моделируя стрессовую ситуацию. Понять, насколько финансовая организация готова к отражению такой атаки.

Вторая задача — проверить, в какой степени она готова локализовать проблему, предотвратить дальнейшее развитие инцидента.

Задача третья — выявить ресурсы финансовой организации для предотвращения либо устранения последствий инцидента.

Все три перечисленных момента складываются в единую общую задачу. Понять, как конкретная атака, инцидент может повлиять на устойчивость функционирования финансовой организации. По итогам проверочной деятельности при выявлении серьёзных проблем будут приниматься меры реагирования.

На первом этапе это будут командно-штабные учения, то есть никаких информационных атак на финансовые организации генерироваться не будет.

Методология киберучений прорабатывалась с несколькими участниками финансового рынка и отражает коллективную позицию, а не только точку зрения Банка России. Документ станет доступным для всех участников финансового рынка

ОБНОВЛЕНИЕ КОМПЕТЕНЦИЙ КАДРОВ

Формат киберучений — моделирование атак определённого типа и отслеживание последовательности действий служб информационной безопасности. Например, в случае распространения злоумышленниками вредоносного программного обеспечения — вируса, шифрующего данные.

Важно проверить, насколько и на каком этапе проверяемая организация сумела его выявить. Начал ли вирус-шифровальщик распространяться по корпоративной сети, какую работу успел проделать, какие действия, в какой последовательности и кем были предприняты, чтобы локализовать инцидент и устранить последствия. Будет проводиться оценка ущерба и сроки восстановления полноценной работы организации.

Методология киберучений идёт не от произвольного набора инструментов, типовых уязвимостей в технологиях. Перед началом стресс-тестирования крайне важно понимать бизнес-модель работы банка. На её базе формируется представление о сопутствующих рисках, уязвимостях и типах атак, которые могут быть использованы.

Проверки будут проводиться не по единой для всех схеме. Только с учётом особенностей бизнес-процессов и технологий реальных конкретных финансовых организаций.

Это не очень легко и для Банка России, и для проверяемых организаций. Потребуется перестройка всего механизма и надзорной деятельности, и работы подразделений информационной безопасности финансовых организаций.

Их сотрудникам теперь придётся отвечать на вопросы не только исключительно технические, но и связанные с бизнес-деятельностью. Для чего надо будет выстраивать отношения как с коллегами в информатизации, так и с руководителями, участвующими в управлении кредитной организацией.

Испытание будет непростым. Специалистам по информационной безопасности надо будет учиться выстраивать обратную связь: доносить свои мысли до руководства и получать ответы по существу.

Эти новые актуальные компетенции учитываются в разработке профессионального стандарта специалиста в области информационной безопасности. Можно надеяться, что в 2021 году этот документ будет утверждён, что приведёт к изменению учебных программ, проведению курсов повышения квалификации.



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

ЗАЛЕЗЬ В ЯЩИК... ПАНДОРЫ!

РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД — ЭТО
О ТОМ, КАК НЕ ВЫПОЛНЯТЬ ТРЕБОВАНИЯ,
ИЛИ СОВСЕМ НАОБОРОТ?

С 01.01.2018 кредитно-финансовые организации свободно могут пользоваться, казалось бы, ключом от ящика Пандоры — разделом 6.1 ГОСТ Р 57580.1–2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер».

ЧТО ТРЕБУЕТ РЕГУЛЯТОР:

И Банк России, и ФСТЭК требуют от подконтрольных организаций осознанных и обоснованных решений в области защиты информации.

А КАК ЖЕ МЫ РАНЬШЕ РАБОТАЛИ?

Долгое время можно (и нужно) было просто чётко выполнять все установки того же семейства стандартов СТО БР ИББС «Обеспечение информационной безопасности организаций банковской системы Российской Федерации», Приказов ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» или от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и, в общем, не сильно задумываться о том, насколько они необходимы и достаточны в конкретной организации, адекватны и соразмерны масштабам, специфике её деятельности.

Справедливости ради надо отметить, что и тогда указанные документы предусматривали возможность некоторой настройки лежащих в их основе лучших практик под конкретную ситуацию — например, с помощью оценки актуальности угроз безопасности¹.

¹ См. «Методику определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждённую заместителем директора ФСТЭК России 14.02.2008.

Вполне можно было² построить модель угроз и нарушителя и именно под них подобрать комплекс мер и средств защиты. Однако построение полноценной модели угроз и нарушителя для всей организации и даже для отдельной автоматизированной системы (во всяком случае, такой, с которой потом можно работать и реально на её базе делать какой-то математически обоснованный прогноз) — дело нетривиальное и требующее больших компетенций и ресурсов, поэтому подавляющее большинство организаций вполне устраивал предлагаемый регуляторами набор требований, лишь бы в эти дебри не лезть.

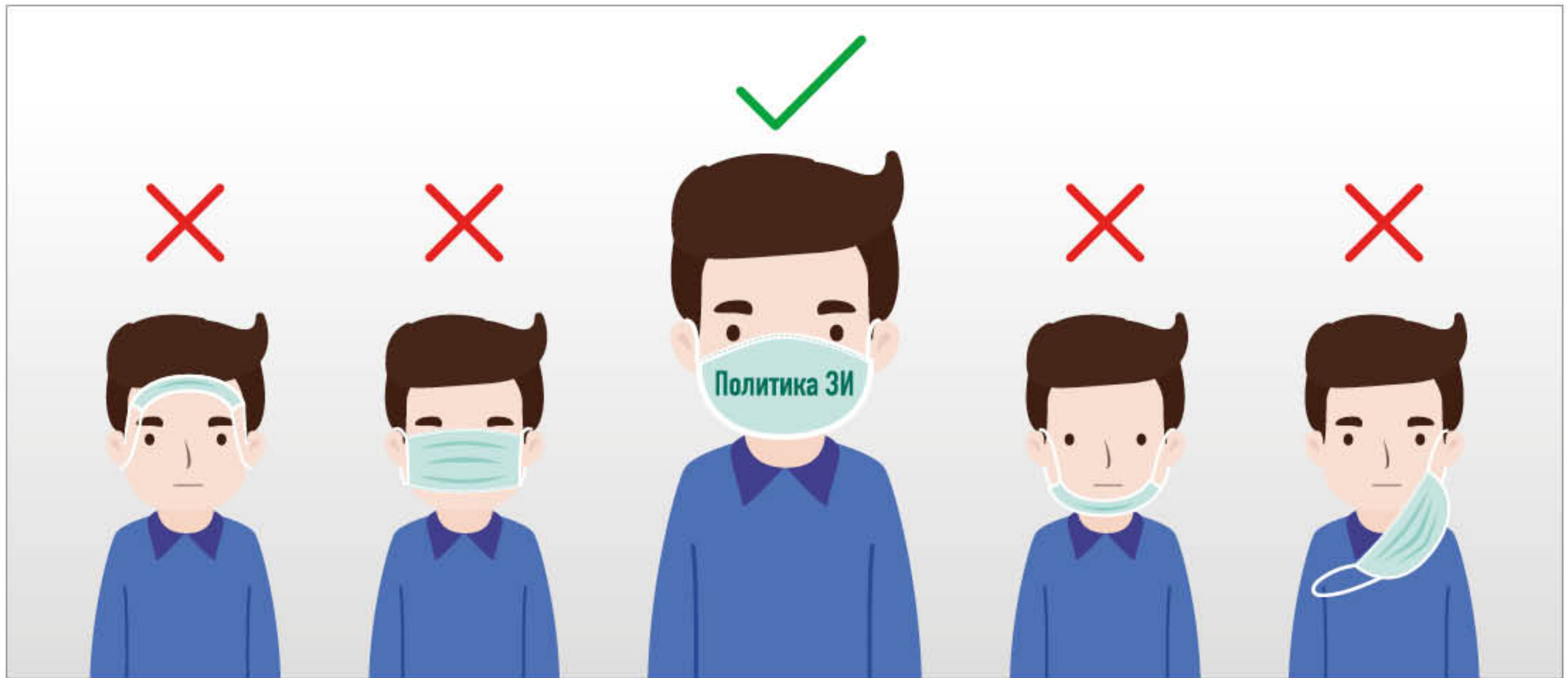
А ПОЧЕМУ СЕЙЧАС ТАК НЕЛЬЗЯ?

Можно. Можно просто выполнять базовый набор требований. У регуляторов он такой подробный и большой, что если удастся его реализовать весь, то в подавляющем большинстве случаев этого будет достаточно.

Только при этом надо помнить, что безопасность уже давно не «бумажная». Это значит, что номинально утвердить в организации типовой комплект нормативных актов, в которых будут декларироваться «правильные вещи», уже будет недостаточно, чтобы набрать баллы, например, на рекомендованную Банком России оценку³ по результатам очередного аудита. Методики проверки изменились (и началось это не с ГОСТ Р 57580.2–2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика

² См. СТО БР ИББС-1.0–2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» раздел «Исходная концептуальная схема (парадигма) обеспечения информационной безопасности организаций банковской системы Российской Федерации» п. 5.7 и далее.

³ См. п. 11.4 СТО БР ИББС-1.2–2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0–2014».



оценки соответствия», а с требований категории 3 в Положении Банка России от 09.06.2012 № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»), теперь без практики и свидетельств деятельности «на троечку», которой надо соответствовать в 2021-м⁴, не вытянуть.

А ПОЧЕМУ ПРОСТО НЕ ПРИНЯТЬ РИСКИ НЕВЫПОЛНЕНИЯ ВСЕХ «НЕУДОБНЫХ» ТРЕБОВАНИЙ?

Аналогично тому, почему нельзя до бесконечности заматывать мусор под ковёр. Формально, конечно, можно выбрать и такую стратегию. Но тогда придётся резервировать много средств на случай не «если», а «когда» принятые риски реализуются.

Изменился ландшафт цифрового мира. С тех пор как в него переместились большие деньги и вообще большие рычаги управления, в нём всё стало масштабнее, быстрее, серьезнее — потенциал злоумышленника, разнообразие угроз, неотвратимость их реализации, последствия (финансовые и репутационные, конечно, а не ответственность по статьям 13.12 и 19.5 КоАП

РФ, про которые вспоминают чаще всего только при оценке регуляторных рисков). Уже давно вопрос не в том, реализуется ли атака, а в том, когда она реализуется; не в том, удастся ли её предотвратить, а как быстро и с какими потерями удастся её остановить.

Создание и поддержание таких резервов рискует оказаться затратнее реализации соответствующих мер защиты, чего, скорее всего, и надо регулятору, чтобы заставить сообщество думать, оценивать, выбирать, а не закрывать проблемы формальными бумагами (не хочется называть их «отписками»).

ТО ЕСТЬ, КОГДА СТАЛО МОЖНО НЕ СОБЛЮДАТЬ ТРЕБОВАНИЯ, ОКАЗАЛОСЬ, ЧТО ЭТО УЖЕ НИКОМУ НЕ НУЖНО?

Да, получается так. Своего рода «вредные советы» от регулятора. Сейчас сами организации стали заинтересованы в том, чтобы эффективно защитить свои информационные технологии и ресурсы оптимальным образом не для регулятора, а «для себя». Пришли к тому, чтобы искать, что именно нужно реализовать, а не «можно не делать». В кредитно-финансовой сфере сейчас наблюдается переход организаций на новый уровень зрелости процессов защиты информации. Вступившее в силу Положение Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе» и находящийся в разработке проект стандарта управления риском реализации информационных угроз скорее являются ответом на запрос и потребности сообщества, чем навязанной опережающей нормой.

⁴ См. п. 9.2 Положения Банка России от 17.04.2019 № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента» с учётом информационного письма Банка России от 14.05.2020 № ИН-014-56/88 «О неприменении мер в связи с коронавирусной инфекцией (COVID-19)».

**Константин МАРКЕЛОВ**

заместитель директора по развитию бизнеса, руководитель R&D компании ОТП, председатель комитета АРБ по информационным и интернет-технологиям, кандидат физико-математических наук

**Валерий ШИПИЛОВ**

исполнительный директор Ассоциации российских банков, кандидат технических наук

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ В БАНКАХ КАК НЕИЗБЕЖНОСТЬ

И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК СРЕДСТВО РАЗВИТИЯ БАНКИНГА

Бизнес банков и клиентское обслуживание перемещаются из офисов и операционных касс в так называемое цифровое пространство. Появляются online-банки, функционирующие без офисов. При этом постоянно увеличивается потребность клиентов в цифровых финансовых сервисах, в том числе предоставляемых через интернет и мобильные приложения и позволяющих экономить значительные объёмы времени и денежных средств. Возрастают требования клиентов не только к перечню, но и к качеству банковских сервисов. Теперь уже банкам для поддержания своей конкурентоспособности нужно формировать индивидуальные предложения для каждого клиента.

И, как следствие, приходит осознанная банками необходимость трансформации своих бизнес-моделей и информационной архитектуры.

ОТ ДОКУМЕНТОЦЕНТРИЧНОСТИ К ДАТА-ЦЕНТРИЧНОСТИ

Трансформация бизнес-моделей — это в первую очередь предоставление финансовой услуги не в офисах банка, а там и тогда, где и когда такая услуга востребована клиентом. Это может

быть как чисто финансовая услуга (например, банковский перевод), так и часть комплексной услуги (например, покупка автомобиля за счёт кредита или оплата ЖКХ).

Суть же цифровой трансформации — это переход от документоцентричности деятельности к дата-центричности.

Сейчас большинство банков ориентированы на финансовые документы (платёжные поручения, кредитные договоры, гарантии и др.).

Основной актив цифровой организации — это её данные. Дата-центричность предполагает учёт не только цифр (счетов, проводок, документов), но также их семантического смысла, т.е. должно быть единство формы и содержания.

В ЦЕНТРЕ — КЛИЕНТ

Именно такой подход позволяет сделать клиента центром банковской деятельности, привязать к нему не только историю использования клиентом предоставляемых банком услуг, но и прогнозировать его поведение, выявлять клиентские потребности и предпочтения, вырабатывать рекомендации для принятия оптимальных решений со стороны клиента.

В части организационной культуры при цифровой трансформации необходим переход от функциональных исторически сложившихся подразделений к кросс-командам, объединяющим бизнес, ИТ и маркетинг.

Банки должны приспосабливаться к изменениям внешней среды, создавая или вливаясь в так называемые финансовые экосистемы — динамичные и совместно развивающиеся сообщества, состоящие из разнообразных субъектов,

Банки должны приспосабливаться к изменениям внешней среды, создавая или вливаясь в так называемые финансовые экосистемы — динамичные и совместно развивающиеся сообщества

создающих и получающих новое содержание в процессе как взаимодействия, так и конкуренции.

Но главное — банки должны сделать своих клиентов частью этой экосистемы.

ИИ КАК ДВИГАТЕЛЬ РАЗВИТИЯ

Для реализации сказанного выше необходима цифровая финансовая платформа, предусматривающая повсеместное внедрение основных трендов развития информационных технологий. И главным средством развития и наиболее передовой составляющей частью цифровой трансформации, конечно же, является искусственный интеллект (ИИ).

По ИИ написано достаточно много работ. В качестве свидетельства его противоречивости можно привести пример технологии IBM Project Debater, которая может участвовать в качестве ИИ в различных дискуссиях. По этой технологии был создан проект, в который было занесено порядка тысячи рефератов и научных статей студентов и молодых учёных. С одной стороны, результат показал, что ИИ не способен принимать моральные решения, потому что мораль — уникальная способность и черта человека. Поэтому если ИИ применять широко, то он может быть опасен. Но, с другой стороны, он может взять на себя часть рутинных функций и дать людям больше свободного времени. ИИ спорит как бы сам с собой.

ДВА ПОДХОДА И БОЛЕЕ

Существуют два подхода к развитию ИИ. Первый, традиционный, — это повтор человеческих возможностей. Второй — это создание оригинального машинного ИИ.

При традиционном подходе необходимо переложить способности человека в программный код. Здесь главной задачей является распознавание и обработка графических и звуковых образов, так как основную массу информации о внешнем мире человек получает через зрение и слух. Реализуя традиционный подход, освобождаем человека от рутинных действий — для творчества и аналитики. Главное в этом подходе — не написание алгоритмов, а умение увидеть и правильно поставить прикладную задачу.

Второй подход — инновационный. Он более рискованный. Это когда роботы с ИИ начнут на определённом этапе самостоятельно обучаться и обучать себе подобных. И в этом случае человек становится лишним звеном в цепочке эволюции? Не хотелось бы...

На стыке обоих подходов можно говорить о создании универсального ИИ, правда, с большой оговоркой. Он должен решать широкий круг задач, но функционировать только в закрытых

средах, где существуют определённые правила поведения и конечный набор состояний. То есть универсальный ИИ может измеряться не способностью достигать сложных целей в широком диапазоне изменчивости внешней среды, а эффективностью приобретения навыков.

Также можно говорить об узком ИИ, который применяется для узких прикладных задач. Чем уже эта задача, тем более эффективными могут быть ИИ-решения. Например, распознавание документов — это узкий ИИ.

Основные алгоритмы распознавания визуальных образов и обучения машин были придуманы ещё лет 50–70 назад. Но эти адаптивные алгоритмы нужно было хорошо «обучать» не только на больших выборках, но и быстро. Однако вычислительных мощностей того времени для этого не хватало.

Сейчас эти алгоритмы вполне реализуемы и востребованы.

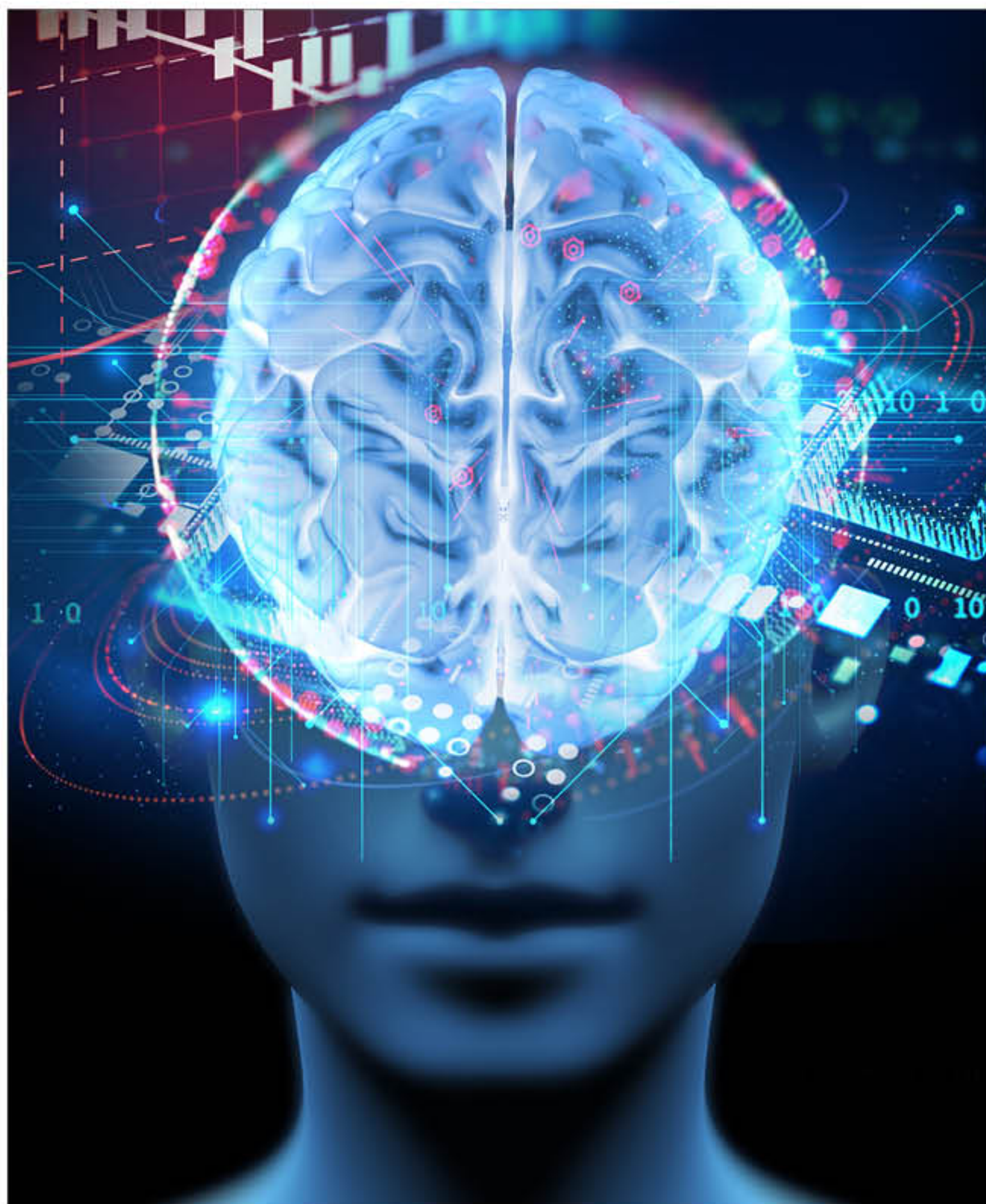
ПРИМЕРЫ РОБОТИЗАЦИИ

Внедрение элементов ИИ в повседневную жизнь происходит не так быстро, как того хотелось бы. Но это болевая точка любой молодой технологии, любого революционного новшества. Однако, даже невзирая на новизну применяемых алгоритмов, программы уже способны воспроизвести множество функций, которые ранее выполняли люди.

Например, роботизация коснулась самых обыденных операций в работе финансовых организаций, а именно тех, которые требуют больших временных затрат, но просты по сути и дают на выходе небольшую добавленную стоимость. Приведём несколько примеров:

1) При анализе кредитозаёмщика необходимо автоматически проанализировать его социальный интернет-профиль, получить информацию из государственных организаций, проверить документы на их действительность. Затем — собрать всю информацию о заёмщике воедино и проранжировать его по доходности, надёжности, риску. Это уже могут делать программные роботы.

2) Обработка потоков бумажных документов: счёта-фактуры, акта выполненных работ, акта сверки, товарных накладных, универсальных передаточных документов. Эту «бумагу» необходимо отсканировать, распознать, разнести по учётным регистрам, сделкам и договорам. Это также уже умеют делать роботы, не те же самые, а другие — программные роботы всегда имеют узкую специальность. При этом участие человека ограничивается исключительно только теми документами, которые робот не распознал или в которых робот «сомневается».



3) Большинство российских банков уже задумываются о перспективах замены живых операторов клиентской поддержки чат-ботами. Роботы становятся незаменимыми там, где нужно проинформировать клиента о продуктовой линейке или помочь корректно заполнить реквизиты, сориентироваться в навигации по сайту или предупредить о сроках платежа.

4) Если речь идёт о внутренних бизнес-процессах в банке: чаще всего это касается доработки потока бумажных документов, выгрузки выписок, переноса данных из одной системы в другую и пр.

5) Параллельно активное применение получают программы, позволяющие оценивать качество общения с клиентом. Роботы научились реагировать не только на определённые ключевые слова, но и в целом анализировать (по целому ряду параметров) поведение сотрудников при беседе с клиентом. Ну а отслеживание удовлетворённости клиента конкретной услугой было едва ли не первым направлением роботизации, причём не только и не столько в финансовой сфере.

РОБОТЫ-КОЛЛЕКТОРЫ

В качестве ещё одного примера из перспективных направлений внедрения роботизации, имеющего и большую социальную значимость, приведём общение с должниками.

Для этого банки разрабатывают специальные программы — роботов-коллекторов.

В чём преимущества роботизации при работе с должниками? Они лежат на поверхности: деятельность коллекторов — один из наиболее чувствительных в социальном плане сегмент финансового рынка.

Достаточно вспомнить, сколько внимания и СМИ, и чиновники всех ветвей власти уделяли проблеме общения коллекторов с должниками, сколько жалоб на действия коллекторов поступало от граждан. Сегодня, после того как профильный закон чётко определил границы дозволенного в общении с должниками, процедуру взыскания долга удалось описать машинным языком, задав строгие скрипты общения с гражданами. И эти программы не просто робот-магнитофон, способный позвонить должнику и выдать стандартный набор шаблонных фраз. ИИ выбирает следующую фразу на основе анализа полученного от собеседника ответа, анализирует эмоции абонента, однако сам не подвержен эмоциям и, следовательно, избавлен от нервных срывов, а в результате и от жалоб на некорректное поведение.

СФЕРЫ ПРИМЕНЕНИЯ

Роботизация позволяет высвободить миллионы человеко-часов и сэкономить финансы. Недавно один крупный банк заявил, что экономит до ста миллионов рублей ежегодных расходов с помощью роботизации рутинных процессов. Современные технологии настолько искусны, что не требуют перестройки всей системы, будь то внутренние процессы в компании или коммуникация с клиентами, — они научились дополнять функционирование, например, всей ИТ-инфраструктуры, не нарушая основы её работы. Словом, действуют почти как человек. При этом машины работают без перерывов на обед и сон, а количество ошибок только снижается. Робот, в отличие от человека, не наступает на одни и те же грабли дважды и не подвержен эмоциональным всплескам. Роботизация в работе банков привела к тому, что появились новые специальности, например оператор чат-ботов — сотрудник, основные обязанности которого состоят в регулярной отладке программного обеспечения под актуальные запросы регуляторов или клиентов. Важно то, что сфера применения машинного интеллекта постоянно расширяется — по мере развития алгоритмов.

Всё активнее в кредитных организациях применяются элементы ИИ:

1) **Платежи и переводы.** Например, клиент при включённом мобильном приложении просто голосом говорит, что хочет отправить деньги «Маме!», или «Сыну за учёбу», или «Дочери на мобильный телефон», и этого достаточно, чтобы платёжное поручение было сформировано. Далее идёт только подтверждение на выполнение операции, а всё остальное делает ИИ.

2) **Планирование и управление активами.** Здесь ИИ может вести алгоритмическую торговлю, заключая по несколько сотен сделок в секунду, что недоступно человеку; главное — правильно отладить алгоритмы. Также на основе фундаментального и технического анализа курсов ценных бумаг (это уже большие данные) можно давать рекомендации по изменению составляющих портфеля.

3) **Управление рисками.** До управления операционными рисками ИИ пока не добрался, а вот что касается финансовых и кредитных рисков — здесь обширная область его использования. Ведь банковская деятельность — это искусство управления в координатах «риск — доходность». Кто-то из банков ведёт рискованную политику и этим повышает свою доходность (главное — не выходить за рамки действующих нормативов), а каким-то банкам категорически нельзя приближаться к нормативным пределам риска. До недавнего времени поддержание баланса «риск — доходность» держалось на конкретных людях или на долгих расчётах, а теперь искусственный интеллект выдаёт «подсказки» в реальном времени.

4) **Кредитование.** Немного выше мы говорили о том, как программные роботы помогают анализировать кредитозаёмщиков, проводят их скоринг. А кредитному менеджеру остаётся только принятие решения на достоверных и актуальных данных.

5) **Автоматизация рутинных и «нормативно неизбежных» операций,** сюда же относится подготовка регуляторной отчётности. Один из примеров — про потоковую обработку бумажных документов — мы уже обсуждали. Она значительно освобождает время либо для творческой работы, либо для работы со «слабораспознанными» документами. Здесь же надо упомянуть действия банков по ПОД/ФТ, которые вручную требуют очень много ресурсов, а недостаток ресурсов или некачественная отчётность может повлечь лишение лицензии. Принцип действия остаётся прежним: информационные системы и программные роботы готовят данные для принятия решения, которое остаётся за человеком.

В АКАДЕМИЧЕСКОЙ СРЕДЕ

Интересно, что если банкиры, как правило, используют термин «искусственный интеллект», то сами научные работники относятся к нему весьма осторожно и стараются не упоминать всуе. Учёные видят вместо ИИ в основном математические задачи и алгоритмы. И главным для них является подготовка кадров для решения таких математических задач. Интеллект, по мнению академической науки, нужен не столько искусственный, сколько человеческий, чтобы слышать задачи бизнеса, понять, адекватно интерпретировать и поставить математические задачи. Затем — решить их!

В академической среде и среди ряда российских технологических компаний популярной является точка зрения, что ИИ в большей своей части — это обыкновенный прецедентный анализ. И этот прецедентный анализ хорошо работает, иногда даже лучше, чем сам человек, особенно в ситуациях, которые похожи на те, что встречались раньше. При этом никакой этики и морали, которыми пытаются «нагрузить» ИИ, в прецедентном анализе нет. В каждом случае по отношению к текущему анализу важно и нужно решить две задачи. Первая задача — определение похожей ситуации как прототипа, вторая задача — собственно анализ с опорой на данные обучающей выборки и поиск управляющего решения.

ПОСЛЕСЛОВИЕ

Мировой опыт показывает, что ИИ традиционно занимаются в основном инженеры. Математиков в этой области почти нет. Инженеры — важная и нужная профессия, но в этом деле они должны идти после математиков.

Если говорить про нашу страну, то и в Советском Союзе, и в современной России проблемами ИИ на высоком теоретическом уровне занималась и продолжает заниматься большая группа выдающихся математиков.

И одним из них является академик РАН Константин Владимирович Рудаков, который известен не только своими высокими математическими достижениями, но и практически разработками.

Однако современная мода некоторых наших чиновников — смотреть только на «зарубеж» — коснулась и ИИ. Например, недавно прошла информация, что главный у нас по ИИ — Сбербанк!

И как правильно ответил на эту новость в одном из интервью Константин Владимирович: «Если главный по искусственному интеллекту — Сбербанк, то главной по кредитам должна быть Академия наук»!



**Георгий
ГАРБУЗОВ**
Департамент
кибербезопасности
Сбербанка



**Алексей
ТЕРЕНИН**
Департамент
кибербезопасности
Сбербанка

ИИ НА СТРАЖЕ БАНКОВСКИХ ДАННЫХ — 2¹

ОПЫТ СБЕРБАНКА

ТАЙНОЕ ВСЕГДА СТАНОВИТСЯ ЯВНЫМ... И ДОРОГИМ

Ранее мы уже рассказывали о нашем опыте применения технологий искусственного интеллекта (ИИ) при решении задач поиска и классификации данных, требующих защиты. Сегодня хотелось бы поговорить ещё об одном практическом аспекте ИИ-технологий, при котором они работают в связке с классическими системами защиты информации, значительно повышая их эффективность. Речь пойдёт о процессе защиты от утечек информации и системах DLP (Data Leakage Prevention), применение которых давно стало обязательным в любой организации, реализующей комплексный подход к информационной безопасности.

С момента своего появления эти системы непрерывно совершенствовались, сохраняя в основе всё тот же принцип анализа потока информации на предмет соответствия критериям, определённым в виде фиксированного набора правил (политик). Недостатки такого подхода, ранее не столь заметные, сегодня стали очевидны: эффективность алгоритмов, основанных на статических правилах, в условиях развития экосистем и нарастания объёма и разнообразия коммуникаций оказывается недостаточной. Прежде всего это относится к неструктурированной и не основанной на регулярных выражениях информации, а ведь именно она подчас представляет наибольшую ценность для современных компаний — это новые разработки и технологии, ценная аналитика и прочее.

Вместе с этим из года в год растёт и стоимость утечек персональных данных: согласно оценкам института Ponemon², средняя стоимость утечки в 2019 году составила 3,92 миллиона долларов США, а средняя стоимость одной записи — 150 долларов. Последствия таких

утечек также могут быть весьма чувствительны для организации. Так, утечка данных гостей сети отелей Marriott в 2018 году оценивается в 2,2 млрд долларов³.

СЛАБОЕ ЗВЕНО

Настройка политик DLP-системы осуществляется вручную, по результатам обследования бизнес-процессов. По сути, политики представляют собой статичный срез информационной картины бизнеса, склонный к постепенному старению и утрате актуальности.

По опыту внедрения и экспертным оценкам специалистов Сбербанка, совокупную точность (соотношение ложноположительных и ложноотрицательных срабатываний) классической DLP-системы редко удаётся удержать на уровне выше 70%. Дальнейшее повышение точности ведёт к значительному росту затрат на управление и актуализацию политик.

Невысокие показатели точности не позволяют переводить DLP-систему в режим предотвращения утечек (в режим блокировки, «в разрыв») из-за рисков прерывания бизнес-процессов, а служба кибербезопасности сталкивается с целой лавиной ложных срабатываний политик DLP и необходимостью применять разветвлённый набор фильтров для того, чтобы сузить воронку срабатываний до приемлемого уровня. Таким образом, DLP-система, являясь ядром технологического стека процесса защиты от утечек, становится его слабым звеном именно с точки зрения конечного результата: к моменту разбора инцидента по факту утечки сама утечка уже состоялась, а информация покинула периметр.

Радикально поднять точность DLP-систем можно, лишь выполнив два условия:

- ◆ принципиально повысить качество политик;
- ◆ обеспечить актуальность политик — резко сократить скорость реагирования на изменения, в том числе за счёт пересмотра процесса формирования политик.

¹ Продолжение. Первая статья этого цикла — в BIS Journal № 2/2020.

² Cost of a Data Breach 2019 — Ponemon Institute.

³ The Times, 20 августа 2020.

МЕТОДИКА ФОРМИРОВАНИЯ И ВЫБОРА МОДЕЛЕЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Какие модели были обучены

Для построения модели выбран алгоритм NER (Named-entity recognition — алгоритм распознавания именованных сущностей). Данный алгоритм был выбран, так как:

- ◆ Существует версия, адаптированная для распознавания данных на русском языке.
- ◆ Алгоритм NER — открытый алгоритм.
- ◆ Алгоритм изначально предназначен для поиска данных в текстах, поэтому может учитывать синтаксические особенности, что позволяет качественнее классифицировать ячейки, в которых больше одного слова.
- ◆ Выбрана версия от iPavlov с репозитория deeppmt (она предназначена для русского языка), так как входящие данные на русском языке.
- ◆ Также апробирован Topic Modeling.

Критерии отбора

- ◆ Качественный критерий: классифицирует каждый фрагмент данных.
- ◆ Верно классифицирует каждый фрагмент данных с точностью выше 80%.
- ◆ Из обученных моделей выбираются модели с наилучшими показателями:
 - «относительный коэффициент верной классификации» — количество верно классифицированных представителей типа ко всем представителям данного типа;
 - по показателям, показывающим, насколько неверно классифицированы данные (например, классификация имени как фамилии более приоритетна, чем классификация имени как номера банковской карты).

Категории данных

Список категорий создавался как наиболее полный список, покрывающий все виды чувствительных данных, любой новый вид ЧД выражается через виды из списка. Список построен на основе анализа Конституции и федеральных законов РФ и ВНД банка.

Подготовка данных

- ◆ Создание датасетов для каждого вида данных.
- ◆ Очистка датасетов от шума.
- ◆ Расстановка тегов в каждом датасете.
- ◆ Создание тренировочной, валидационной и оценочной выборок.

Приоритет обучения

- ◆ Наиболее часто используемые защищаемые данные.
- ◆ Персональные данные.
- ◆ Данные PCI DSS.

Обучение моделей

- ◆ Обучение моделей на тренировочных выборках.
- ◆ Проверка моделей на отдельно созданных таблицах с различными типами данных.
- ◆ Выбор обучающих датасетов и лучшей модели.

Врезка 1. Методика формирования и выбора моделей искусственного интеллекта

Решение этих задач традиционными способами, например наращиванием вычислительных мощностей или персонала, выглядит неудачной идеей в силу существования принципиально неустранимых проблем ручного труда с его субъективными суждениями, неполнотой и трудностями получения информации. Но что, если доверить «интеллектуальный» труд более интеллектуальной системе? Например, передавать срабатывания DLP-системы обученной AI-модели

для компенсации неточности политик? Такая пилотная модель была реализована в Сбербанке силами специалистов кибербезопасности.

НОВЫЕ ТЕХНОЛОГИИ ДЛЯ СТАРЫХ ЗАДАЧ

Для реализации подхода и обучения детектирующих моделей были выбраны типы данных, на которых чаще всего происходят сбои в детекции утечки системой DLP. Массив таких данных был

На основе алгоритма NER обучено два типа моделей

- ◆ Первые две модели на CNN и RNN не учитывают синтаксические особенности. Каждый экземпляр данных расценивается как единый неделимый элемент.
- ◆ Вторые две модели на CNN и RNN уже учитывают синтаксические особенности — последовательность слов (последовательностей символов, разделяемых пробелом). Каждый экземпляр данных расценивается как упорядоченный массив.
- ◆ Вспомогательные негибкие алгоритмы: *regex* — регулярные выражения, *digit* — контрольные значения.
- ◆ Модели разработаны и обучены на выборке в 100 000 строк, содержащей конфиденциальные данные.
- ◆ После добавления вспомогательных быстрых алгоритмов скорость работы системы повысилась на 33 %, но точность распознавания четырёх видов данных снизилась на 1–2 %, точность распознавания остальных видов данных не изменилась. Решено использовать ансамбль из трёх моделей с анализом контрольных разрядов и проверками на регулярных выражениях, при количестве распознаваемых типов данных 35 показывает среднюю точность 95 %, из них ~40 % атрибутов распознаются с точностью > 99,9 %.
- ◆ Отбор обученных моделей производится по результатам работы на валидационной выборке — синтетически подготовленном наборе данных, содержащем все используемые в модели виды данных и состоящем из 1000 экземпляров каждого вида.

Достигнутое качество распознавания

		F	N	T
Сверточные нейронные сети	cnn_1	0,68	21	0,5
	cnn_2	0,69	24	0,5
Рекуррентные нейронные сети	rnn_1	0,61	22	1
	rnn_2	0,69	23	1

F — средняя F-мера — метрика, объединяющая точность и полноту распознавания каждого вида данных

N — количество распознаваемых видов данных

T — относительное время работы

Сверточные сети работают в 2 раза быстрее, чем рекуррентные сети

Самый низкий показатель средней F-меры у rnn_1, и он существенно отличается от остальных сетей. Было решено его **не использовать**

Врезка 1 (продолжение). Методика формирования и выбора моделей искусственного интеллекта

размечен и обогащён набором, который точно относится к анализируемому типу (например, номера паспортов, счетов и т.д.), при этом символьная информация и неструктурированные данные также преобразовываются в цифровой структурированный вид при помощи ещё одних моделей, работающих перед основной. Ансамбль таких моделей помогает обнаруживать в потоке информации данные счетов, паспортов и банковских карт, при этом для данных, уже преобразованных в цифровой формат, и для ускорения фильтрации применяются регулярные выражения, алгоритмы определения контрольного разряда и Луна⁴.

⁴ Алгоритм вычисления контрольной цифры номера пластиковой карты в соответствии со стандартом ISO/IEC 7812. Предназначен для определения правильности указания номера карты путём расчёта контрольного значения.

Ансамбль моделей составляют нейронные сети (в большинстве своём класса NLP — Natural Language Processing) и «классические». Для NLP используются модели CNN и RNN (сверточные и рекуррентные нейронные сети). При обучении использовались различные параметры настройки слоёв нейронных сетей. Не все варианты оказались удачными, но те, что удовлетворяли заданным метрикам по точности, нашли применения в промышленном решении. Модели дополняют друг друга, усиливая точность взаимного результата отнесения анализируемых данных к тому или иному типу и категории защищаемой информации.

Подробнее приведено на врезке 1; на врезке 2 представлены подробные данные по основным типам распознаваемых типов данных. Как мы видим, основной упор делается на поиск персональных данных, так как их

ОСНОВНЫЕ ТИПЫ РАСПОЗНАВАЕМЫХ ДАННЫХ

- ◆ Основной номер держателя карты (PAN)
- ◆ Номер ИНН
- ◆ Номер ОГРН
- ◆ Номер СНИЛС
- ◆ Номер ОГРН ИП
- ◆ Номер полиса обязательного страхования
- ◆ Число
- ◆ Номер КПП
- ◆ Дата
- ◆ Номер счёта
- ◆ Код LEI
- ◆ IP-адрес
- ◆ Счёт депозита
- ◆ Воинское звание
- ◆ Пол ФЛ
- ◆ Идентификатор ФЛ в социальных сетях
- ◆ Vin-номер машины
- ◆ Форма собственности ЮЛ
- ◆ Номер ДУЛ
- ◆ Номер трудовой книжки
- ◆ Email-адрес
- ◆ Научная степень ФЛ
- ◆ Телефон
- ◆ Паспорт транспортного средства
- ◆ Организационно-правовая форма ЮЛ
- ◆ Регистрационный номер машины
- ◆ Не является ЧД
- ◆ Индивидуальный предприниматель
- ◆ Отчество
- ◆ Орган, выдавший ДУЛ
- ◆ Ф. И. О.
- ◆ Адрес
- ◆ Полное и краткое наименование ЮЛ
- ◆ Фамилия
- ◆ Структурное подразделение банка
- ◆ Должность
- ◆ Гражданство
- ◆ Профессия
- ◆ Специальность
- ◆ Имя
- ◆ Номер военного билета
- ◆ IMEI
- ◆ MAC-адрес

Здесь приведены только основные типы данных, на этом список не исчерпывается.

Врезка 2. Основные типы распознаваемых данных

охрана — одно из важнейших требований различных регуляторов (законы РФ, ЦБ РФ⁵, GDPR⁶).

Как результат: обучены четыре модели на рекуррентных и сверточных нейросетях на базе NER (Name Entity Recognition). По результатам сравнения качества моделей на валидационной выгрузке отобраны три лучшие из них. Ансамбль из трёх моделей с анализом контрольных разрядов и проверками на регулярных выражениях показывает среднюю точность 95 %, из них ~40 % атрибутов распознаются с точностью > 99,9 %.

В первую очередь модели настроены работать с табличными файлами и проходили обучение на структурированных данных, накопленных в аналитическом хранилище данных банка. Также активно разрабатываются модели для работы с текстами и неструктурированной информацией, но это темы для следующих статей. Например, для работы с текстом приме-

няется бэггинг двух CNN-моделей, одной RNN-модели, регулярных выражений и проверок на контрольные разряды. Также проводится исследование качества работы при векторизации, с дальнейшим использованием различных ML-моделей; бэггинг на основе взвешивания фич в векторах.

ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ

В банке был успешно проведён пилот по интеграции сервиса распознавания конфиденциальной информации и системы DLP.

Схема реализованного взаимодействия DLP-системы и модели ИИ изображена на рис. 1.

При взаимодействии DLP-системы и AI-модели был реализован следующий алгоритм:

1. Пользователь отправляет сообщение, содержащее подозрительный файл, сообщение перехватывает DLP-система.

2. DLP-система направляет уведомление о нарушении программному роботу (специальный модуль, написанный на Python, служащий посредником между моделью и DLP в связи с отсутствием у последней необходимой функциональности).

3. Программный робот с использованием API-интерфейса забирает подозрительный файл

⁵ ЦБ РФ — Центральный банк Российской Федерации.

⁶ GDPR — General Data Protection Regulation (Общий регламент по защите данных) — постановление Европейского союза, с помощью которого Европейский парламент, Совет Европейского союза и Европейская комиссия усиливают и унифицируют защиту персональных данных.

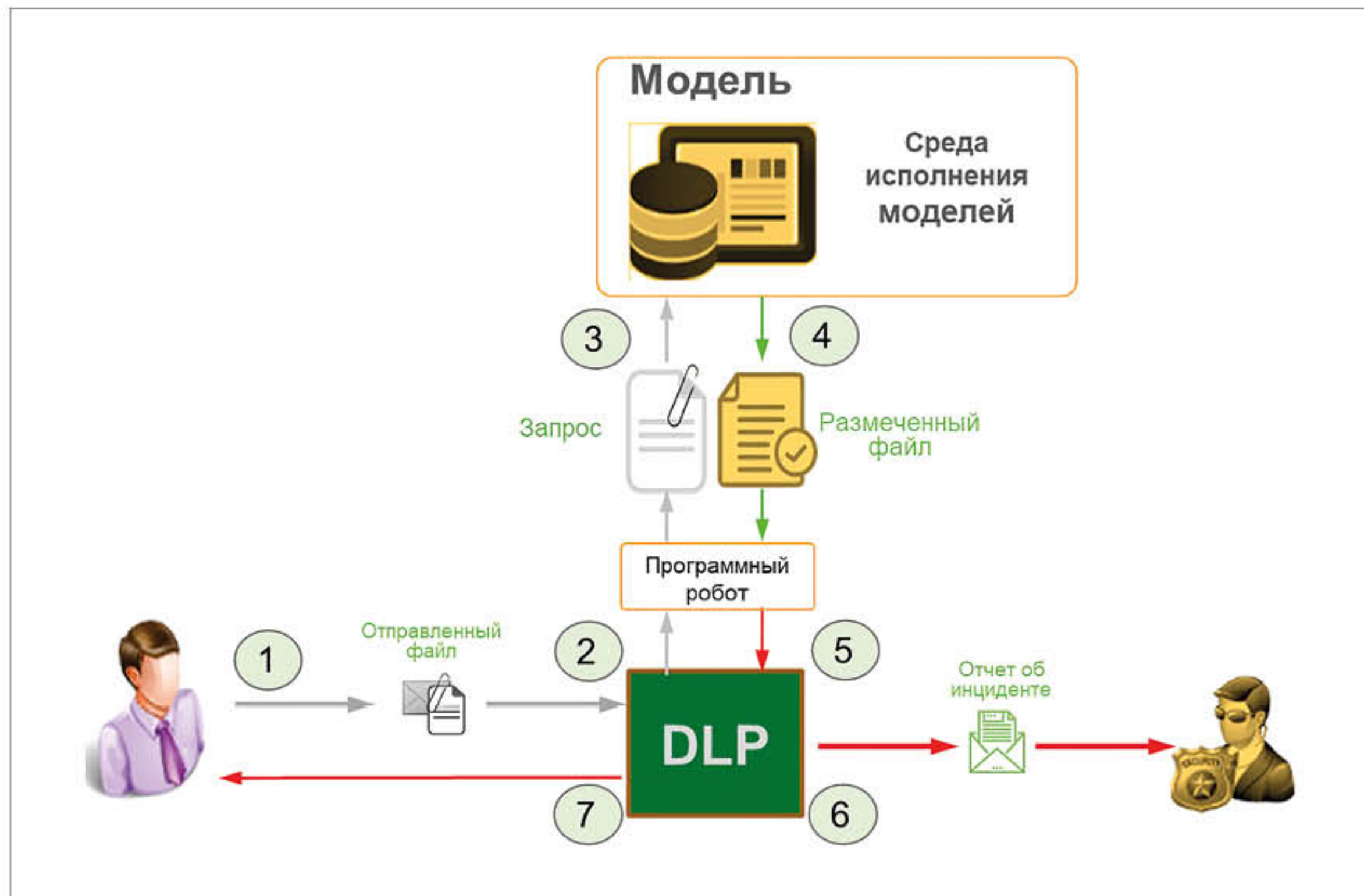


Рисунок 1. Схема взаимодействия DLP-системы и модели

из DLP-системы и передаёт его в исполняемую среду модели.

4. Модель проводит анализ файла, размечает его и передаёт программному роботу.

5. Программный робот анализирует размеченный файл и в случае наличия в нём разметки, указывающей на наличие конфиденциальной информации (формат разметки, воспринимаемой роботом, согласовывается заранее), предоставляет признак инцидента в карточке события в системе DLP.

6. Уведомление о подтверждённом инциденте направляется офицеру безопасности (для старта дисциплинарного процесса и т.д.)

7. Отправителю направляется уведомление о блокировке сообщения в связи с нарушением требований кибербезопасности.

Измерения показали точность порядка 95–98% на синтетических данных. Предварительная оценка показывает, что при общем количестве событий около 3000 в месяц такая автоматизация позволит сэкономить не менее 300 человеко-часов, т.е. полноценно заменить трёх квалифицированных офицеров безопасности, причём, в отличие от них, она будет работать в круглосуточном режиме, без перерывов на обед, праздников и выходных.

Конечно, при смене системы DLP приходится заново переписывать реализацию интеграции между системами, поэтому можно либо совершенствовать универсального программного робота, либо сделать программные API для безболезненного перехода с одной системы на другую.

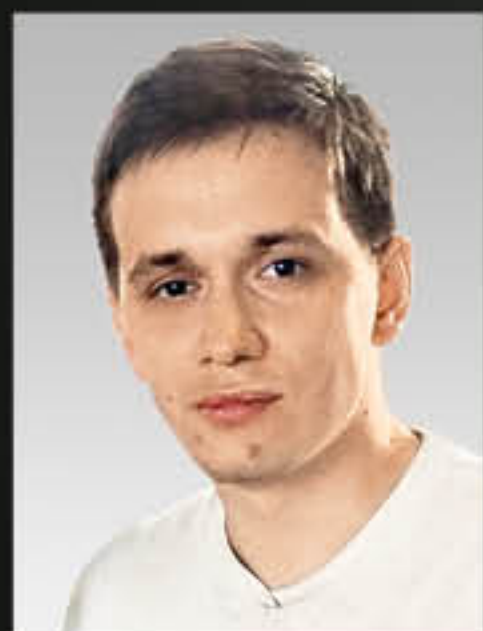
ЗАКЛЮЧЕНИЕ

Описанный выше подход при сравнительно невысокой стоимости обладает целым рядом ценных преимуществ в сравнении с классическими статическими системами. Остаются возможности для развития и улучшения способов интеграции, расширения распознаваемых типов данных, внедрения новых, ещё более точных моделей, с применением самообучения для повышения скорости и гибкости адаптации комплексной системы к меняющимся потокам данных и условиям функционирования. ИИ можно использовать в связке не только с DLP, но и с другими системами, например, для поиска конфиденциальных данных в файловых хранилищах, а также в качестве сервиса, помогающего работникам классифицировать данные.

Конечно, на сегодня не до конца решён ряд важных задач, это и вопросы интеграции, и проблема обучения моделей на неструктурированных данных с произвольным текстом для надёжного выявления в информационном потоке сведений, составляющих коммерческую тайну предприятия, и других. Тем не менее успешный опыт Сбербанка доказывает эффективность и потенциал систем искусственного интеллекта для облегчения труда аналитиков безопасности по разбору инцидентов утечек данных, а также наглядно показывает дальнейшие пути развития систем ИИ на других этапах жизненного цикла управления инцидентами. Предлагаем коллегам делиться своим опытом в изучении этого перспективного направления развития кибербезопасности.



Анатолий КОНКИН
руководитель
направления
«Развитие технологии
распределённого
реестра»
Ассоциации ФинТех



**Илья
ДРУЖИНИН**
аналитик-
исследователь
Ассоциации
ФинТех

ZKP — БЛОКЧЕЙН. СОЮЗ СКОРОГО БУДУЩЕГО

КАК ДОКАЗАТЬ, ЧТО У ВАС В КАРМАНЕ 100 РУБЛЕЙ,
НЕ ПОКАЗЫВАЯ БАНКНОТУ ПРОВЕРЯЮЩЕМУ

Ассоциация ФинТех внимательно следит за развитием технологий, применяемых в блокчейн-сфере. Мы выделяем ZKP в качестве передового способа усиления конфиденциальности в распределённых реестрах. Однако ZKP-протоколы до сих пор остаются недостаточно изученными в контексте блокчейн-технологий и тем более не стандартизированными для применения. Ассоциация ФинТех проводит исследования протоколов и заинтересована в стандартизации ZKP-протоколов для применения в финансовой сфере.

Недавно создатель Ethereum Виталик Бутерин рассказал о «масштабной и тихой технологической революции», которая произошла благодаря

применению в блокчейне протокола доказательства с нулевым разглашением. Эта технология позволяет решить одну из проблем, наиболее остро стоящих перед блокчейн-сообществом, а именно обеспечение конфиденциальности передаваемых данных, когда детали операции и корректность транзакций должны подтверждаться участниками сети. В том числе эта проблема препятствует широкому использованию блокчейна корпорациями. Активно исследовать применение протокола в России уже начали разработчики блокчейн-платформ.

Доказательство с нулевым разглашением (zero knowledge proof; ZKP) — это криптографический коммуникационный протокол, в котором есть по крайней мере две стороны:

Технология обеспечивает конфиденциальность, сводя при этом необходимость вычислений к минимуму: «Вместо проверки чего-то большого нужно проверить маленькое доказательство»

доказывающий и проверяющий. Цель доказывающего — убедить проверяющего в том, что некое вычислительное утверждение истинно, не раскрывая дополнительной информации. В самом простом понимании при помощи ZKP вы можете доказать, что у вас в кармане есть 100 рублей, не показывая банкноту проверяющему. Впервые группа криптографов выдвинула концепцию интерактивной системы доказательств с нулевым разглашением в 1985 году.

Почему Бутерин называет это революцией? Он объясняет так. Технология обеспечивает конфиденциальность, сводя при этом необходимость вычислений к минимуму: «Вместо проверки чего-то большого нужно проверить маленькое доказательство».

Развитие протоколов ZKP позволит реализовать много новых бизнес-кейсов на распределённых реестрах, где нужна конфиденциальность бизнес-процессов. Сейчас ZKP-протоколы активно исследуются мировым криптографическим сообществом, но зрелых решений с использованием ZKP ещё нет. Как нет и стандартов: ни NIST, ни ГОСТ, ни ISO... Наиболее известное на сегодня применение доказательства с нулевым разглашением — в анонимной криптовалюте Zcash, обеспечивающей её владельцам конфиденциальность расчётов. В конце прошлого года банк ING — один из наиболее активно развивающих блокчейн — объявил о запуске своего решения для распределённых реестров на основе ZKP, которое может быть востребовано в финансовом секторе, где важной задачей является не только сохранение конфиденциальности, но и соответствие регуляторным требованиям, таким как KYC.

Теория ZKP различает два типа доказательств: ZKP знания (ZKPК) подтверждает владение конфиденциальной информацией, а ZKP принадлежности (ZKPM) доказывает истинность утверждения о вхождении в некоторое множество, набор. Учитывая это, на наш взгляд, можно выделить три сценария применения, для которых протоколы с доказательством с нулевым разглашением подходят лучше всего и где в ближайшее время можно ждать «революции», в том числе и в России.

СОХРАНЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ

Для сохранения конфиденциальности личности. Можно, например, доказать корректность личных данных, например, возраста и места проживания, не раскрывая более подробную информацию, такую как дата рождения и адрес. Идея идентификации при помощи протоколов ZKP заключается в том, что у пользователя есть набор атрибутов, которые подтверждены удостоверяющим центром. Например, для получения финансовой услуги Алисе нужно доказать, что ей больше 18 лет и она живёт в стране, которая входит в ЕАЭС. Алиса могла бы использовать доказательства с нулевым разглашением, чтобы подтвердить, что она соответствует определённым критериям. Например, она может использовать ZKRP (Range proof), чтобы доказать, что её возраст превышает 18 лет, и ZKSM, чтобы доказать, что она живёт в стране, которая принадлежит ЕАЭС. Это доказательство может быть передано проверяющему, который должен подтвердить информацию, чтобы разрешить Алисе воспользоваться некоторой услугой. Использование ZKP в этом случае позволит нивелировать риски кражи личных данных, слежки, социальной инженерии и т.д.

ПЕРЕДАЧА АКТИВОВ

Для передачи активов. Финансовые учреждения обычно требуют идентификации отправителя и получателя, а также типа и суммы активов. Протоколы ZKP допускают вариант сохранения конфиденциальности, когда сделка совершается между анонимными сторонами и в то же время гарантирует, что они и их активы удовлетворяют нормативным требованиям (подробнее об этом — в третьем сценарии). В общем случае рассматриваемое состояние системы — это (зашифрованный) баланс счёта каждого пользователя системы. Каждый баланс счёта шифруется с помощью аддитивно гомоморфной криптосистемы ключом владельца счёта. Транзакция уменьшает баланс счёта отправителя, одновременно увеличивая счёт получателя на соответствующую сумму. Если количество пользователей фиксировано и известно заранее, то транзакция может скрыть всю информацию об отправителе и получателе, одновременно обновив все остатки на счетах. Это обеспечивает высокую степень конфиденциальности. Если количество пользователей чрезвычайно велико, динамически изменяется или неизвестно отправителю, он должен выбрать «набор анонимов», которые будут включены в протокол.

СООТВЕТСТВИЕ РЕГУЛЯТОРНЫМ ТРЕБОВАНИЯМ

Для соответствия регуляторным требованиям. Важным типом приложений, в которых используются ZKP-протоколы, являются приложения, в которых регулирующий орган хочет контролировать некоторых участников. Системы, использующие ZKP, позволяют аудитору получить доказательства того, что бизнес-процесс удовлетворяет ряду требований, без необходимости подробно изучать, как они были исполнены. Одним из таких примеров может быть контроль уплаты налогов владельцем счёта; проверка, является ли банк или какое-либо другое финансовое учреждение платёжеспособным.

Регулирующий орган в таких случаях заинтересован в изучении «итоговых показателей», которые обычно выводятся из некоторых совокупных оценок, основанных на более детальных нижележащих данных, но регулятору необязательно знать все детали. Например, ответ на вопрос: «Не брал ли банк слишком много кредитов?» в итоге имеет один бит (Да/Нет) и может быть дан без детализации каждого отдельного кредита. Для того чтобы вычисления над скрытыми данными были полезны, вводимые

сведения должны быть изначально корректны (проблема GIGO, «Мусор на входе — мусор на выходе»). В противном случае доказывать правильность вычислений было бы бессмысленно. Поэтому данные, которые используются для доказательств, должны, как правило, передаваться сторонами, которые не ангажированы доказывающему и вряд ли вступят в сговор с проверяющим.

* * *

Подводя итог, можно сказать, что использование протоколов ZKP отлично сочетается с блокчейном, такой союз позволит повысить конфиденциальность пользователей и одновременно создать доверие к используемым данным, поскольку блокчейн гарантирует неизменность записываемой в него информации. Использование протокола ZKP для своей цифровой валюты на блокчейне анализировал даже Банк Канады, правда, пока отказался от этой идеи. Но само внимание регулятора к этой технологии говорит о том, что всё больше игроков интересуются этим решением и в будущем мы можем увидеть много новых проектов с использованием ZKP.



Александр ЧЕРЁМУШКИН
эксперт BIS Journal

BIS-КОММЕНТАРИЙ

Статья затрагивает вопросы будущего применения технологии доказательства с нулевым разглашением (ZKP) для обеспечения конфиденциальности информации, хранимой в распределённых реестрах (блокчейне). Хотя она и написана с налётом научной фантастики, когда авторы описывают целый ряд ситуаций, о которых пока остаётся только мечтать, но тем не менее процесс развития технологий ZKP идёт такими быстрыми темпами, что вполне возможно, что те три задачи, о которых пишут авторы, в будущем найдут свои решения.

В настоящее время спектр задач, для решения которых возможно применять ZKP, и арсенал приёмов и методов для их решения настолько расширяется, что уже удалось преодолеть многие казавшиеся ранее непреодолимыми

ограничения. Если раньше, по сути, преобладали только различные способы доказательства знания ответа на решение какой-либо сложной вычислительной математической задачи, то сейчас разработано много протоколов для более широкого класса задач, включая доказательство факта принадлежности числа определённому интервалу ZKRP (Zero Knowledge Range Proof), доказательство вхождения набора строк в некоторое скрытое множество ZKSM (Zero Knowledge Set Membership), которые могут выступать как в интерактивном, так и в неинтерактивном вариантах. Вместе с тем сложность математических задач, на которых основаны такие доказательства, а также самого применяемого математического аппарата создаёт труднопреодолимый барьер для их широкого применения. Поэтому «приземление» таких задач к конкретным ситуациям, возникающим в реальной жизни, требует серьёзных усилий для поиска способов кодировки и интерпретации фактической информации в виде, пригодном для их представления в качестве данных, используемых в протоколах на основе каких-либо математических задач. Причём такие трудности возникают не только при реализации и программировании известных протоколов, но и в поиске принципиальных решений, позволяющих создавать такие реализации.



Вениамин ЛЕВЦОВ
директор департамента
корпоративного бизнеса
«Лаборатории Касперского»

«ЛАБОРАТОРИЯ КАСПЕРСКОГО» ДЛЯ КРУПНОГО БИЗНЕСА

ВЕНИАМИН ЛЕВЦОВ — О ЗАПРОСАХ КРУПНОГО БИЗНЕСА
В СФЕРЕ ИБ, НОВЫХ ПРОДУКТАХ И РАЗВИТИИ КОМПАНИИ

«Лаборатория Касперского» традиционно сильна в защите конечных устройств, но сегодня она успешно продвигает и комплексные решения кибербезопасности для всех сегментов крупного бизнеса — от корпораций до организаций уровня CERT. На вопросы BIS Journal отвечает директор департамента корпоративного бизнеса «Лаборатории Касперского» Вениамин Левцов.

НАЧАЛО

— Когда и как вы пришли к тому, что надо не только делать антивирусы, но и расширять линейку продуктов?

— Системно мы начали развивать группу продуктов NonEPP (Non Endpoint Protection Platform) примерно с 2013 года, когда стало очевидно, что всё больше заказчиков требуют от нас полноценной системы защиты, а не просто безопасности конечных точек. «Лаборатория Касперского» — игрок глобальный, и если наши решения в России лидируют, то за её пределами за место под солнцем приходится бороться. Сложно пробиваться к новому заказчику, имея одно-единственное решение, особенно когда это защита конечной точки, которая часто является корпоративным стандартом, и его приходится

менять при переходе с одного решения на другое. Получается целый миграционный проект, и зачастую его себестоимость превышает стоимость годового владения антивирусным решением.

Кроме того, сегодня защита конечной точки невозможна без понимания процессов в её сетевом окружении. Именно поэтому мы давно уже не рассматриваем наш продукт как самодостаточный, а планируем развитие системы наших решений в рамках единого пространства инцидентов, единого «озера данных» телеметрии, связанных механизмов распознавания и классификации угроз, единых политик реакции и так далее.

ТРИ ФАЗЫ

— Сейчас в «Лаборатории Касперского» существует экосистема продуктов для крупных компаний. Что представляет собой эта экосистема?

— Конечной точкой может быть не только офисный компьютер, но и виртуальная машина в облаке, мобильное устройство, хранилище больших объёмов данных, банкомат, технологические устройства... И у каждого из них есть специфика, которая накладывает ограничения на продукт защиты. Тут важно отметить, что мы в состоянии

защитить все типы конечных точек, обеспечить для них единое покрытие технологиями защиты, единообразное применение политик информационной безопасности.

Кроме того, разумно ловить угрозы на подлёте. Для этого мы обеспечиваем безопасность почты и веба, в том числе и посредством технологий «песочницы». Естественно, мы уделяем внимание системам централизованного управления нашими решениями. Планируем развивать собственную единую платформу управления. Мы видим её как важный элемент системы ИБ заказчика. В нашей стратегии она должна обеспечивать единую систему хранения логов, отчётов, телеметрии, иных событий, приходящих от разных продуктов, единый механизм расширенного обнаружения угроз и связанные автоматизированные инструменты реагирования на обнаруженные угрозы.

— Расскажите подробнее, как устроена система Kaspersky Threat Hunting?

— Концепция защиты корпоративной сети проходила через несколько фаз по мере усложнения угроз и созревания рынка, сообщества и технологий. В 2000-х все боролись с вирусами и троянами, используя такие самодостаточные решения, как антивирус и

Firewall. Я бы назвал эту эру Malware-centric — тогда главной задачей было найти и обезвредить вирус.

На следующем этапе вредоносные технологии стали многокомпонентными и начали использовать уязвимости информационных систем, в том числе уязвимости нулевого дня. Они стали использовать легитимные способы доставки, например, макросы в документах Microsoft Office. Многокомпонентность привела к «разделению труда» между элементами угрозы: одни модули проникали в инфраструктуру, другие устанавливали связь с внешними управляющими центрами, третьи доставляли тело зловреда и т.д. То есть от атомарного единого приложения мы пришли к сложной комплексной угрозе. Именно на этом этапе «угроза» (Threat) как понятие и цель и появилась в фокусе служб ИБ. Чтобы бороться с этими угрозами, пришлось внедрять разные механизмы мониторинга в сети и поиска их по разным следам и проявлениям.

Потом эти угрозы стали ещё более изощрёнными, началось использование социальной инженерии и технологий, которые мы раньше наблюдали только в так называемых спонсируемых государством атаках. Плюс к этому атаки стали длительными: от захвата устройства до активных действий иногда проходят сотни дней. Началась третья фаза.

Тут ключевым понятием для ИБ становится «инцидент» как сложное длящееся событие, серьёзно влияющее на бизнес или дееспособность организации. На первый план выходит проактивный поиск уже состоявшегося заражения, когда угроза ещё не проявила себя в полной мере — это и есть Threat Hunting. То есть служба ИБ по умолчанию исходит из того, что заражение в системе уже есть и его надо искать. А для проактивного поиска нужны специфические инструменты, в частности механизмы анализа больших данных, приходящих с компьютеров и из сети, и многое другое. Вот это всё и обеспечивается в рамках сервиса MDR (Managed Detection and Response) «Лаборатории Касперского». Кроме того, я считаю, именно эта задача — проактивного поиска угроз в

Задача проактивного поиска угроз в сети станет главной для сервис-провайдеров, вклад которых в ИБ предприятий разного уровня будет неизбежно расти

сети — станет главной для сервис-провайдеров, вклад которых в ИБ предприятий разного уровня будет неизбежно расти.

ПРО ЗАПРОСЫ БИЗНЕСА

— Давайте поговорим о запросах крупного бизнеса в сфере ИБ? Как вы эти запросы отслеживаете?

— В «Лаборатории Касперского» функционирует глобальная служба сбора запросов по крупным и значимым проектам. Кроме того, наши эксперты, в том числе и моя команда, вовлечены во все крупные активности и пилоты на всех ключевых для компании рынках. Россия для нас, конечно, рынков номер один.

В целом основные запросы по-прежнему касаются максимальной автоматизации процессов служб ИБ, проведения периодической проверки защищённости и проактивного поиска проблем в инфраструктуре. В последнее время чаще стали появляться запросы на поддержку виртуальных десктопов и вообще облачных решений, защищённости рабочих мест сотрудников на удалённой работе. Также вырос аппетит к развёртыванию решений не на серверах внутри компаний, а в виртуальных средах.

Несмотря на то что в России к концепции публичных облаков по-прежнему относятся настороженно, мы видим, что ситуация заставляет внимательно рассматривать все возможные облачные подходы, включая частные облака, частные дата-центры, публичные облака, расположенные в пределах РФ.

ПРО ИМПОРТОЗАМЕЩЕНИЕ

— Готовы ли вы «вписаться» в волну импортозамещения на объектах КИИ?

— Масштаб рисков, с которыми сталкиваются операторы объектов КИИ, настолько велик, что, несмотря на все сложности, мы видим, насколько серьёзно ИТ-сообщество относится к этой истории. И «Лаборатория Касперского»

не могла не подумать о том, как внести свой вклад. Во-первых, мы активно развиваем наши специфические решения для защиты технологических процессов, причём как на конечных точках, так и в сети. Продолжаем совершенствовать нашу операционную систему, которой, надеюсь, будут оснащаться многие критические системы. Кроме того, мы понимаем, что ключевой элемент системы ГосСОПКА — это центр сбора консолидированной информации об угрозах, который пронизывает всю экосистему объектов КИИ. Но такой сбор предполагает использование унифицированных платформ, и именно эта задача является одной из важнейших для нашего нового продукта KUMA (Kaspersky Unified Monitoring & Analysis Platform), относящегося к классу SIEM, который мы планируем выпустить в следующем году.

О БУДУЩЕМ

— Планируется ли разработка новых продуктов и сервисов для крупного бизнеса?

— Во-первых, растёт объём и сложность угроз, с которыми приходится сталкиваться. Мы планируем расширить механизмы автоматического блокирования в случае обнаружения угроз в сетевой песочнице. То есть службе ИБ придётся лишь констатировать факт, что какой-то зловред был остановлен, и в соответствии с рекомендациями, которые предложит система, провести долечивание или устранение проблем, а не самостоятельно, с нуля, проектировать ответ на обнаруженный детект.

Во-вторых, как я уже сказал, продуктов у нас много, и надо признать, что выпускались они как самодостаточные решения. Сейчас крупные заказчики, и не только в России, используют множество наших продуктов, и эти продукты продолжают действовать как независимые единицы, а нам хочется получить согласованную работу всей защитной системы, управляемую из единого

Единственный, на мой взгляд, эффективный путь — это создание *human firewall*, то есть превращение сотрудников в обученный, настороженный защитный кордон

центра. И вот эти технологии унификации управления и объединения информационных потоков являются для нас важнейшей задачей.

Также мы планируем активно развивать наши EDR-продукты, причём с разной функциональностью для разных компаний. То, что 20 лет назад начиналось как антивирус, превратилось в мощное многокомпонентное решение — оно функционирует как самодостаточная защитная единица, которой достаточно своих технологий и логики. Принципиальное же отличие EDR в том, что фактически это среда управления информационной безопасностью — эти продукты позволяют искать следы сложных угроз, иметь полную картину состояния всей сети и, главное, быстро реагировать на замеченные угрозы, причём самыми разными средствами. В нашем понимании заказчик от 500 узлов уже может получить ощутимую выгоду от использования решений класса EDR в своей инфраструктуре.

«ЛЮДСКОЙ FIREWALL»

— Как вы относитесь к повышению грамотности сотрудников?

— Сколько бы вы ни инвестировали в дорогие средства защиты, рано или поздно неумелый пользователь, имеющий какой-то набор прав, совершит ошибку, и все ваши старания пойдут прахом.

Фактически основной угрозой является фишинг, социальная инженерия. И ничего нельзя поделать с людьми, которые открывают письма с привлекательными заголовками или, как им кажется, письма от доверенных партнёров или руководства. Они их открывают, нажимают на ссылки, открывают вложения. В результате злоумышленник захватывает учётную запись и использует этот вход как точку распространения контроля внутри сети. Множество атак, приводящих к многомиллионным ущербам, начинается именно так. Посмотрите, насколько важную роль

в структуре областей работы директора по ИБ, очень системно изложенной, например, в курсе ISACA® на сертификацию CISM®, занимает раздел, посвящённый осведомлённости и обучению персонала.

В общем, единственный, на мой взгляд, эффективный путь — это создание *human firewall*, то есть превращение сотрудников в обученный, настороженный защитный кордон, воспринимающий любое письмо или сообщение как подозрительное. Обучить этому можно только за счёт привлечения эмоциональной составляющей в рамках цикла регулярных тренингов. Чтобы воспринять информацию глубоко и не забывать её, сотрудник должен пережить её в жизни, игре или на тренинге, причём в рамках некоторого цикла. Через такой цикл обучения, предполагающий эмоциональность, вовлечённость и периодичность, удаётся в итоге сформировать новый поведенческий шаблон, который действительно превращает «офисного хомячка» во внештатного сотрудника службы ИБ. Именно такие принципы заложены в основе нашей обучающей платформы Automated Security Awareness Platform, ASAP. Ей уже больше двух лет, и она продолжает активно развиваться.

СОВЕТЫ

— Какие советы по защите от киберпреступников вы могли бы дать крупным компаниям (помимо приобретения продуктов «Лаборатории Касперского»)?

— Специфика «Лаборатории Касперского» в том, что к нам стекаются насущные проблемы, желания и боли из сотен компаний, и мы все их анализируем. Поэтому какие-то полезные советы я дать могу.

Во-первых, рекомендовал бы очень серьёзно относиться к угрозам, которые кажутся примитивными, понятными и потенциально не очень опасными. В первую очередь речь об угрозах

шифровальщиков. Они не только приводят к потере корпоративных данных, но и ставят под угрозу человеческие жизни, когда шифрованию подвергается, например, медицинское оборудование. Мы настоятельно рекомендуем компаниям иметь бэкапы, располагать их в обособленной инфраструктуре, внедрить и поддерживать систему управления уязвимостями, обучить персонал видеть и выявлять признаки социальной инженерии в любых коммуникациях.

Во-вторых, растёт желание наших клиентов передавать задачи ИБ на аутсорсинг, и это отранно. На мой взгляд, многие сервисы, такие как мониторинг, администрирование отдельных систем ИБ, расследование простых инцидентов и даже проактивный поиск следов атак, вполне могут быть переданы доверенной российской компании, использующей надёжный инструментарий. Но! Крайне важно при этом не растерять собственный экспертный потенциал. Речь о высококлассных экспертах-безопасниках, работающих в компании годами, к мнению которых прислушивается бизнес. Именно они должны задавать требования к сервисам, выбирать оптимальных поставщиков и отслеживать качество услуг. Потому что невозможно оценить качество сервиса на аутсорсинге, не имея надёжной экспертизы внутри компании.

Ну и про актуальное для этого непростого года. Боюсь, что удалённый режим работы пришёл в нашу жизнь всерьёз и надолго. Это не временное явление, поэтому надо менять к нему отношение. Фактически сеть большинства компаний превращается из консолидированной в распределённую, состоящую из массы домашних микроофисов. Их безопасность необходимо рассматривать в парадигме новой политики безопасности. В частности, необходимо распространить принцип владения конечной точкой на компанию, обеспечить установку на этой конечной точке всех корпоративных систем безопасности, активно развивать терминальные и виртуальные технологии и так далее. Сегодня это реальность, которую мы вынуждены принять и именно исходя из неё строить новую стратегию жизни и, соответственно, её безопасности.



Тимур ЗИННЯТУЛЛИН
директор Центра
киберустойчивости ACRC

СТУПЕНЬЮ ВЫШЕ

ЦЕНТР КИБЕРУСТОЙЧИВОСТИ ANGARA CYBER
RESILIENCE CENTER ОТМЕНИЛ ГРАНИЦЫ

Острую потребность в организации качественного мониторинга и реагирования на инциденты ИБ испытывают предприятия как крупного, так и среднего и малого бизнеса. Отслеживать состояние информационной инфраструктуры, предотвращать и нейтрализовать последствия кибератак можно несколькими способами. Строить собственный SOC (Security Operations Center) либо покупать стандартизированный пакет необходимых услуг у коммерческих SOC. В ряде случаев сложившееся разделение между практиками предоставления услуг интеграторов и сервисных услуг безопасности снижает эффективность процесса мониторинга ИБ, поскольку не даёт инструменты для решения специфических и уникальных задач бизнеса в каждой отдельно взятой организации. В этой статье мы расскажем, как группа компаний Angara решила сложившуюся проблему путём запуска сервисов Managed Detection and Response Services (MDRS).

ЕСТЬ ТОЛЬКО ДВА ПУТИ?

Сегодня у функционального заказчика есть два варианта решения задачи по автоматизации процессов ИБ в части мониторинга событий, их последующего анализа и реагирования на возможные подозрения или инциденты. Отдать мониторинг ИБ на аутсорсинг коммерческому SOC либо обеспечивать

данный процесс с использованием собственного штата экспертов и средств защиты информации, наняв экспертизу у интегратора для их проектирования, внедрения, настройки и технического сопровождения.

Во втором случае на нашей практике заказчики нередко сталкиваются с проблемой, когда технические решения внедрены и работают, а трудовых ресурсов для полноценной реализации самого процесса мониторинга и реагирования нет или их недостаточно. В зависимости от имеющейся стадии зрелости процессов SOC — SOMM (Security Operations Maturity Model) здесь скажется как высокая стоимость ФОТ, так и кадровый дефицит в этой области, с которым многие сталкиваются на протяжении последних лет. При этом передать эту функцию на аутсорсинг редко представляется возможным, поскольку чаще всего коммерческие SOC отказываются работать по данному направлению с использованием сторонних решений заказчиков, которые не применяются в основе их услуги. И это одно из немногих ограничений, которые существуют в рамках сложившегося разделения между двумя способами решения на сегодняшний день.

В результате необходимое развитие жизненных циклов процессов мониторинга ИБ замедляется, а в крайнем случае и вовсе откладывается, оставляя заказчика и его команду на той же стадии зрелости, что были в конце этапа внедрения, с постоянно растущей

информационной инфраструктурой и создающимися сервисами. Суровая статистика ряда известных игроков в индустрии однозначно показывает, к чему это обычно приводит: до половины оповещений о возможных угрозах ИБ могут оставаться необработанными, а в отношении оставшейся обработанной половины не всегда применяются минимально необходимые меры по предотвращению или ликвидации угрозы. При наличии подобных пробелов в столь критичном для защиты бизнеса и его интересов направлении с учётом сегодняшнего перечня угроз высока вероятность оказаться в составе той самой статистики, учитывая, что только от ransomware за 2020 год пострадал 51 % представителей крупного бизнеса, согласно отчёту Sophos. И это только те случаи, о которых заявили публично.

SOC ON-PREMISE ИЛИ OUTSOURCE? БОЛЬШЕ НЕ НАДО ВЫБИРАТЬ

Группа компаний Angara решила стереть границу между SOC on-premise и SOC outsource и предложить заказчикам самим выбирать, как «перемешивать» эти направления в соответствии с особенностями стоящих перед ними задач и проблем. Для этого мы представляем рынку новое ценностное предложение в рамках обновлённого Центра киберустойчивости ACRC — MDRS, которое объединит классические услуги по обоим направлениям и удовлетворит самые специфичные запросы

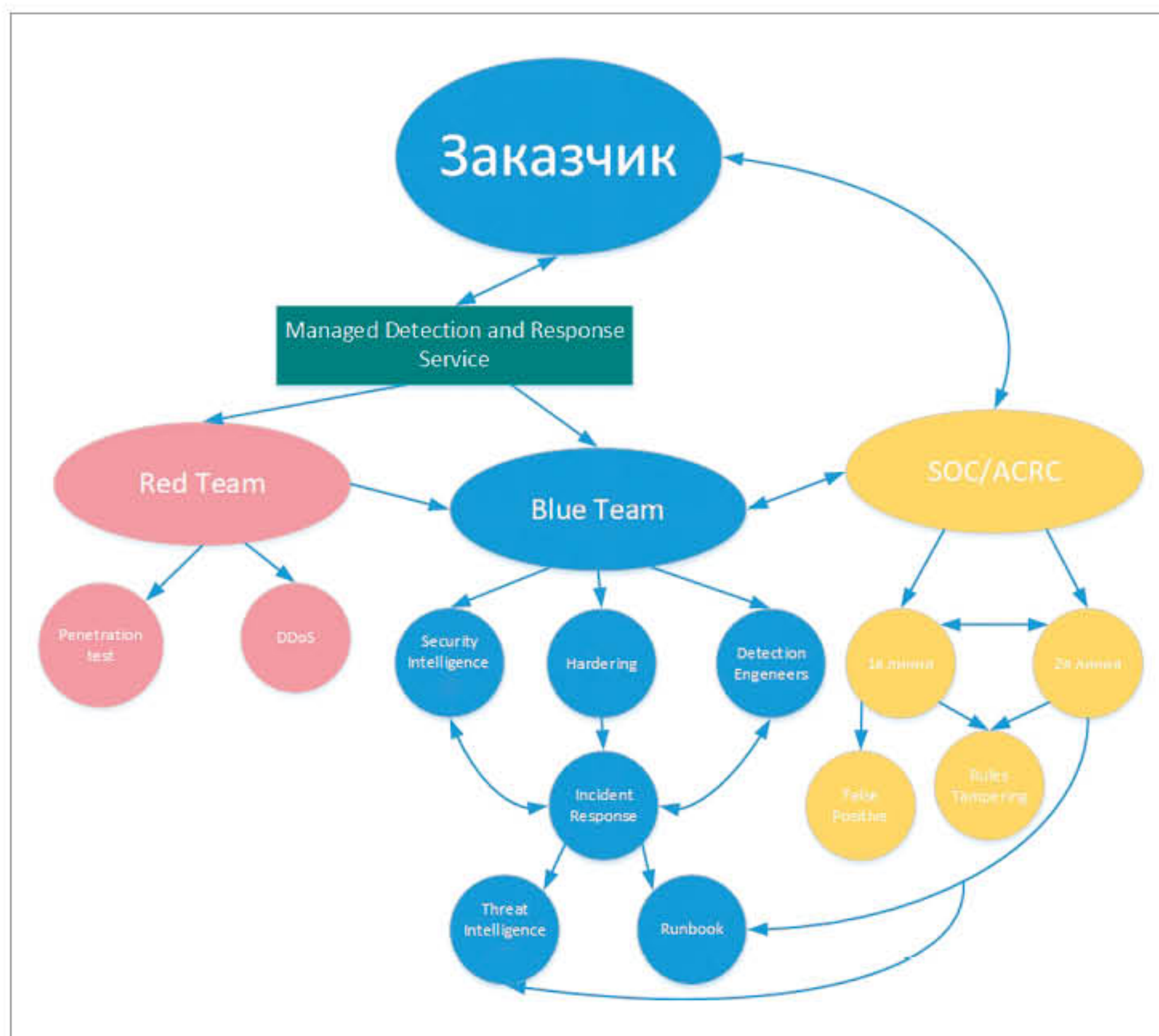


Рисунок 1. Верхнеуровневая схема взаимодействия сервисных подразделений в рамках модели MDRS

бизнеса, предвосхитив тем самым рост потребностей в MDRS в течение ближайших двух-трёх лет.

Напомним, что в классический перечень услуг интеграторов в рамках решения задач по направлению мониторинга информационной безопасности входят:

- ♦ автоматизация процессов ИБ в части организации мониторинга событий (SIEM/SEM);
- ♦ обогащение процессов ИБ сторонней аналитикой (Security Feeds & TI);
- ♦ мониторинг и управление инцидентами ИБ (SIEM/IR-SOC);
- ♦ автоматизация управления и реагирования на инциденты ИБ (IRP/SOAR-SOC);
- ♦ визуализация и контроль метрик эффективности (SI-SOC).

Классический перечень услуг в рамках коммерческих SOC с применением использующихся у них решений включает:

- ♦ обнаружение и анализ инцидентов ИБ;
- ♦ оценка и принятие эффективных мер реагирования на инциденты ИБ;

- ♦ выработка рекомендаций по осуществлению превентивных защитных мер и улучшение общего подхода к управлению инцидентами ИБ;

- ♦ минимизация воздействия инцидентов ИБ на бизнес-процессы заказчиков.

В рамках запущенной модели оказания услуг MDRS клиенты получают возможность подключить Red team, Blue team, Purple team и SOC L1/L2 в любом формате, на любом этапе и платформе. Также в предложение компании входят: совместная разработка карт реагирования и карт контактов, регламентов взаимодействия, карточек ролей и полномочий, матриц RACI и другой операционной нормативной базы, совместная или экспертная разработка сценариев детектирования угроз, параметров hardening (настройки аудита) контролируемых объектов информационной инфраструктуры и их согласование с Data Castodian (владельцами сервисов заказчика), с одновременным наполнением и сохранением результатов в базах знаний заказчиков. В рамках

Red Team, кроме классических услуг данного направления, также доступна услуга по проверке стойкости используемых в информационной инфраструктуре паролей.

В портфеле обновлённого Центра киберустойчивости ACRC, помимо собственной запатентованной платформы ACR Platform, находятся решения, занимающие остальные основные доли сегодняшнего рынка решений класса SIEM, а также решения класса IRP/SOAR, Security Intelligence (BI для ИБ) и аналитический программный комплекс Dataplan, позволяющий работать с большими данными и, применяя алгоритмы машинного обучения и статистического анализа, строить по этим данным метрики, покрывая дополняющую SOC деятельность по ретроспективному анализу больших данных.

ВОЗМОЖНОСТИ MDRS

Сервис MDRS по модели подписки обладает неоспоримыми преимуществами. Во-первых, он обеспечивает интерактивность в проведении любых видов работ, предоставив возможность реализации повторяемого и циклического процесса обмена экспертизой по направлению SOC, играющего столь важную роль во всех областях информационной безопасности. Во-вторых, позволяет сместить фокус на операционные расходы в тех случаях и для тех заказчиков, для которых это является важным аспектом в процессах управления финансами предприятия. В-третьих, выборочное привлечение экспертизы для работы на уже внедрённых решениях позволит не потерять вложенные ранее средства, а также накопить собственный опыт в данном большом направлении ИБ в ходе обмена компетенциями, повысив тем самым эффективность всех процессов ИБ в целом.

Обновлённый перечень услуг в рамках взаимодействия с Центром киберустойчивости ACRC смотрите в таблице 1.

ПОЧЕМУ ГРУППА КОМПАНИЙ ANGARA

Запустить модель MDRS позволяет накопленная экспертиза как коммерческого SOC группы компаний Angara

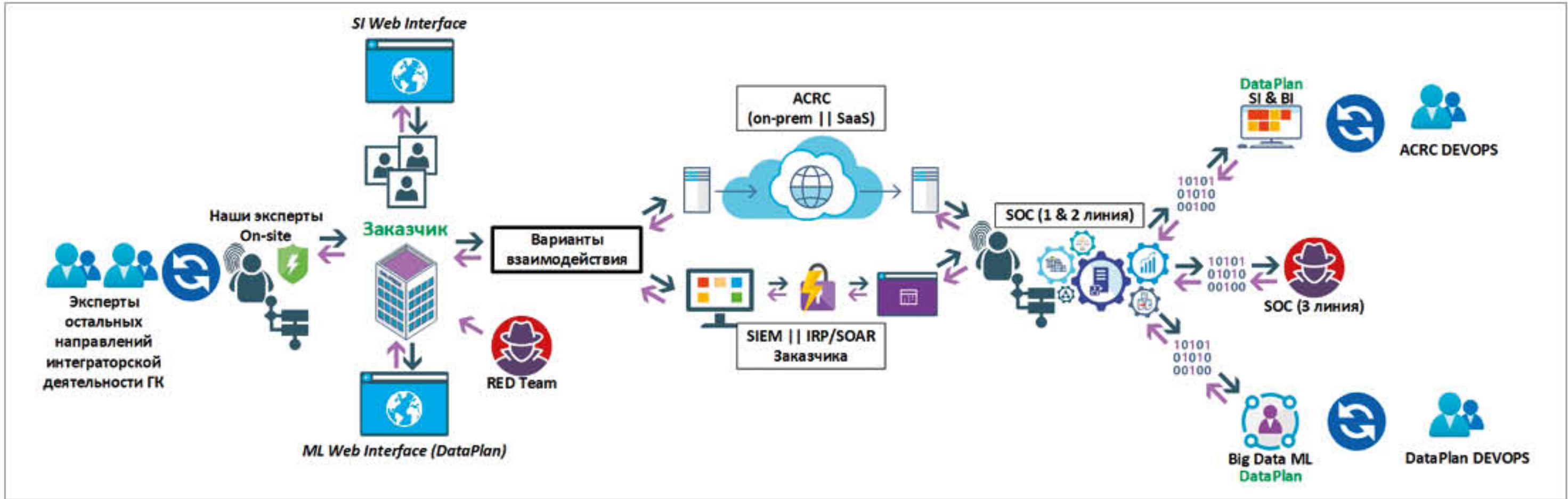


Рисунок 2. Схема оказания услуг в рамках модели MDRS

(Центр киберустойчивости ACRC), так и отдела систем мониторинга и реагирования.

ACRC оказывает услуги по мониторингу и выявлению инцидентов информационной безопасности в круглосуточном режиме. С 2019 года является оператором ГосСОПКА. Среди пользователей сервисов — кредитно-финансовые организации, телекоммуникационные и транспортные компании.

Отдел систем мониторинга и реагирования, помимо реализации проектов по внедрению решений класса SIEM, SGRC, IRP/SOAR, Security Feeds & TIP и Security Intelligence, вносит активный вклад в улучшение общего состояния отрасли. Так, экс-руководитель отдела, а сегодня директор Центра киберустойчивости ACRC Тимур Зинятуллин — один из организаторов международной инициативы Open Security Collaborative Development (OSCD). Кроме того, эксперты развивают открытые репозитории со сценариями детектирования угроз (Sigma).

Объединив накопленный опыт двух направлений, группа компаний Angara обеспечивает более комплексный подход к решению любых функциональных задач, стоящих перед заказчиками по всем веткам направления мониторинга событий, их обогащения и последующего анализа, а также реагирования на возможные подозрения или инциденты информационной безопасности.

Услуга MDRS

Автоматизация процессов ИБ в части мониторинга [On-premise или Out-source]

Автоматизация процессов ИБ в части реагирования [On-premise или Out-source]

Обогащение процессов ИБ сторонней аналитикой [On-premise или Out-source]

Мониторинг событий ИБ, выявление и управление инцидентами ИБ [On-premise или Out-source]

Мониторинг инцидентов ИБ и реагирование на инциденты ИБ [On-premise или Out-source]

Визуализация и контроль метрик эффективности [On-premise или Out-source]

Red Team [Software или Physical]

Purple Team [On-premise или Partial-Out-source]

Методологическое сопровождение

Какую задачу решает

Увеличение количества контролируемых объектов информационной инфраструктуры (далее — ИИ) без увеличения текущего штата ИБ

Увеличение количества анализируемых угроз ИБ для контролируемых объектов ИИ без увеличения текущего штата ИБ

Получение информации об актуальных угрозах ИБ, уменьшение количества ложноположительных срабатываний

Увеличение количества выявляемых угроз ИБ на контролируемых объектах ИИ без увеличения текущего штата ИБ

Увеличение скорости анализа инцидентов ИБ на контролируемых объектах ИИ без увеличения текущего штата ИБ

Оценка эффективности процессов (BI) и эксплуатируемых СЗИ и сотрудников ИБ (SI)

Контроль эффективности процессов мониторинга событий ИБ, выявления и управления угрозами и инцидентами ИБ

Повышение квалификации ответственных за процессы мониторинга событий ИБ, выявления и управления угрозами и инцидентами ИБ

Разработка и актуализация внутренней документации, начиная с функциональных матриц RASCI, карточек ролей и полномочий, заканчивая регламентами по взаимодействию и положениями о подразделениях

Таблица 1. Обновлённый перечень услуг в рамках взаимодействия с Центром киберустойчивости ACRC



Дмитрий КАНДЫБОВИЧ
генеральный директор StaffCorp,
ООО «Атом Безопасность»

НА ТРЁХ КИТАХ

STAFFCORP ENTERPRISE ОСУЩЕСТВЛЯЕТ КОНТРОЛЬ НАД ЛЮБЫМИ ОПЕРАЦИЯМИ С ЛЮБЫМИ ОБЪЕКТАМИ

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ СОГЛАСНО ТРЕБОВАНИЯМ РД

В этой статье мы рассмотрим требования из следующего списка приказов и положений:

- ♦ Приказ ФСТЭК России от 25 декабря 2017 г. № 239 (далее — № 239)
- ♦ Приказ ФСТЭК России от 18 февраля 2013 г. № 21 (далее № 21)
- ♦ Положение от 9 июня 2012 года № 382-П (далее — № 382-П)
- ♦ Приказ ФСТЭК России от 11 февраля 2013 г. № 17 (далее — № 17)
- ♦ ISO 27001
- ♦ Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры» (КИИ) (далее — № 187-ФЗ)

Мы сгруппируем требования этих документов по основным направлениям и рассмотрим, какие функции должна предоставлять система контроля сотрудников:

1. Контроль машинных носителей, стороннего ПО и состава АРМ
2. Контроль операций с файлами/ресурсами и контроль печати документов
3. Регистрация и просмотр зарегистрированных событий
4. Контроль сетевого трафика
5. Контроль системы защиты на АРМ

Рассмотрим каждую группу через призму функциональности программного комплекса Staffcorp Enterprise, имеющего сертификат ФСТЭК № 4234 и предназначенного для реализации мер защиты согласно

приказам ФСТЭК России № 17, 21, 31, 239 (напрямую относится к № 187-ФЗ) в составе автоматизированных систем (АС) до класса защищённости 1Г; информационных систем персональных данных (ИСПДн); государственных информационных систем (ГИС); на объектах критической информационной инфраструктуры (КИИ).

КОНТРОЛЬ МАШИННЫХ НОСИТЕЛЕЙ, СТОРОННЕГО ПО И СОСТАВА АРМ

Для этой группы приказы ФСТЭК № 17 и 239 содержат требования по контролю МНИ: контроль подключения; управление доступом; контроль ввода/вывода информации; а также контроль состава ТС, ПО и СЗИ.

Приказ ФСТЭК № 21 содержит требования:

- ♦ по контролю МНИ: контроль копирования информации; блокировка незарегистрированных МНИ и запрещённой к передаче информации; регистрация фактов стирания информации;
- ♦ по контролю ПО: исключение установки/запуска незарегистрированного ПО; регистрация и контроль установки/удаления/обновления/запуска и состава используемого ПО;
- ♦ по контролю АРМ: учёт и контроль фактического состава ресурсов и объектов доступа.

Staffcorp Enterprise позволяет определить список разрешённых к использованию МНИ (причём назначить разным

пользователям разные возможности взаимодействия с МНИ) и осуществляет регистрацию всех действий с МНИ — чтение, запись или удаление файлов, простое подключение МНИ (об этом может сразу же уведомлять ответственных лиц). Причём это может быть USB или CD-накопитель.

С помощью функций «Инвентаризация программного обеспечения/оборудования» Staffcorp позволяет осуществлять контроль за изменением состава АРМ, а также попыток установки и запуска стороннего программного обеспечения. Причём это относится не только к АРМ, но и к, например, банкоматам на системах Windows и Linux.

КОНТРОЛЬ ОПЕРАЦИЙ С ФАЙЛАМИ/РЕСУРСАМИ И КОНТРОЛЬ ПЕЧАТИ ДОКУМЕНТОВ

В требования приказов ФСТЭК № 21 и 239 для этой группы входят: контроль операций по созданию/удалению / резервному копированию ресурсов доступа; регистрация фактов вывода на печать и защита информации от утечек.

Также добавляется Положение Банка России № 382-П — требование запрета несанкционированного копирования информации.

Staffcorp регистрирует все факты отправки документов на печать, а также сохраняет теневые копии распечатанных файлов, позволяя распечатывать их самому администратору безопасности. Конечно же, в системе записывается

полная информация касательно инцидента — кто, когда, на каком принтере, с какой рабочей станции пытался распечатать документ.

В рамках имеющейся функции под общим названием «Файловый контроль» Staffcop Enterprise осуществляет контроль над любыми операциями с любыми объектами. Это касается как файлов данных, так и сетевых папок и т.п. — система регистрирует все факты взаимодействия с ресурсами.

РЕГИСТРАЦИЯ И ПРОСМОТР РЕГИСТРИРОВАННЫХ СОБЫТИЙ

Для этой группы приказы ФСТЭК № 17, 21 и Положение № 382-П требуют регистрировать все действия персонала и используемые ресурсы доступа, а также иметь возможность просматривать и анализировать события безопасности, в том числе по каждому конкретному пользователю.

Инструмент должен позволять собирать доказательную базу. Цитируя Приказ ФСТЭК № 17, «Исключение возможности отрицания пользователем факта отправки информации другому пользователю или факта получения информации от другого пользователя» смело можно сократить до «Исключение возможности отрицания пользователем фактов». Staffcop собирает наиболее полную информацию — регистрирует все события и взаимодействия, осуществляет теневое копирование всех внесённых в файлы изменений и формирует базу данных, которая представляется в удобной форме: в виде графиков, таблиц, тепловых диаграмм и т.д., что значительно ускоряет обработку инцидентов информационной безопасности.

Staffcop связывает события, относящиеся к одному пользователю, в единую систему, что позволяет на временной линии отследить, с кем сотрудник контактировал и чем он пользовался.

Кроме того, инструмент «Детектор аномалий» выявляет отклонения от нормы поведения сотрудника — например, чрезмерное увеличение распечатки документов или копирования файлов. Это позволяет быстрее выявлять и реагировать на опасные для компании действия.

Инструмент «Детектор аномалий» выявляет отклонения от нормы поведения сотрудника — например, чрезмерное увеличение распечатки документов или копирования файлов. Это позволяет быстрее выявлять и реагировать на опасные для компании действия

А также это строгий учёт времени работы сотрудника — включая все прогулы, опоздания, уход с рабочего места и простои. Имея полную картину того, как сотрудник тратит рабочее время, гораздо проще выявить инциденты ИБ или недобросовестных сотрудников.

КОНТРОЛЬ СЕТЕВОГО ТРАФИКА

В этой группе приказы ФСТЭК № 17 и 21 требуют выявлять и блокировать скрытые каналы передачи данных; контролировать и анализировать сетевой трафик, циркулирующий внутри и поступающий в/исходящий из информационной системы; контролировать, анализировать и при необходимости блокировать передаваемую информацию. Приказы № 239 и 21 также требуют регистрировать все операции работников в сети Интернет и блокировать запрещённые к использованию сайты.

Контроль интернет-ресурсов, которыми пользуются сотрудники, является очень важным, а особенно важен контроль сообщений, которыми обмениваются сотрудники с посторонними лицами. Staffcop позволяет определять содержимое сообщений — по словам, регулярным выражениям, сочетаниям слов и т.д. Содержание входящих и исходящих сообщений фиксируется, делаются скриншоты во время посещения веб-ресурсов, а также при заполнении веб-форм. Staffcop контролирует любую передачу информации по любому каналу, что и является основой требований РД.

КОНТРОЛЬ СИСТЕМЫ ЗАЩИТЫ НА АРМ

В эту группу согласно требованиям Приказов ФСТЭК № 17 и 21 входят функции контроля и регистрации

изменений параметров системы защиты или её отключения и возможности удалённого контроля/перехвата управления.

Staffcop позволяет осуществлять удалённое управление АРМ, позволяя вносить изменения в конфигурацию рабочих мест, а также осуществлять контроль в онлайн-режиме и прекращать логический доступ к защищаемой информации при необходимости. Эта функция является необходимой как для защиты информации, так и для системного администрирования, позволяя быстрее реагировать на сообщения от пользователей.

ЗАКЛЮЧЕНИЕ

Как мы показали, несмотря на многообразие руководящих документов, набор функций для систем контроля, в том числе и для объектов ККИ, является ограниченным. И, по большому счёту, система должна стоять на трёх китах:

1. Контроль и регистрация всех без исключения событий в информационной системе предприятия — непосредственно на АРМ, при сетевом взаимодействии и при подключении внешних носителей.

2. Контроль состояния самого АРМ и системы защиты — с регистрацией и/или запретом всех изменений.

3. Представление всей собранной информации в удобном формате для обеспечения сбора доказательной базы и получения полной картины происходящего.

Наличие сертификата ФСТЭК подтверждает, что система защиты способна обеспечить выполнение всех требований РД в этих трёх аспектах, а в случае Staffcop — это ещё и дополнительные функции, невысокая стоимость, передовые технологии и качество исполнения.



Ольга ПОПОВА
директор по развитию бизнеса
компании «Индид»

«МЫ ДЕРЖИМ РУКУ НА ПУЛЬСЕ ВРЕМЕНИ»

КОМПАНИЯ «ИНДИД» СОЗДАЁТ ЭКОСИСТЕМУ ПРОДУКТОВ ДЛЯ ОРГАНИЗАЦИЙ ФИНАНСОВОЙ СФЕРЫ

— Компания «Индид» работает на рынке средств защиты информации более 10 лет и имеет весомый опыт разработки и внедрения своих продуктов. Как вы оцениваете текущие потребности заказчиков в вопросах информационной безопасности?

— Действительно, мы наблюдаем тенденцию изменения задач заказчиков с течением времени. И эти изменения отражаются на наших продуктах. Компания «Индид» выходила на рынок с одним продуктом, предназначенным для усиленной аутентификации сотрудников, который закрывал текущие потребности заказчиков, но потребности менялись. Мы подстраивали своё ПО под них, расширяя функциональные возможности продукта. Анализируя накопленный опыт, мы поняли, что заказчикам нужно решать ещё и задачи по управлению цифровыми сертификатами. В ответ на запрос рынка мы разработали второй продукт: для автоматизации работы с инфраструктурой открытых ключей. В последнее время, исходя из нашего опыта и актуальных тенденций, мы сами можем прогнозировать будущие потребности заказчиков и формировать свои задачи на разработку. Несколько лет назад выпустили платформу для управления доступом привилегированных пользователей. А в ближайшем будущем

выпустим ещё один продукт. Работаем на опережение!

Отмечу, что наблюдается рост интереса к использованию IT-экосистем. Информационная безопасность не исключение: компании стремятся использовать ПО одного разработчика, способное закрыть их потребности в защите информации сразу по нескольким направлениям. Есть несколько причин использования «экосистем» продуктов: получение высокоуровневого сервиса, более высокого статуса среди других пользователей этой же системы, экономия времени и средств сотрудников и многие другие. Мы стремимся выпускать продукты, позволяющие любому бизнесу автоматизировать свои процессы в ИБ. Именно такую линейку продуктов и разрабатывает компания «Индид»: это наша «экосистема» решений для информационной безопасности заказчиков, используя которую они закрывают все свои задачи по контролю и управлению доступом линейных и привилегированных сотрудников, управлению жизненным циклом цифровых сертификатов и ключевых носителей.

Ещё одним аспектом, объясняющим тенденции к росту внедрений IT-экосистем, является переполненность рынка коробочными решениями, которые ограничены в своей

функциональности. То есть разработчики ПО очень редко кастомизируют свои продукты под потребности того или иного заказчика. Компания «Индид» одна из немногих, кто предлагает сервис доработки своих программных комплексов. У нас были случаи, когда приходилось кастомизировать компоненты платформ даже на этапе тестового внедрения. Для заказчика это означает, что мы готовы закрывать его потребности, даже когда речь идёт о поддержке узкоспециализированных продуктов или реализации нестандартных сценариев. Эти и другие доработки будут доступны и последующим заказчикам — все они входят в состав технических релизов, которые мы выпускаем 3–4 раза в год, дополняя функциональность каждого продукта.

— Расскажите об опыте решения задач технической защиты информации в организациях финансовой отрасли.

— У нас действительно большой опыт в этом направлении. Среди наших заказчиков Банк «Санкт-Петербург», «СДМ-Банк», «Абсолют банк», банк Armswissbank, «Беларусбанк», Альфа-Банк, и это только открытые кейсы. Расскажу несколько интересных.

В одном крупном банке была поставлена задача реализации двухфакторной аутентификации сотрудников при уда-

лётном доступе к корпоративным ресурсам по каналам VPN. Рассматривались разные варианты, но в итоге выбрали усиленную аутентификацию сотрудников по отпечатку пальца, как наиболее подходящую в этом случае. В результате внедрения Indeed Access Manager была создана централизованная система беспарольной аутентификации с использованием биометрии в ОС Windows и корпоративных приложениях.

В другой финансовой организации была реализована многофакторная аутентификация сотрудников при доступе в ОС по используемым RFID-картам. Для этого провели интеграцию наших платформ Indeed AM и Indeed CM со СКУД заказчика. В результате сотрудники используют одну карту для доступа в помещения банка и для аутентификации на рабочих местах.

Ещё один интересный кейс связан с внедрением системы управления

доступом привилегированных пользователей. Требовалось реализовать контроль за действиями внутренних сотрудников с расширенными правами в ИС банка. Решили задачу с помощью внедрения Indeed PAM для контроля и записи действий внутренних администраторов при работе с внутренними компонентами ИТ-инфраструктуры.

В целом у нас более 50 успешных проектов, реализованных в финансовой отрасли — банках, страховых компаниях и прочих.

— Помогает ли ПО «Индид» заказчикам в выполнении требований стандартов и других нормативно-правовых актов, предъявляемых к компаниям финансового сектора?

— Не секрет, что работу финансовых организаций регулирует множество требований, описанных в НПА.

Законодательство всесторонне регламентирует работу банков, МФО, страховых и подобных кампаний: от организации внутренней работы до вопросов защиты информации клиентов этих компаний. Основные требования перечислены в Приказах ФСТЭК № 21 и 239, ГОСТ 57580, PCI DSS, ISO 27001. Мы понимаем, какие требования отражены в этих документах и какой объём работы нужно провести в организации, чтобы эти требования выполнить.

У организаций финансовой отрасли есть несколько сложных задач в части организации ИБ, чтобы их деятельность соответствовала регламентирующим документам. Первая связана с сопоставлением своих информационных систем с наборами требований, описанных в каждом НПА и составлением общего перечня требований к защите информации во всей



Анатолий СКОРОДУМОВ
начальник управления по обеспечению
информационной безопасности,
Банк «Санкт-Петербург»

КОММЕНТАРИЙ ЗАКАЗЧИКА

«МЫ ДОВЕРИЛИСЬ КОМПАНИИ «ИНДИД»

Нас объединяет многолетнее сотрудничество. Банк начал использовать продукты компании «Индид» в 2012 году с внедрения аутентификации сотрудников по отпечатку пальца. С течением времени наши компании развивались: продуктовая линейка «Индид» расширялась в ответ на рост потребностей и задач. Иногда нам даже казалось, что они выполняют наш спецзаказ, хотя аналогичные задачи были и у других представителей финансовой сферы.

Когда видишь отклик на свои запросы, взаимодействие выходит на новый уровень. Мы доверились компании «Индид» и внедрили ещё два их продукта. Теперь используем все возможности, которые предоставляют эти программные комплексы: они дополняют функции друг друга и отлично интегрируются.

Получился эффективный комплексный подход к решению наших задач, связанных с автоматизацией ряда процессов в информационной безопасности. Продукты компании «Индид» настолько

вжились в наши бизнес-процессы, что мы уже не представляем себе, как эффективно и оперативно решать рабочие вопросы без использования этих платформ. Замечу, что на всех этапах внедрения и эксплуатации продуктов мы получаем поддержку от разработчика. При этом нам приятно сознавать, что наши пожелания и идеи всегда рассматриваются всерьёз для будущего развития продуктов. Мы с гордостью рассказываем о том, что сейчас используем у себя три программных комплекса «Индид».

ИТ-инфраструктуре. Вторая задача тоже ресурсоёмкая, она вытекает из первой, связана с проектированием комплексной системы информационной безопасности, учитывающей все требования, предъявляемые к ИТ-инфраструктуре организации. Поэтому сотрудникам департаментов ИБ приходится своими силами перерабатывать огромный объём информации о ПО, чтобы выбрать такое, которое поможет организации соответствовать требованиям.

Могут ли финансовые организации как-то облегчить себе выполнение этих задач? Конечно! Но, к сожалению, отечественные разработчики редко уделяют внимание разработке оценки выполнения требований НПА, которые можно реализовать с использованием их ПО. Чаще они просто заявляют, что выполняют эти требования, но не поясняют, какие именно требования помогут выполнить их продукты и каким образом.

Мы, понимая это, облегчаем процесс приведения системы защиты информации в соответствие с требованиями НПА. Для всех документов, о которых я говорила, нами подготовлены детализированные оценки выполнения требований НПА с помощью программных комплексов компании «Индид».

— Вы замечаете изменения в подходах к защите информации среди заказчиков финансового сектора?

— Любая компания — это прежде всего бизнес. Мы организовали свои внутренние процессы таким образом, что при разработке стратегии развития продуктов мы всегда отталкиваемся от потребностей заказчика в решении вопросов информационной безопасности и рассматриваем эти вопросы через призму бизнеса. Соответственно, мы «держим руку на пульсе», наблюдая за тем, как эволюционируют потребности наших заказчиков, и оперативно реагируем на все изменения. Ещё недавно

акцент защиты информации был смещён в сторону решения разрозненных технических задач, а комплексный подход отсутствовал. Теперь заказчики рассматривают информационную безопасность как полноценный бизнес-процесс.

При этом информационная безопасность как бизнес-процесс не сводится к применению только технических инструментов. Важными составляющими стали документационное обеспечение и персонал. Исходя из этого, наш подход тоже эволюционирует. Сейчас мы делаем большой акцент на то, как наши продукты выполняют требования законодательства, насколько их легко эксплуатировать и использовать для оперативного реагирования на различные инциденты.

К сожалению, в современном законодательстве отсутствует ряд требований, направленных на повышение эффективности и удобство эксплуатации системы защиты информации. Например, нет требований, предъявляемых к цен-



Владимир СОЛОНИН
директор по информационной безопасности, СДМ-Банк

КОММЕНТАРИЙ ЗАКАЗЧИКА

«У НИХ ЕСТЬ УНИКАЛЬНЫЙ БОНУС...»

Мы очень часто взаимодействуем с командой поддержки «Индид», так как банк развивается и наши потребности растут. Во-первых, периодически требуется поддержка какого-либо нового оборудования. Во-вторых, мы постоянно улучшаем свой продукт, используем новые инструменты, а это значит, что наши бизнес-процессы тоже меняются и, как следствие, требуется доработка используемых продуктов.

При каждом обращении в «Индид» мы получаем неизменно высокий уровень поддержки, который включает в

себя не только отработку заявок, но и консультации по вопросам более эффективного использования продуктов «Индид». Саму поддержку мы получаем в разных форматах. Чаще нам хватает онлайн-консультаций, но бывает, требуется и выезд специалистов. И всегда мы остаёмся довольны результатом. Что нам нравится больше всего? Оперативность! Команда «Индид» использует современный инструментарий, например, можно оставить заявку на портале или сразу задать вопрос в онлайн-чате. Консультант всегда на месте!

Неоспоримым преимуществом «Индид» я бы назвал уникальный бонус, который, я так думаю, получает каждый заказчик. Это включение в сервис технической поддержки небольших доработок продуктов «Индид» под наши потребности. Мы запрашивали даже масштабные доработки (не нарушающие концепцию продуктов компании) и получили их в рамках дополнительного соглашения. Конечно, долгосрочные проекты требуют отдельной проработки и обсуждения, но «Индид» всегда идёт навстречу.

трализованному управлению доступом в корпоративные системы, и заказчикам приходится использовать несколько разных инструментов для закрытия этих задач. А это, в свою очередь, влечёт дополнительные расходы финансовых, временных и трудовых ресурсов.

Мы — за комплексный подход! И поэтому предлагаем комплексные решения — ту самую «экосистему» продуктов, о которой я говорила.

— Расскажите, пожалуйста, об актуальных направлениях развития компании «Индид».

— Как я уже говорила, потребности наших заказчиков эволюционируют. Развиваются технологии, появляются новые задачи, новые концептуальные направления. Например, за последние 5 лет резко возросло использование

облачных сервисов, а корпоративная мобильность развивается семимильными шагами почти 10 лет. Каждый из таких примеров — вызов для разработчиков. И мы должны не просто замечать их и пассивно реагировать, а использовать свои ресурсы и знания для прогнозирования будущих потребностей рынка.

Например, простым управлением доступом сотрудников в ОС уже никого не удивить. Сегодня заказчики хотят получить инструменты анализа действий сотрудников и единого мониторинга событий этого доступа. Причём не в виде сложного для восприятия текста, а в виде красивых графиков, скриншотов и даже видеозаписи того, что видел этот сотрудник на своём мониторе. Это удобно и позволяет экономить ресурсы специалистов, осуществляющих контроль за другими сотрудниками.

Мы делаем большой упор на развитие собственных сервисов, оказываемых заказчикам, и создаём собственную «экосистему» продуктов, которые берут на себя автоматизацию рутинных операций. Такой подход к ИБ даёт специалистам по безопасности рычаги для оперативного управления ситуациями и удобные панели мониторинга, благодаря которым можно сэкономить финансовые и временные ресурсы, повысить производительность труда, не говоря уже о повышении общего уровня информационной безопасности.

Мы стремимся выпускать лучшее ПО и предоставлять лучший сервис на рынке. Внедрение наших платформ приносит свои выгоды каждому участнику в цепочке разработчик — партнёр — заказчик.



Александр САМУТКИН
руководитель направления информационной безопасности, SoftwareONE Company

КОММЕНТАРИЙ ПАРТНЁРА

«100% РОССИЙСКИЙ РАЗРАБОТЧИК»

К выбору партнёра мы всегда подходим очень щепетильно, так как значение имеют много разных аспектов. Сотрудничество с компанией «Индид» соответствует всем нашим требованиям и ожиданиям. Больше всего нас заинтересовало в этой компании то, что она разрабатывает продукты сама, то есть это 100% российский разработчик. Это значит, что её продукты не просто будут востребованы на рынке и закроют актуальные задачи наших заказчиков, но и круг потенциальных потребителей будет значительно шире по сравнению с зарубежными аналогами.

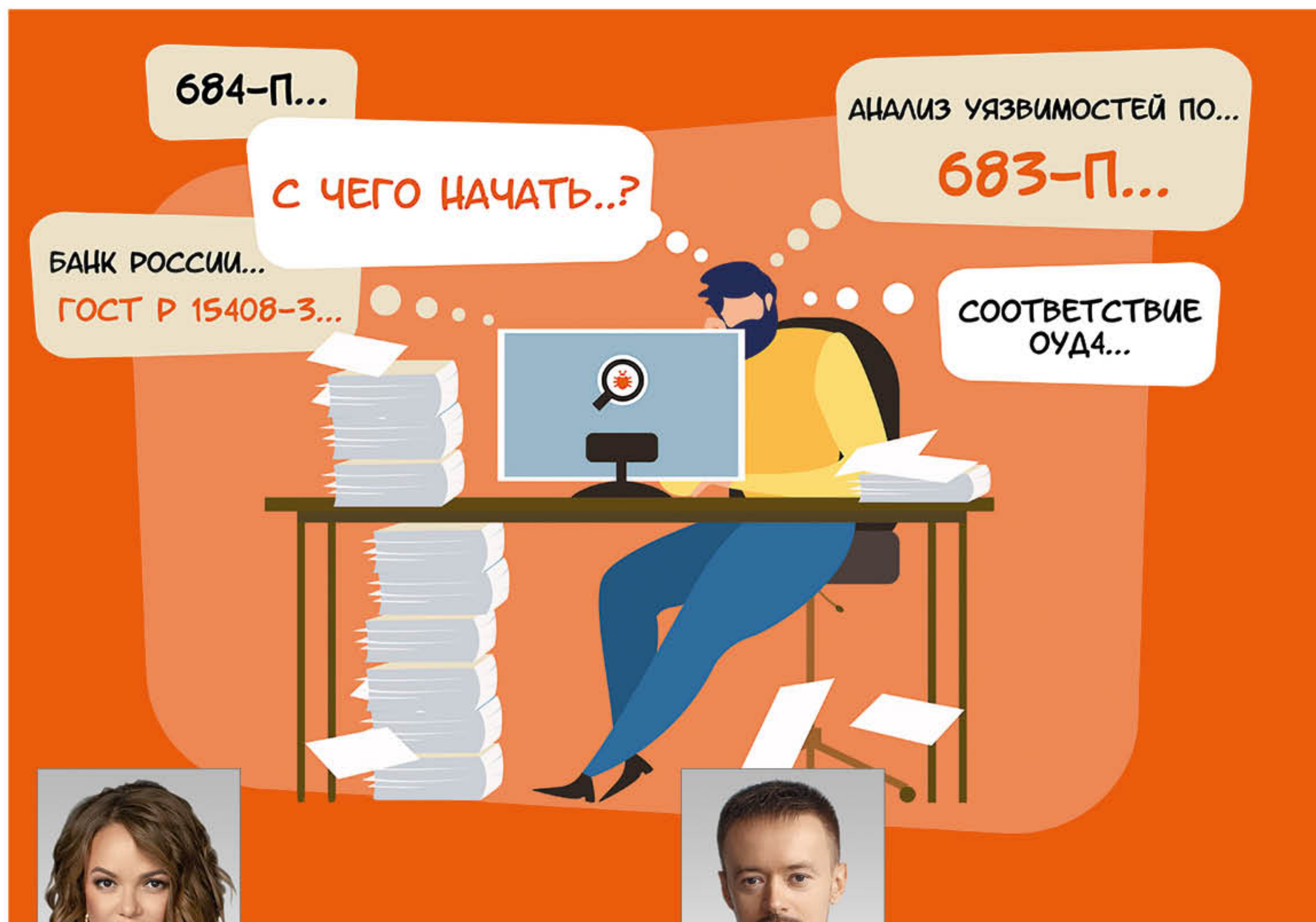
Компания «Индид» предоставляет возможности для обучения наших технических специалистов, в процессе которого

максимально полно показываются и описываются нюансы внедрения и эксплуатации продуктов. Если такого обучения ещё не произошло, то вендор готов предоставить всеобъемлющую помощь своим партнёрам в вопросах поддержки внедрённого ПО. То есть, если интегратор на начальном этапе развития партнёрских отношений не может оказывать первую и вторую линию технической поддержки своим заказчикам, то компания «Индид» возьмёт решение этой задачи на себя.

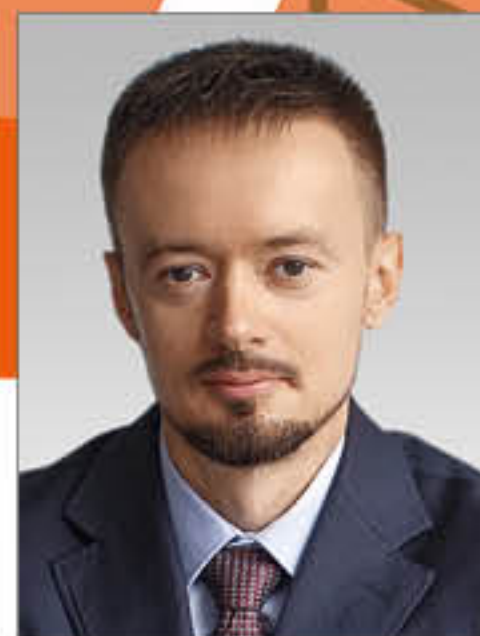
Если говорить о таких продуктах «Индид», как решения по управлению доступом, то у них есть одна особенность — это необходимость их глубокой интеграции в ИТ-инфраструктуру заказчика. Такие решения нельзя назвать

коробочными, они всегда требуют грамотного внедрения для обеспечения всех заявленных функциональных возможностей. В этом вопросе технические специалисты «Индид» всегда готовы проконсультировать нас либо подключиться самостоятельно.

Коллеги готовы обсуждать индивидуальные условия взаимодействия, всегда стараются погрузиться в нашу проблематику и специфику. В особенности это актуально для региональных проектов. Такой подход позволяет нам вести совместные сделки с разным уровнем участия, в зависимости от масштабов или других факторов. Наше эффективное взаимодействие помогает успешно реализовывать любые проекты.



Анастасия ХАРЫБИНА
директор по развитию
AKTIV CONSULTING



Павел СЕМЁНОВ
консультант
по информационной безопасности
AKTIV CONSULTING

ДЕРЖИТЕ УРОВЕНЬ!

КАК АНАЛИЗИРОВАТЬ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ПО ОУД4

Банки и некредитные финансовые организации всё чаще задаются вопросом, как провести анализ программного обеспечения в соответствии с требованиями ОУД4 ГОСТ Р 15408-3. С января 2020 года вступили в силу требования положений Банка России 683-П, 684-П и 382-П об анализе уязвимостей ПО финансовых организаций в соответствии с ОУД4. Интерпретация этих требований вызывает противоречия и многочисленные дискуссии у экспертов.

КАКОЕ ПО ПОДЛЕЖИТ АНАЛИЗУ ПО ОУД4?

Любая финансовая организация обладает обширным парком ПО и автоматизированных систем (АС). Что же из этого парка подлежит анализу уязвимостей по ОУД4? Для начала необходимо определить, какие операции проводятся в организации, и выделить среди них те, о которых говорят 683-П/684-П и 382-П/719-П. Для кредитных организаций это такие банковские операции, как переводы денежных средств, открытие счетов, генерация выписок

и прочее. А для некредитных финансовых организаций (НФО), например, покупка страхового полиса, покупка/продажа активов на бирже, платежи за накопительную пенсию. Затем следует проанализировать весь парк АС и отобрать те, которые участвуют в финансовых операциях.

Для банков, в первую очередь, следует отобрать системы ДБО, в том числе API-интерфейсы. В них под анализ попадает и javascript код веб-интерфейсов, и код хранимых процедур на PL-SQL, и исполняемый код модулей,

и bash-скрипты и другие, так как они обеспечивают проведение платежей. Также под анализ попадают мобильные приложения для банковских операций, которые банки размещают в магазинах приложений Google и Apple. Их следует подвергать анализу уязвимостей согласно 683-П. В эту же группу следует включить приложения «Банк-Клиент», передаваемые клиентам напрямую без использования магазинов приложений.

Теперь обратимся к крупным некредитным финансовым организациям. Под проверку по 684-П попадают различные системы дистанционного обслуживания. Это сервисы управления активами клиентов на сайтах НФО, личные кабинеты, системы документооборота, приёма платежей за полисы или пенсии и др. В список ПО попадут и мобильные приложения, размещённые в магазинах Google и Apple, которые НФО используют для финансовых операций и предоставления клиентам информации о своих активах.

КАК ПОДГОТОВИТЬСЯ И ЧТО ПРОВЕРЯТЬ?

Банк России для оценки безопасности ПО предлагает обратиться к ГОСТ Р ИСО/МЭК 15408. Это не набор каких-либо конкретных требований для реализации, а фреймворк для оценки — описание инструментария и процессов. Посмотрим на этот фреймворк верхнеуровнево. Есть объект оценки — это информационная система (ИС). Для объекта в процессе его разработки составляется задание по безопасности, в котором описываются цели безопасности и способы, которыми эти цели достигаются. ГОСТ предполагает, что для составления заданий может использоваться профиль защиты, в котором уже заранее для различного типа информационных систем подготовлены упомянутые цели безопасности и способы их достижения. Банком России был разработан, утверждён и рекомендован к использованию профиль защиты ПО для дистанционного обслуживания клиентов финансовых организаций.

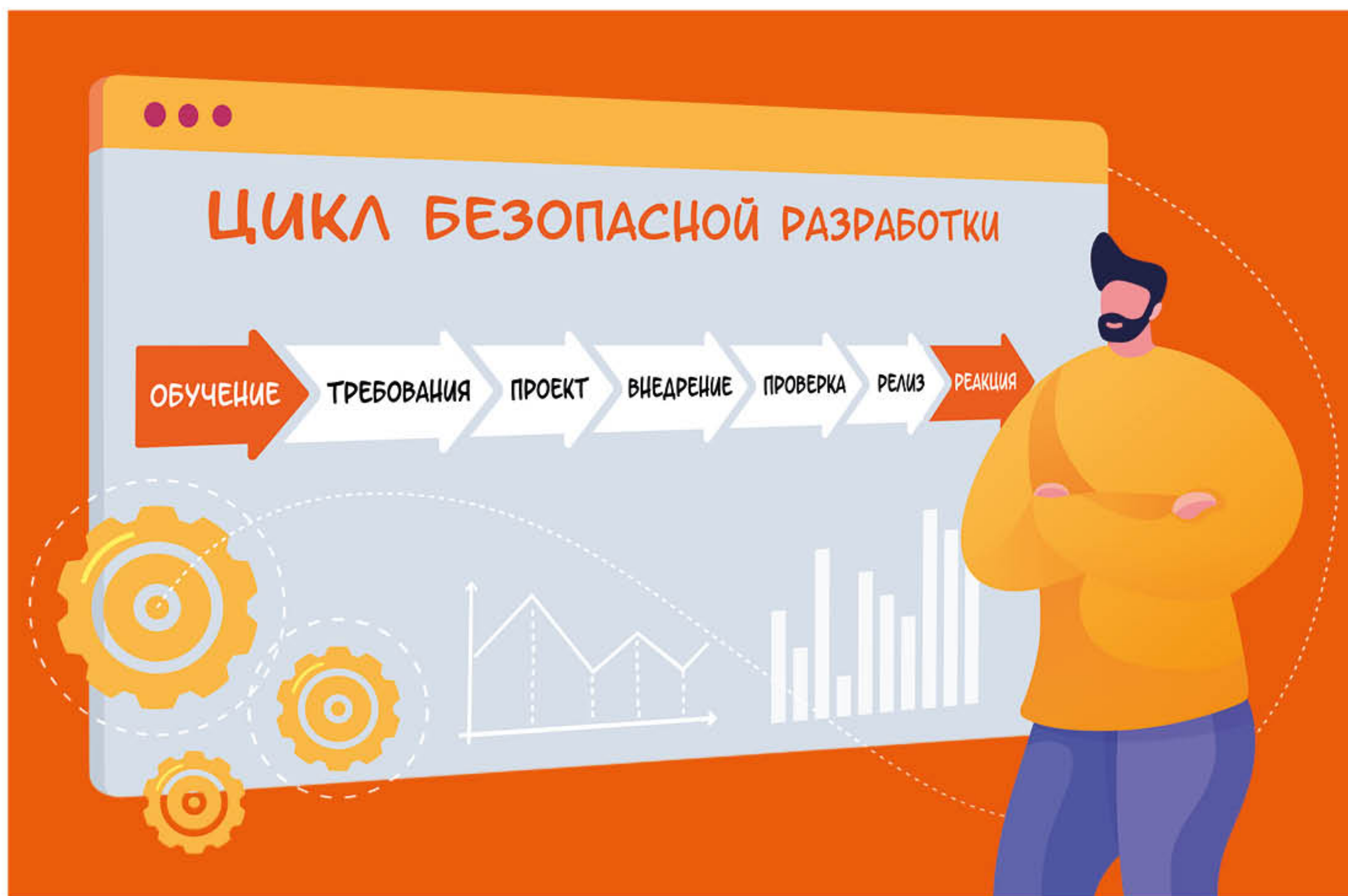
А что же такое оценочный уровень доверия? Терминология ГОСТ говорит, что уровень доверия к системе — это уровень соответствия целям безопасности. ГОСТ описывает семь таких уровней доверия (ОУД), включающих в себя определённые компоненты для оценки. Таким образом, к ОУД можно относиться как к глубине анализа безопасности ПО — чем выше ОУД, тем более тщательно проводится работа по оценке соответствия и тем больше компонентов ПО подвергается анализу.

Процесс анализа уязвимостей на ОУД4 в ГОСТ описывает использование документации на ПО, включая полное проектное описание и исходный код ключевых компонентов. После анализа уязвимостей проводится тест на проникновение, чтобы определить возможность эксплуатации выявленных уязвимостей.

ПРОБЛЕМА КОМПЛЕКТНОСТИ ПО

ПО разделяется на две категории: приобретённое с доработками или





без у вендора и собственное, созданное под себя. При этом собственное ПО может быть разработано как in-house, так и с привлечением сторонних разработчиков.

Если в организации используется ПО от вендора, следует обратиться к нему и запросить сертификат ФСТЭК или отчёт о соответствии ОУД4. При этом необходимо понимать, что разработчик может и не иметь таких документов или запросить оплату соответствующих услуг по сертификации и анализу уязвимостей, а может и вовсе отказаться от сотрудничества. Даже если предложить вендору вариант, при котором финансовая организация самостоятельно делает анализ уязвимостей, он может не предоставить исходный код или документацию для его проведения. По этой причине следует как можно раньше начать переговоры с разработчиками приобретённого ПО, чтобы иметь резерв времени для урегулирования соответствующих вопросов.

Как мы писали ранее, для подготовки к анализу любого ПО следует

проверить его комплектность: есть ли задание по безопасности, различные руководства, подробные описания архитектуры, API и, самое главное, есть ли исходные коды. Если каких-то из этих компонентов не хватает, то следует их запросить у команды разработки (неважно, сторонняя она или состоит из внутренних специалистов). На будущее рекомендуем принять у себя практику заказа документации и проверки наличия актуального исходного кода при приёмке работ.

АНАЛИЗ УЯЗВИМОСТЕЙ СИЛАМИ ВНЕШНЕГО ПОДРЯДЧИКА

Если говорить о привлечении внешнего подрядчика для проведения анализа ПО на ОУД4, возникает вопрос, кто же может им стать. Положения Банка России требуют от таких компаний только наличия лицензии ФСТЭК на ТЗКИ на виды работ, предусмотренных подпунктами «б», «д» или «е» Положения о лицензировании деятельности по ТЗКИ. И на первый

взгляд, при выборе подрядчика можно ограничиться этим требованием, но такой подход носит достаточно формальный характер. Всего на момент написания статьи в реестре соответствующих лицензий находится более 2500 компаний, и это очень много. Можно ли обращаться в любую из них? И что им потребуется для проведения анализа?

Шаг 1: выявляем методику проведения анализа

Первое, что следует выяснить у потенциального подрядчика, — какова методика проведения анализа уязвимостей. Эта методика должна быть впоследствии описана в итоговом отчёте о выполненной работе, так как Банк России во время проведения проверки будет смотреть не только на наличие отчёта и его итоговый результат, но и на методику проведения анализа для оценки его адекватности. Очевидно, что «пустой» отчёт на 2–3 страницах с безосновательными выводами о соответствии ПО требованиям ОУД4 не

будет принят, и финансовой организации будут выданы предписания в рамках полномочий Банка России.

Также методика должна содержать этапы работ: от оценки документации и развёртывания ПО на стенде до применения специального инструментария: статического анализатора кода или системы динамического анализа ПО. Дополнительно методика должна описывать этап тестирования на проникновение.

Шаг 2: оцениваем штат и квалификацию специалистов

Далее нужно узнать, каковы ресурсы подрядчика на проведение анализа: есть ли у него помимо методики тот самый инструментарий и квалифицированные специалисты, умеющие им пользоваться. Статический анализатор может выдавать огромные отчёты о несоответствиях практикам безопасного программирования, и нужно уметь их «читать» и формулировать понятные рекомендации, равно как и отсеивать ложные срабатывания. Кроме этого, подрядчик должен иметь штат пентестеров, которые будут оценивать возможность эксплуатации уязвимостей и по мере возможностей находить новые.

Шаг 3: убеждаемся в наличии дополнительных компетенций

Третьим шагом необходимо выяснить, способен ли подрядчик самостоятельно подготовить недостающие документы. Например, написать или скорректировать задание по безопасности или руководство по конфигурации ПО. Конечно, эта услуга в рамках оценки уязвимости ПО на ОУД4 носит дополнительный характер, но она говорит об уровне квалификации подрядчика.

САМОСТОЯТЕЛЬНЫЙ АНАЛИЗ ПО НА ОУД4

Ещё один путь — самостоятельный анализ ПО на ОУД4. Почти все требования к внешнему подрядчику для проведения анализа вполне подходят и для внутреннего применения. В крупных финансовых организациях инструментарий и специалисты зачастую уже имеются, необходимо их лишь перенаправить. Противоположным образом

обстоят дела в средних и небольших организациях с собственной разработкой. Для самостоятельного анализа уязвимостей им потребуется выделить значительные ресурсы, как финансовые для приобретения инструментов статического/динамического анализа кода или найма квалифицированного персонала, так и временные.

После того как необходимый инструментарий и ресурсы будут выделены или приобретены, следует разработать методику проведения анализа уязвимостей и встроить сам анализ в релизный процесс ПО с генерацией отчёта о соответствии ОУД4. Необходимо это сделать не только для нового разрабатываемого ПО, но и для крупных обновлений существующего.

Перед запуском ПО в промышленную эксплуатацию нужно проверить исходные коды статическим анализатором, а само ПО на тестовом стенде подвергнуть динамическому анализу и тесту на проникновение. После того как недостатки будут устранены, комплект ПО вместе с документацией и отчётом о проведённом анализе уязвимостей необходимо сохранить в репозитории. Данную работу потребуется повторять при крупных обновлениях, при этом минорные изменения допустимо не рассматривать.

Что же делать с тем программным обеспечением, которое уже сейчас находится в промышленной эксплуатации? Его потребуется проанализировать точно так же, как и описано выше для нового разрабатываемого ПО: с использованием той же методики и последующей подготовкой отчёта о его соответствии ОУД4.

НОВАЯ КУЛЬТУРА РАЗРАБОТКИ ПО

Зачастую комплаенс-нагрузка на ИБ рассматривается в отрыве от так называемой реальной безопасности и тем более от бизнес-целей организации. В случае с внедрением анализа кода в релизный процесс ПО это может стать первым шагом для трансформации функции ИБ в бизнес-функцию финансовой организации. Речь идёт о встраивании процессов SSDLC, которые очевидным образом повышают уровень зрелости ИТ/ИБ процессов

компаний. Более зрелые организации внедряют процессы SSDLC, автоматизируют установку ПО, его тестирование, и в целом эта модель хорошо коррелирует с требованиями регулятора.

Фреймворк ГОСТ/ИСО 15408, в соответствии с которым необходимо делать анализ уязвимостей ПО на ОУД4, хорошо ложится, например, в широко известное описание процесса Secure SDLC от компании Microsoft. Он точно так же предусматривает подготовку требований к ПО с учётом потенциальных нарушителей и применение инструментов статического и динамического анализа.

При этом не обязательно ориентироваться на описание Secure SDLC именно от вышеупомянутой компании. Любой встроенный в соответствии с лучшими практиками Secure SDLC процесс разработки ПО, даже с полной автоматизацией DevOps-конвейера, автоматизированным тестированием и релизами каждые 3 часа, удовлетворит требованиям ОУД4 и даже более строгим. И здесь мы уже говорим не только о выполнении регуляторных требований Банка России, но и об участии ИТ/ИБ-функции в формировании качественного продукта для клиентов, что ставит её на один уровень с бизнес-функциями организации.

* * *

Тема анализа ПО на уязвимости не нова, и в зрелых с точки зрения подходов к разработке и внедрению ПО компаниях давно встроены соответствующие процессы. Но нужно признать, что далеко не все финансовые организации находятся на этом уровне ИТ/ИБ-развития. При этом к желанию регулятора стандартизировать подходы к решению этой задачи можно относиться по-разному, но в любом случае соответствующие требования — это реалии сегодняшнего дня, которые необходимо принять. Более того, на них можно смотреть в позитивном ключе, если подходить к ним не со стороны дополнительной комплаенс-нагрузки, а со стороны повышения общего уровня зрелости ИТ/ИБ-процессов, а значит, и зрелости всей организации.



Илья КОНДРАТЬЕВ
заместитель
директора
департамента ИБ
АМТ-ГРУП

КАК ЗАЩИТИТЬ КРИТИЧНЫЙ СЕГМЕНТ: АКТУАЛЬНЫЕ СЦЕНАРИИ

РЕШЕНИЕ INFODIODE СЕРТИФИЦИРОВАНО
ФСТЭК И ОБЕСПЕЧИВАЕТ РЕАЛИЗАЦИЮ
ПЛАНОВ ПО ИМПОРТОЗАМЕЩЕНИЮ

Наиболее разрушительные современные атаки имеют целенаправленный и многоступенчатый характер, и для их успеха важно наличие технической возможности организации канала удалённого управления системой-жертвой, например, за счёт фишинга. Также весьма болезненным для организаций является факт утечки данных из внутренних ИТ-систем, последующая публикация или продажа украденных данных в DarkNet наносит существенный ущерб.

СЕГМЕНТАЦИЯ

Распространённый способ недопущения несанкционированного доступа — надёжная сегментация сети и отделение критичных сегментов от общей сетевой инфраструктуры организации. В ряде организаций к критичным сегментам относят:

- ♦ сегменты размещения АРМ КБР, сегменты размещения АРМ ДБО с банками-корреспондентами;
- ♦ сегменты процессинга, хранения резервных копий, а также различные внутренние ИТ-системы, доступ к которым извне недопустим ни при каких обстоятельствах;
- ♦ часто встречается практика отделения систем разработки и тестирования от продуктивных систем.

ВЧЕРАШНИЙ ДЕНЬ

Многие компании для таких сегментов применяют физическую изоляцию с помощью «воздушного зазора», и для переноса данных между сегментами используются съёмные носители. Изоляция с помощью «воздушного

зазора», наряду с очевидными достоинствами с точки зрения безопасности, имеет ряд недостатков:

- ♦ затрудняет автоматизацию ИТ и влечёт за собой дублирование АРМ и серверов;
- ♦ при необходимости передачи данных между сегментами приходится использовать съёмные носители, что, в свою очередь, замедляет процессы и имеет высокую трудоёмкость, если нужно передавать значительные объёмы информации;
- ♦ передача данных в реальном времени невозможна;
- ♦ провоцирует эксплуатирующий персонал на создание «скрытых» соединений между сегментами.

Какие-то организации в силу традиций продолжают мучения с «воздушным зазором», но всё больше наших заказчиков предпочитают идти в ногу

со временем и ищут пути повышения удобства и скорости обмена информацией между сегментами с учётом требований по обеспечению ИБ. В данном случае сочетать высокую степень изоляции на физическом уровне и удобство передачи данных по сети позволяют устройства однонаправленной передачи данных.

РЕШЕНИЕ АМТ INFODIODE

АПК АМТ InfoDiode предназначен для надёжного и гарантированного разделения критичных сегментов на физическом уровне модели OSI, при этом обеспечивая возможность однонаправленной передачи информации из одного сегмента в другой. Для передачи данных поддерживаются протоколы файлового обмена (CIFS, FTP), протокол передачи почты SMTP, а также протоколы, использующие в качестве

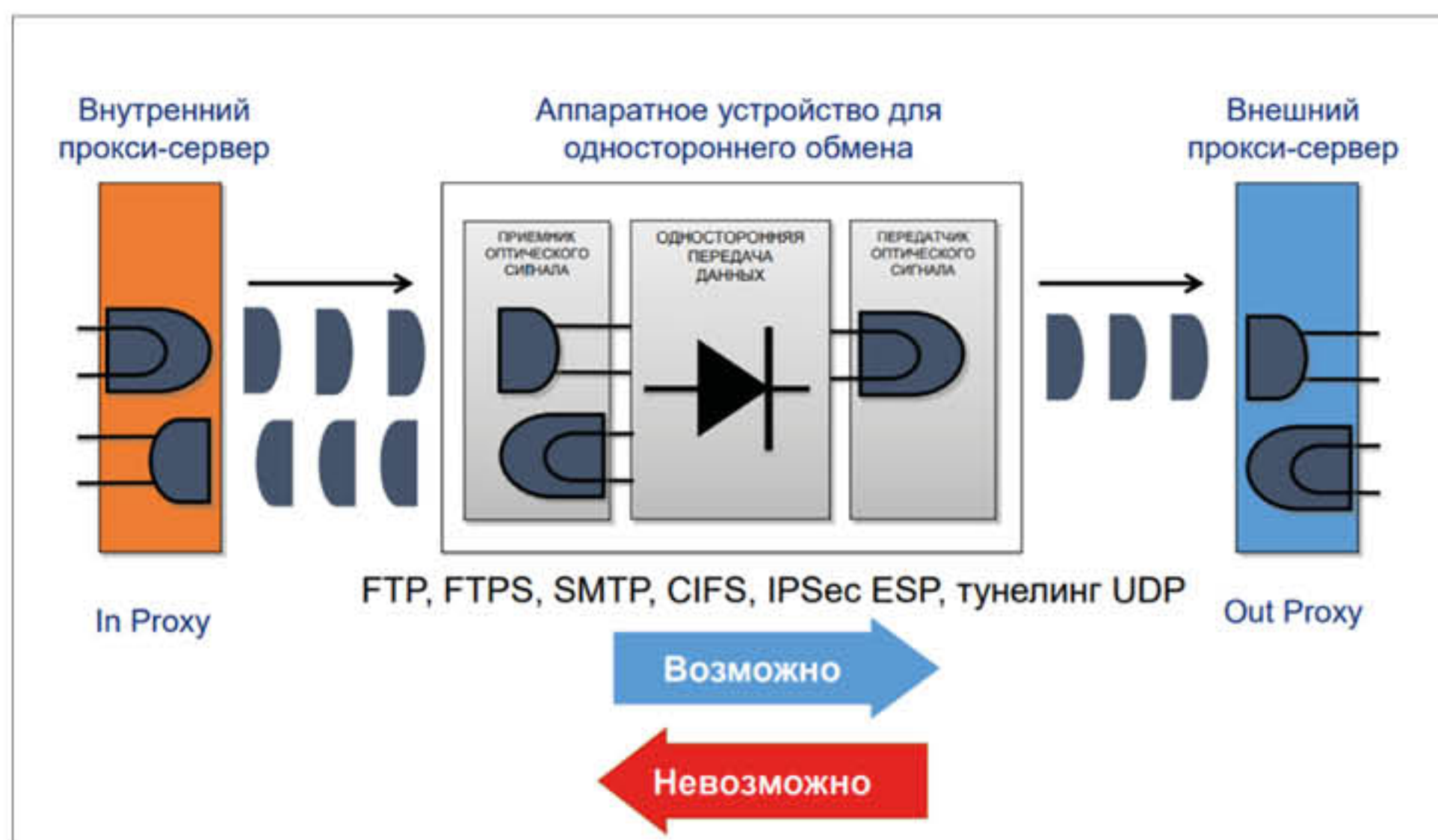


Рисунок 1. АПК АМТ InfoDiode позволяет надёжно отделить критичные сегменты от остальной СПД и одновременно обеспечить необходимые взаимодействия

транспорта UDP (SNMP, Syslog, NTP, Netflow и т.д.).

Данное решение (рис. 1) находит своё применение в финансовых организациях и позволяет надёжно отделить критичные сегменты от остальной СПД и одновременно обеспечить необходимые взаимодействия. Решение сертифицировано ФСТЭК России.

РЕАЛЬНЫЕ СЦЕНАРИИ ДЛЯ ФИНАНСОВОЙ ОТРАСЛИ

В настоящее время есть несколько практических кейсов, в которых финансовые организации используют AMT InfoDiode для решения задач обеспечения необходимого уровня защиты.

1. Доставка в защищаемый сегмент информации от новостных агентств (Reuters, Bloomberg) и биржевых площадок через Интернет без риска утечки информации из защищаемого сегмента (рис. 2). Реализация данного подхода успешно осуществлена в инфраструктуре одного из заказчиков АМТ-ГРУП. В защищаемом сегменте размещаются АРМ аналитиков, для работы которых требуется одновременный доступ к данным во внутренних бизнес-системах и оперативная сводка новостей от Reuters. При этом, учитывая высокую ценность результатов работы аналитиков и значимость данных, с которыми они работают, организации требуется исключить утечку данных из сегмента АРМ аналитиков.

2. Отделение сегмента разработки ПО от продуктивной среды (рис. 3), при этом передача дистрибутивов и образов ПО осуществляется через InfoDiode без риска передачи продуктивных данных в сегмент разработки. Данный случай успешно реализован для финансовой организации, имеющей большое количество ИТ-систем с ПО собственной разработки. После успешного тестирования обновлённых пакетов в среде разработки и тестирования осуществляется загрузка пакетов в продуктивный сегмент через AMT InfoDiode по протоколам CIFS и FTPS.

3. Работа контакт-центра (рис. 4). Операторы контакт-центра, осуществляющие обзвон, при коммуника-

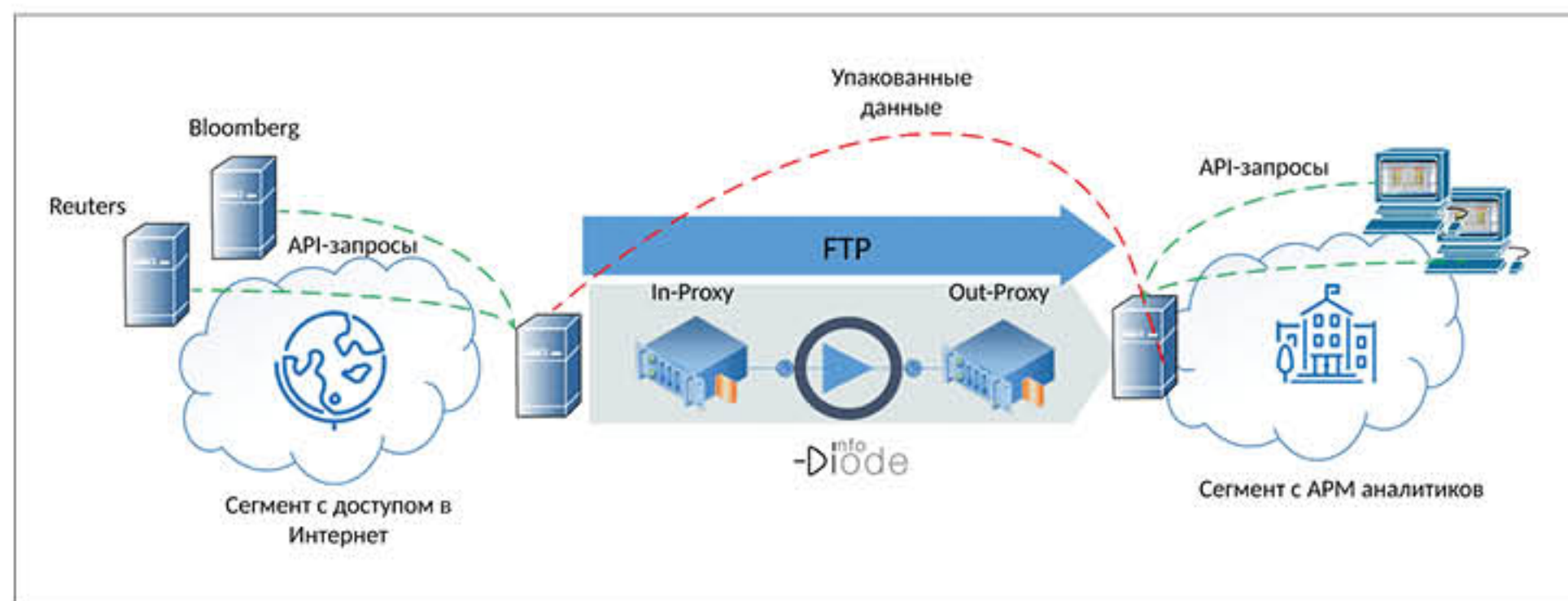


Рисунок 2. Доставка в защищаемый сегмент информации от новостных агентств (Reuters, Bloomberg) и биржевых площадок через Интернет без риска утечки информации из защищаемого сегмента

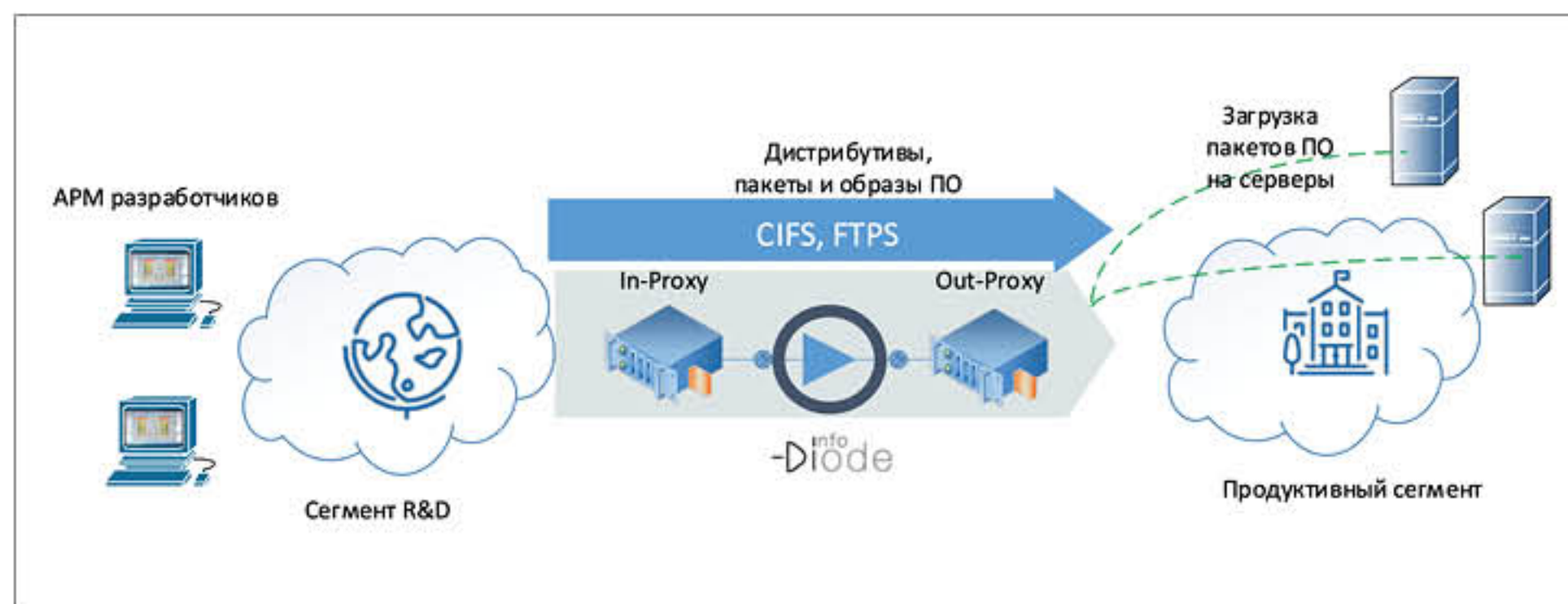


Рисунок 3. Отделение сегмента разработки ПО от продуктивной среды

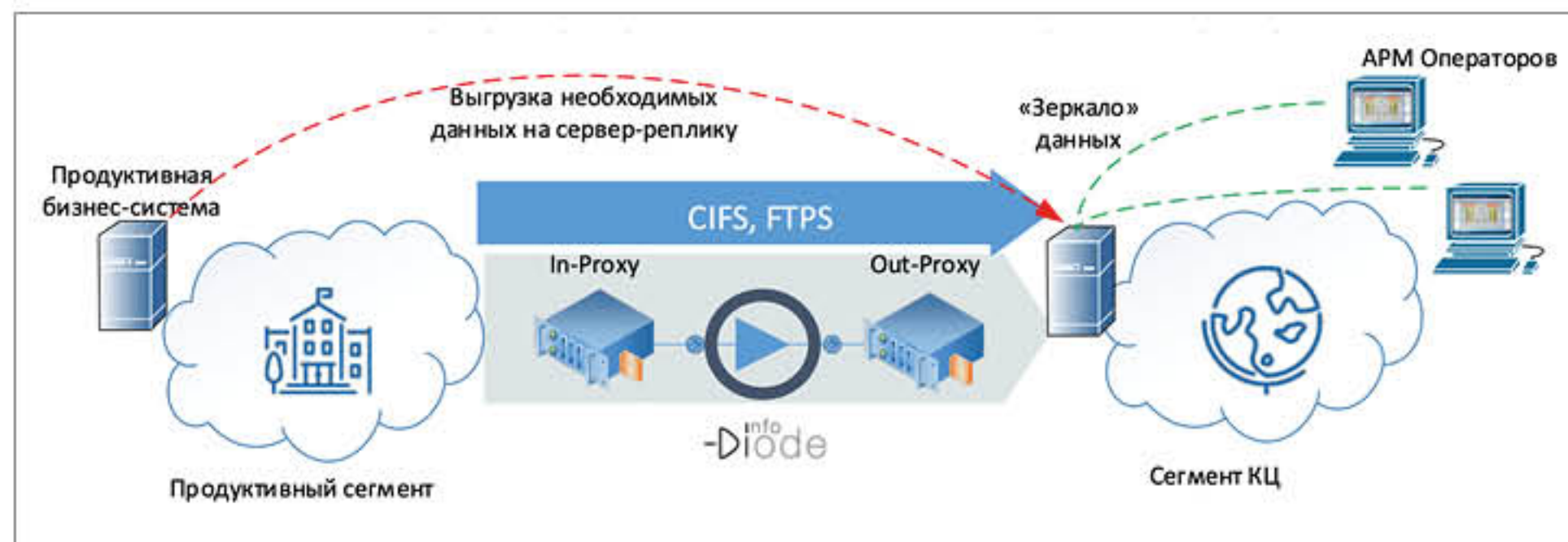


Рисунок 4. Работа контакт-центра

ции с клиентами работают с репличкой информации из базы данных. Необходимые им данные периодически выгружаются из основной БД продуктивного сегмента через InfoDiode. Таким образом, исключается возможность негативного воздействия на серверы продуктивного сегмента со стороны операторов.

Как видно из приведённых примеров, можно констатировать всё больший интерес организаций финансовой отрасли к повышению уровня защищённости своих ИТ-систем и

бизнес-процессов. Одновременно наблюдается расширение сценариев применения систем однонаправленной передачи данных для реализации более серьёзных мер защиты и одновременного повышения удобства пользователей после их внедрения (по сравнению с «воздушным зазором»).

Не менее важно наличие разнообразных сценариев применения, успешно реализованных на практике в инфраструктуре финансовых организаций. А также факт, что решение InfoDiode сертифицировано ФСТЭК и обеспечивает реализацию планов по импортозамещению.



Владимир БЕНИН
директор по развитию
продуктового
направления
Positive Technologies

КАК ГРАМОТНО ВЫСТРОИТЬ УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ

ПОЧЕМУ В БАНКАХ ОПАСНО
«КОНСЕРВИРОВАТЬ» УЯЗВИМОСТИ: КАК
НАСТРОИТЬ VULNERABILITY MANAGEMENT

Пять дней — столько времени в среднем требуется злоумышленнику для проникновения во внутреннюю сеть банка. После чего взломщику обычно хватает двух дней для получения контроля над инфраструктурой кредитной организации — системами управления банкоматами, серверами карточного процессинга, рабочими станциями топ-менеджеров. Подобные исследования проводились нами в прошлом году в российских банках, входящих в топ-50 по активам, относящимся к разным размерным категориям. Одна из ключевых причин компрометации ценных активов связана с уязвимостями ПО. Их эксплуатация была возможна в 9 из 10 этих финансовых организаций.

Сегодня базы MITRE CVE List¹ и NVD² содержат более 100 тысяч записей об уязвимостях. Появление новых уязвимостей — это непрерывный поток. За сутки в среднем регистрируется 13 новых записей. И даже если в опенспейсе подразделения ИБ в момент публикации очередного уведомления будет загораться большая красная лампа, на эти сигналы вскоре перестанут обращать внимание.

На крупнейшем в России форуме по практической кибербезопасности Positive

Hack Days один из гостей³ однажды удивлённо заметил, что «часть специалистов по ИБ существуют словно в отрыве от практической безопасности», например, как это было с WannaCry: злоумышленники The Shadow Brokers выложили архивы с модулями, на базе одного из которых был сделан этот вирус-вымогатель, но многие профильные специалисты даже спустя несколько дней ничего не знали об этой опаснейшей утечке. Об уязвимости стало известно в феврале 2017 года, эксплойт появился в апреле, а останавливать предприятия по всему миру операторы WannaCry начали в мае.

Для создания работающего процесса управления уязвимостями (vulnerability management, VM) нужна всесторонняя работа: инвентаризация, анализ защищённости, приоритизация, создание и выполнение регламентов устранения уязвимостей и проверка результатов этого устранения.

НАВЕДИТЕ ПОРЯДОК В СВОИХ АКТИВАХ

Оптимальный подход к организации процесса управления уязвимостями начинается с актуализации данных об активах — элементов IT-инфраструктуры, подключённых к сети: это могут быть серверы, компьютеры, сетевое оборудование. Важно получить исчерпывающие сведения о них. В противном случае какие-то уязвимости могут быть не обнаружены.

Данные об активах можно аккумулировать за счёт сканирования в режимах

чёрного и белого ящика, импорта данных из внешних каталогов (Active Directory, SCCM⁴, гипервизоры), обнаружения активов по данным других решений ИБ (из анализа событий SIEM⁵ и трафика NTA⁶), контроля недавно обнаруженных активов и тех, о которых давно не было информации.

После обнаружения активы нужно корректно идентифицировать. Чем больше параметров идентификации активов предоставит VM-система (FQDN⁷, адреса MAC⁸ и IP, тип ОС, имя сетевого узла, признаки виртуальности узла), тем лучше: так у вас получится избежать дублирования активов и ложных срабатываний средств защиты.

РАССТАВЛЯЙТЕ ПРИОРИТЕТЫ

Каждому активу должен соответствовать определённый уровень его значимости. Заранее оцените, как актив влияет на конфиденциальность и целостность данных, работоспособность важных для бизнеса сервисов. Это поможет определить уровень опасности найденных уязвимостей, варьировать сроки их устранения и рассчитывать свои финансовые и трудозатраты. Мы рекомендуем объединять

⁴ System Center Configuration Manager (ранее Systems Management Server, SMS) — продукт для управления IT-инфраструктурой на основе Microsoft Windows и смежных устройств.

⁵ Security information and event management — система выявления событий информационной безопасности.

⁶ Network traffic analysis — система анализа сетевого трафика.

⁷ FQDN — имя домена, включает в себя имена всех родительских доменов иерархии DNS.

⁸ MAC-адрес — уникальный идентификатор, присваиваемый каждой единице активного оборудования.

¹ MITRE CVE List — реестр уязвимостей Common Vulnerabilities and Exposures, разработанный американской некоммерческой исследовательской корпорацией MITRE Corporation.

² NVD (National Vulnerability Database) — база данных уязвимостей, поддерживаемая Национальным институтом стандартов и технологий США.

³ Комментарий Евгения Климова, ранее технического директора компании «Информзащита», в настоящее время заместителя генерального директора по информационным технологиям группы «Интерфакс».

активы по принадлежности к структурным подразделениям, автоматизированным системам, к IP-сетям или по наличию определённых ОС. Это позволит быстро проводить сканирование определённых подгрупп.

ВВЕДИТЕ ПРАВИЛА ОБРАБОТКИ УЯЗВИМОСТЕЙ

Если в вашей IT-инфраструктуре более 1000 активов, то управлять уязвимостями вручную невозможно. Отведите на ручную обработку только самые опасные уязвимости для конкретно вашей инфраструктуры, система анализа защищённости должна позволять специалистам ИБ определять такие уязвимости.

VM-система выявляет открытые сетевые порты и доступные службы, уязвимости в ПО, а также недостатки конфигурации оборудования, серверов и средств защиты. Данные по активам также следует соотносить с правилами, заданными в базе знаний VM. Разработчики систем используют общие базы уязвимостей (MITRE CVE List, NVD, OSVDB, БДУ ФСТЭК России), а также собственные базы знаний.

По итогам сканирования специалисты по ИБ, как правило, сталкиваются с огромным списком уязвимостей, и на этом этапе важно определить, какие уязвимости необходимо устранить в первую очередь. Можно опираться на оценку по CVSS⁹ и искать дополнительную информацию: например, существуют ли доступные эксплойты для этой уязвимости и удавалось ли её использовать в процессе тестирования на проникновение. Другой путь — доверять оценке от вендора, но при условии, что вендор действительно обладает такой экспертизой.

УСТРАНЯЙТЕ УЯЗВИМОСТИ И ПРОВЕРЯЙТЕ ИХ ОТСУТСТВИЕ

Есть два подхода к устранению и проверки устранения уязвимостей — реактивный и проактивный.

При реактивном подходе IT-подразделение устанавливает патчи после того, как служба ИБ предоставит информацию об обнаруженных уязвимостях,

сформирует списки активов, ОС и ПО для реагирования. После проведённых работ специалисты по ИБ контролируют отсутствие уязвимостей через определённое число дней после их обнаружения на активе. Сроки устранения ИБ и IT обсуждают по каждой уязвимости или списку уязвимостей отдельно.

При проактивном подходе IT-подразделение регулярно устанавливает патчи или обновления ОС и ПО, не дожидаясь информации об уязвимостях от службы ИБ. В этом случае специалисты по ИБ лишь контролируют отсутствие уязвимостей через определённое количество дней после публикации информации о них.

Если появляются особо опасные уязвимости, реагирование и проверки происходят вне очереди.

НА КАКИЕ УЯЗВИМОСТИ ОБРАТИТЬ ВНИМАНИЕ

В локальной сети банков можно встретить множество необновлённых систем, содержащих опасные уязвимости. До сих пор мы сталкиваемся с уязвимостью, используемой операторами шифровальщика WannaCry.

Кроме того, наша команда исследователей безопасности находила в инфраструктуре банков следующие уязвимости:

1. CVE-2018-9276. Уязвимость в ПО PRTG Network Monitor позволяет выполнить команды операционной системы на сервере при наличии прав администратора приложения. Данное ПО широко применяется во множестве компаний различных отраслей в качестве вспомогательного элемента, осуществляющего контроль за состоянием устройств в сети. Для устранения бреши надо установить версию ПО, начиная с 18.2.39.

2. CVE-2016-2004. Эта уязвимость была обнаружена ещё четыре года назад в ПО HP Data Protector, она позволяет удалённо выполнить произвольный код. Программное обеспечение служит для обеспечения автоматического резервного копирования и восстановления данных. Необходимо убедиться, что установлены более свежие редакции системы, чем 7.03_108, 8.15 или 9.06.

3. CVE-2018-0171. Данная уязвимость найдена в приложении Smart Install для Cisco IOS, также позволяет удалённо вы-

полнить произвольный код. Cisco IOS — операционная система, используемая в маршрутизаторах и сетевых коммутаторах Cisco. В 2018 году эта уязвимость использовалась в ходе крупной ботнет-атаки, пострадали провайдеры по всему миру. Для определения версии и устранения уязвимости следуйте рекомендациям, описанным в уведомлении Cisco.

4. CVE-2019-0686. Критически опасная уязвимость в ПО Microsoft Exchange Server позволяет повысить привилегии в системе. По сути, она даёт возможность любому владельцу почтового ящика стать администратором домена. Были затронуты Microsoft Exchange Server 2019, Microsoft Exchange Server 2016, Microsoft Exchange Server 2013 — эти системы необходимо обновить до последних редакций.

5. CVE-2017-10271. Это уязвимость в Oracle WebLogic Server с уязвимым компонентом WLS-WSAT, позволяет удалённо выполнить произвольные команды на сервере. Брешь использовалась для заражения веб-серверов трояном Neutrino и атак на кластеры Elasticsearch. Для устранения проблемы необходимо установить более свежую версию продукта, нежели 12.2.1.2.0.

* * *

В ноябре мы представили систему управления уязвимостями нового поколения MaxPatrol VM. Решение позволяет организовать все перечисленные этапы управления уязвимостями. С помощью MaxPatrol VM можно:

- ♦ собирать полные и постоянно актуализируемые данные о составе IT-инфраструктуры;
- ♦ учитывать значимость защищаемых активов;
- ♦ выявлять, приоритизировать и задавать правила обработки уязвимостей для IT-отдела;
- ♦ контролировать устранение уязвимостей;
- ♦ отслеживать общее состояние защищённости компании.

Возможности системы помогут контролировать управление уязвимостями как в штатном режиме, так и при срочных проверках. Продукт поступит в свободную продажу в первом квартале 2021 года.

⁹ Common Vulnerability Scoring System, CVSS — общая система оценки уязвимостей.



Дмитрий КУРАШЕВ
сооснователь UserGate

«СДЕЛАНО В РОССИИ, СЕРТИФИЦИРОВАНО ФСТЭК» — 2¹

МАСШТАБИРУЕМЫЕ ПЛАТФОРМЫ USERGATE ДЛЯ
МНОГОВЕКТОРНОЙ ЗАЩИТЫ ЗОКИИ

Исторически сложилось так, что в сфере кибербезопасности Россия обладает большим потенциалом. «Лаборатория Касперского», InfoWatch, Digital Security, Doctor Web сегодня работают на отечественном и зарубежных рынках. И эта когорта компаний постоянно пополняется новыми игроками, среди которых и «Юзергейт». Если говорить о зарубежном опыте, то её решения для фильтрации сетевого трафика используются в аэропортах Хитроу и Абу-Даби, в FiteCollege UK.

Сегодня компания активизирует свою деятельность на российском рынке.

Этому способствует тесная работа «Юзергейт» со ФСТЭК в сфере сертификации своей продукции, что позволяет строить системы защиты ЗОКИИ, соответствующие не только действующим жёстким требованиям ФСБ и ФСТЭК, но и нормативным документам в сфере ИБ отраслевых регуляторов в финансовой сфере, топливно-энергетическом комплексе, «оборонке» и иных отраслях.

Недавно компания приняла участие в выставке оборудования CISO Форум 2020, и нашему корреспонденту удалось не только познакомиться с решениями «Юзергейт», но и задать несколько вопросов совладельцу компании Дмитрию Курашеву.

— Давайте определимся с понятиями. «Платформа UserGate» — это что такое? Как вписывается в процессы сертификации широкая линейка оборудования и продуктов компании — шесть форм-факторов ПАК?

— В составе разрабатываемого нами оборудования «работает» написанный нами программный код, реализующий самые разнообразные функции безопасности, и операционная система UGOS, также поддерживаемая нами. Платформы UserGate могут поставляться в виде виртуальных образов, а также в виде линейки программно-аппаратных комплексов. На данный момент мы используем зарубежные комплектующие, и в России сейчас производится сборка. Однако около трёх последних

лет мы были заняты созданием аппаратных комплексов и технологической подготовкой их производства на территории России. Конечно, сертификация производится на каждой модели, и в силу этого сертификация широкой линейки является сложной и затратной. Однако мы научились справляться с этими задачами достаточно успешно.

— Расскажите, пожалуйста, о заказчиках компании. Какая доля приходится на сферы телекома, энергетики, госорганизаций, вузов и т.д.?

— Мы не можем выделить какую-то одну категорию, наше решение используется в самых разных организациях. Всё больше и больше организаций государственной власти переходят на UserGate. Уже сейчас нас используют 6 из 21 федерального министерства. Во многих регионах нас используют на

уровне местных ЦИТ или ДИТ для защиты всех органов власти. Среди наших клиентов много компаний из топливно-энергетического комплекса, банки, розничные сети, университеты, а также операторы связи, такие как «Мегафон» и «Ростелеком».

— Какие изменения в такой структуре бизнеса вы планируете? Или компания идёт по пути развития функциональных возможностей и технических характеристик оборудования, а отрасли сами сделают свой выбор?

— Мы находимся в стадии бурного роста, поэтому у нас есть широкие возможности для значительных инвестиций в собственное развитие. Мы проводим большую работу по созданию аппаратных платформ с существенно улучшенными характеристиками

¹ Продолжение. Начало темы в №3/2020



Межсетевой экран UserGate F8000 для защиты корпоративных сетей и дата-центров от современных видов атак и других вторжений

по скорости и производительности, а также занимаемся развитием функциональных возможностей наших решений. При этом наше развитие осуществляется на основе плотного взаимодействия с нашими заказчиками. Мы хорошо понимаем их потребности и на основе этого строим свои планы.

— **Какие формы работы использует компания для развития технических компетенций пользователей в сфере применений и эксплуатации платформ UserGate?**

— Конечно, мы делаем всё возможное, чтобы технические специалисты отечественных компаний осваивали оборудование линейки UserGate и систематически актуализировали свои знания и компетенции. Для этого, в частности, нашими партнёрами проводятся обучающие курсы двух уровней: стандартный и продвинутый. Некоторыми заказчиками внедрение UserGate и последующая поддержка проводятся силами своих специалистов. Но в большинстве случаев работы проводятся нашими интеграторами-партнёрами. Существенный рост числа опытных специалистов по установке и настройке оборудования UserGate произошёл за последние три года.

— **Достоинством вашего оборудования, наряду с его функциональными возможностями, является сертификация ФСТЭК. Можете ли вы поделиться «кухней» взаимодействия с регуляторами в сфере ИБ?**

— Прохождение сертификации — это сложный и долгий процесс, при

котором испытательные лаборатории и ФСТЭК России проводят скрупулёзный анализ решений. У нас есть возможность консультироваться непосредственно в самом ФСТЭК России. Это, конечно, помогает, но не избавляет от необходимости проходить все проверки. Насколько мы знаем, оборудование UserGate не только исследовалось в испытательной лаборатории, но и эксплуатируется в самом ФСТЭК России.

— **Традиционный вопрос о кадрах. Как вы можете охарактеризовать коллективный портрет компании?**

— Мы можем говорить о сбалансированном составе. У нас есть немало сотрудников, чей возраст едва превышает 20 лет. При этом у нас работают опытные инженеры, которым уже за 55. Мы также периодически нанимаем специалистов, имеющих опыт работы у наших зарубежных конкурентов. Все основные компетенции мы держим внутри компании. Сторонних специалистов мы стараемся привлекать минимально. Обычно это касается только бухгалтерии, аудита, юридических консультаций. Соотношение программистов и «железячников» постепенно выравнивается.

— **Каким вы видите развитие человеческого потенциала компании?**

— Мы стараемся каждому сотруднику дать возможность для развития: профессиональную, личную и финансовую. А также обеспечить комфортные условия труда и позитивную атмосферу.

— **Планы компании в сфере развития технологий?**

— С точки зрения программного обеспечения мы делаем всё возможное, чтобы удовлетворить запросы как можно более широкого спектра заказчиков. В этом году мы выпустили такие продукты, как UserGate Log Analyzer и UserGate Management Center. Используя их, заказчики не только могут обеспечить защиту корпоративной сети, но и получают отличные возможности по анализу информационной безопасности, а также по управлению распределением сетей.

— **Планы компании в сфере взаимодействия с регуляторами?**

— Взаимодействие со ФСТЭК России у нас налажено достаточно давно. В последнее время новым для нас является взаимодействие с Минпромторгом. С 1 января 2022 года крайне важным будет присутствие оборудования в реестре российского телекоммуникационного оборудования, который ведёт Минпромторг. Наши решения должны однозначно там присутствовать, над чем мы активно работаем. Также мы взаимодействуем с Министерством цифрового развития.

— **Планы компании в сфере взаимодействия с «сообществом»?**

— Для нас очень важно, чтобы возникло сообщество технических специалистов, знающих и любящих UserGate. Мы проводим много мероприятий для воспитания таких специалистов. В этом году многие из них самоорганизовались, создав соответствующий телеграм-канал.

Вопросы задавал
Валерий Куликов



РКИ-ФОРУМ РОССИЯ 2020

КАК ЗДОРОВО, ЧТО ВСЕ МЫ ЗДЕСЬ СЕГОДНЯ
СОБРАЛИСЬ! ИЛИ КАК ПРОШЁЛ РКИ-ФОРУМ ПОСЛЕ
НЕСКОЛЬКИХ МЕСЯЦЕВ ИЗОЛЯЦИИ ИЗ-ЗА ПАНДЕМИИ

В сентябре в Московской области прошла XVIII Международная конференция по проблематике инфраструктуры открытых ключей и электронной подписи — «РКИ-Форум Россия 2020». Главными темами этого года стали поправки к 63-ФЗ «Об электронной подписи», развитие отраслевого законодательства, нормативного и технического регулирования, влияние пандемии COVID-19 на отрасль и другие.

ОБСУЖДАЕМ В ЭТОМ ГОДУ

Несмотря на сложную ситуацию в мире, связанную с распространением коронавируса, форум вызвал огромный интерес профессионального сообщества. В этом году его посетили 205 человек.

Три интенсивных дня работы были заполнены до отказа: пленарная сессия — открытие Форума, шесть тематических сессий, два круглых стола по острым вопросам и долгожданное личное общение после самоизоляции.

Первый заместитель генерального директора АО «НИИАС» Владимир Матюхин в приветственном слове рассказал о современном состоянии рынка электронной подписи. По его словам, кризис, с которым столкнулась Россия и мир в целом в 2020 году, спровоцировал не только негативные последствия, но и определённые успехи в области цифровизации: информационные технологии оказались исключительно важными в условиях, когда привычные бизнес-процессы и жизненный уклад резко изменились.

Он также упомянул о том, что рынок электронной подписи ожидают масштабные преобразования, обусловленные принятием Федерального закона № 476-ФЗ «О внесении изменений в Федеральный закон «Об электронной подписи».

В выступлении директора правового департамента Минцифры России Романа Кузнецова также была затронута тема изменений рынка в ближайшей перспективе. Сегодня уже вступили в силу нормы об увеличенных требованиях к удостоверяющим центрам. С января 2021 г. возникнут права и возможности использования облачной квалифицированной ЭП, появится возможность аккредитоваться операторам доверенной третьей стороны. В январе 2022 г., согласно текущим планам,



Первый заместитель генерального директора АО «НИИАС» Владимир Матюхин



Директор правового департамента Минцифры России Роман Кузнецов

должны полноценно заработать машиночитаемые доверенности, реестры полномочий, ряд государственных УЦ получит исключительное право на обеспечение определённых категорий квалифицированными сертификатами.

Одновременно министерство ведёт работу по корректировке статьи 189 ГК РФ «Последствия прекращения доверенности». Дорабатываются подзаконные акты к уже упомянутому 476-ФЗ.

В фокусе выступления представителя ФСБ России Александра Бондаренко была тема облачной ЭП. Точнее, в ФСБ считают, что использование этого понятия (которое к тому же законодательно не закреплено) может ввести в замешательство некоторых специалистов — и предлагают взять на вооружение термин «удалённая ЭП» или «дистанционная ЭП».

НОВЫЕ ПРАВОВЫЕ РЕАЛИИ

Вопрос вносимых изменений в 63-ФЗ «Об электронной подписи» был, конечно, в основном фокусе внимания форума все три дня. Как считают эксперты, эти изменения могут существенно изменить распределение сил на рынке удостоверяющих центров и электронной подписи. В частности, закон прописывает возможность использования электронных машиночитаемых доверенностей — однако регламент их применения, хранения и отмены ещё не до конца понятен пользователям.

По мнению начальника отдела «Банка ВТБ» Дмитрия Ушакова, в свете указанных изменений вызывает беспокойство судьба усиленной неквалифи-

цированной подписи, так как конструкция 63-ФЗ в целом устанавливает более либеральный режим регулирования для использования усиленной неквалифицированной подписи, но требования к содержанию сертификатов ключа проверки ЭП становятся идентичными как для УКЭП, так и для УНЭП.

Советник генерального директора по взаимодействию с государственными органами «СКБ Контур» Наталья Никитина и руководитель проектов НПЦ «1С» Альберт Салимов подвели предварительные итоги деятельности рабочей группы, которая занимается подготовкой нормативно-правовых актов к закону 476-ФЗ. Как известно, закон не начнёт действовать в части определённых изменений до того, как будут приняты соответствующие нормативно-правовые акты — всего их более 25, и их количество может увеличиться в ходе дальнейшего анализа текста закона.

Научный сотрудник Института государства и права РАН Нина Соловяненко в своём докладе систематизировала все риски, появляющиеся на новом правовом ландшафте электронной подписи, и проанализировала потенциальные проблемы применения новых норм. А Владислав Бржозовский, адвокат, главный эксперт ООО «Право высоких технологий», рассказал о юридических нюансах такого нововведения, как доверенная третья сторона, и о том, как изменится с появлением этого института процесс удостоверения юридической силы электронных документов.

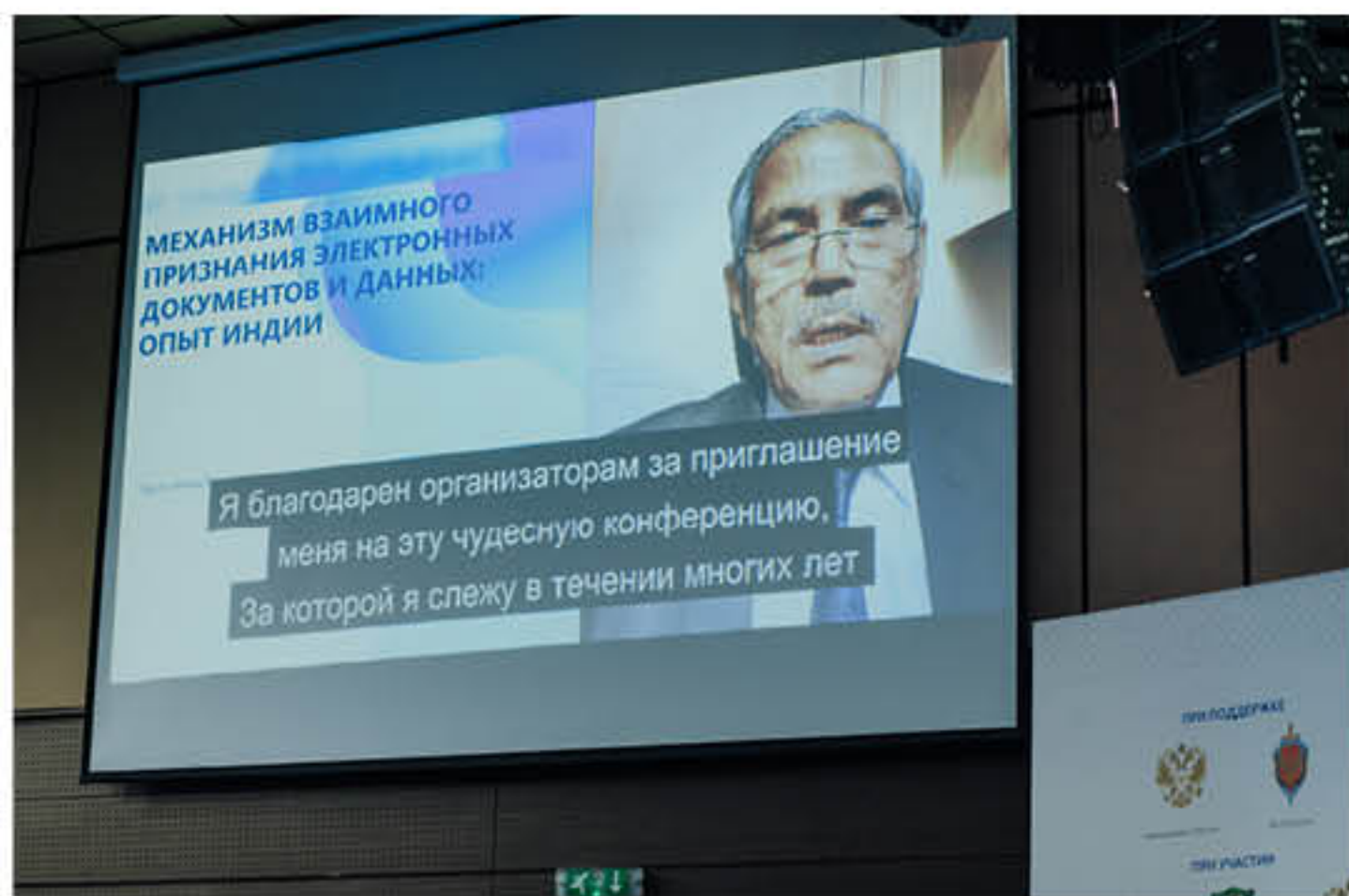
ДИСТАНЦИОННАЯ И НЕ ОЧЕНЬ

Отдельно большую часть докладов и дискуссий на Форуме занимал вопрос создания и применения дистанционной ЭП, а также дистанционной идентификации пользователей. В первую очередь это затронет удостоверяющие центры. По словам экспертов, технология дистанционной идентификации будет популярна, так как не надо будет ездить несколько раз в УЦ, а время получения сертификата сократится до нескольких минут. При этом остаётся множество спорных моментов — доставка ключевых носителей, доставка криптографических средств, вопрос удержания удостоверяющими центрами своих клиентов и так далее.

В этой теме стоит отдельно упомянуть и выступление директора по развитию компании «Актив» Владимира Иванова. Он весьма подробно рассказал, что такие варианты носителей ЭП, как мобильное приложение, SIM-карта, токены, да и в принципе облачные решения при всей их прелесть имеют слишком много недостатков. Например, встаёт вопрос доверия к устройству, а значит, и безопасности самих ключей, надёжности идентификации пользователя. «Актив» старается решить эти вопросы в своих разработках, таких, например, как дуальная смарт-карта Рутокен ЭЦП 3.0 с интерфейсом NFC.

СТАНДАРТЫ И ПРОТОКОЛЫ

Отдельно в фокус вышла тема стандартизированных протоколов для защиты межмашинного взаимодействия и



Выступление заместителя председателя СЕФАКТ ООН Тахсена Кхана (Индия)



Вручение диплома победителю в номинации РКИ-Форума «Эксперт года» Ивану Янсону

интернета вещей, а также промышленного интернета вещей. Этой тематике был посвящён доклад представителя компании «ИнфоТеКС» Ольги Шемякиной.

Так, в сфере межмашинного взаимодействия и интернета вещей существует огромное количество технологий, в том числе широкий набор протоколов. Для передачи данных в этой сфере характерно разнообразие топологий: помимо взаимодействия «точка-точка», распространены широкополосные взаимодействия, мультикаст и другие. Межмашинные протоколы не предназначены для передачи больших объёмов данных. Зачастую у IoT-устройств небольшие вычислительные ресурсы, большое количество подобных гаджетов работают от батареек. В этих задачах мы имеем дело с большой вариативностью технологий, множеством протоколов, низкой пропускной способностью каналов, из чего следует чувствительность к объёму отправляемых данных.

Решая эту проблему, рабочая группа «Криптографические механизмы для промышленных систем» в структуре ТК 26 на сегодняшний день разработала четыре протокола, два из которых уже имеют статус рекомендации по стандартизации, а два остальных будут утверждены в этом статусе до конца года: «Криптографические механизмы защищённого взаимодействия контрольных и измерительных устройств», «Протокол защищённого обмена для промышленных систем», «Использование российских

криптографических механизмов для реализации обмена данными по протоколу dlns», «Протокол безопасности сетевого уровня».

ТРАНСГРАНИЧНЫЙ ЭДО

Знаменательной частью третьего дня Форума стала тема «РКИ в мире», в рамках которой зарубежные эксперты представили своё видение ситуации и перспективы развития РКИ как технологии, широко используемой во всём мире. В центре внимания были безбумажный товаросопроводительный документооборот и растущие объёмы трансграничной торговли. Большой интерес делегатов Форума вызвал международный опыт решения противоречия между различиями в законодательствах стран и критической необходимостью в доверии к механизмам обеспечения юридической силы трансграничных электронных документов.

Рама Ха, эксперт UNNEXT и директор группы по безбумажной торговле KTNET, рассказал об опыте Южной Кореи по упрощению трансграничного безбумажного документооборота. Чтобы реализовать трансграничные безбумажные сервисы, KTNET сотрудничает с Паназиатским альянсом электронной коммерции (Pan Asian E-Commerce Alliance, PAA) — объединением сервис-провайдеров в сфере трансграничной безбумажной торговли, состоящим на данный момент из 12 участников.

Спикер из Индии — Тахсен Кхан, эксперт UNNEXT и заместитель председателя СЕФАКТ ООН — подчеркнул, что

взаимное признание и доверие — один из ключевых факторов трансграничных процессов ЭДО, причём значимость данной дискуссии выходит за рамки только торговых отношений.

При трансграничном электронном обмене данными установление доверия может быть затруднено из-за многих факторов, таких как различия в местном законодательстве, в стандартах электронного обмена и хранения данных. Использование облачных вычислений приводит к получению данных, находящихся в нескольких юрисдикциях. Новые технологии, такие как блокчейн или искусственный интеллект, приводят к увеличению типов и источников данных. Для решения этих вопросов необходим механизм взаимного признания для создания надёжного трансграничного электронного взаимодействия. Вполне возможно, что «Рамочное соглашение об упрощении процедур трансграничной безбумажной торговли», подготовленное ЭСКАТО ООН, станет решением данной проблемы.

ИТОГОВАЯ ДИСКУССИЯ

Последняя часть деловой программы РКИ-Форума — дискуссия по законодательству и стандартизации в РКИ и смежных областях. По большому счёту, экспертам было задано всего два вопроса: что может помочь развитию РКИ в Российской Федерации и чего не хватает российской отрасли РКИ, что может способствовать повышению доверия к сервисам на базе отечественных технологий электронной подписи? Эти



Дискуссия по законотворчеству и стандартизации в РКІ и смежных областях

вопросы вызвали более чем часовое обсуждение не только среди заявленных спикеров, но и среди присутствующих в зале экспертов. Модерировал дискуссию эксперт ISO, заместитель генерального директора «Аладдин Р.Д.» Алексей Сабанов.

Многие эксперты согласились, что необходимо ввести «правильный водораздел» между специалистами, которые занимаются юридически нормативно-правовым регулированием, и техническими специалистами, которые занимаются техническими документами по нормативно-техническому регулированию. При этом их работа должна быть синхронизирована и не должна дублироваться. Также эксперты отметили, что не хватает системности на государственном уровне, до сих пор остаются проблемой вопросы идентификации и аутентификации, а также нет инструмента или технологии проверки архивных ЭП.

Отвечая на вопрос про повышение доверия к сервисам на базе отечественных технологий ЭП, эксперты не были оптимистичны. Например, заместитель генерального директора компании «ИнфоТеКС» Дмитрий Гусев сразу сказал, что повысить доверие к сервисам явно не поможет введение штрафов. «РКІ — это технологически нагруженная тема, требующая в своём

управлении и развитии специалистов и времени. Волшебным образом, в виде введения, например, ответственности оператора (УЦ) в 1 миллиард (почему миллиард? — авт.) доверие к такому оператору не возрастет. А скорее — понизится», — отметил спикер.

Один из выступающих сказал, что принятие новых законов и подзаконных актов может решить эту проблему. Однако, как в конце заключила Нина Соловяненко, «ни один принятый закон ещё никого не осчастливил».

МУЗЕЮ КРИПТОГРАФИИ БЫТЬ

Технологичность РКІ-Форума разбавила презентация Лидии Лобановой, директора Музея криптографии, который распахнёт свои двери осенью 2021 года. Концепция первого в России музея криптографии была разработана год назад. Планируется, что музей будет насчитывать 90 интерактивных инсталляций, которые рассказывают о разных исторических и научных историях и принципах криптографии. Кроме того, там будет и «физическая» коллекция: шифровальная техника, устройства передачи информации, архивные документы.

Экспозиция начнётся с сегодняшней и даже завтрашней цифровой криптографии, далее — переход в научную,

механическую криптографию прошлого века. Заканчиваться выставка будет на времени появления письменности. При этом главной целевой аудиторией музея его создатели считают молодёжь 13–17 лет.

ПРЕМИЯ РКІ

В первый день были также вручены дипломы победителям в ежегодных номинациях РКІ-Форума за 2020 год. По словам организаторов, в этом году программный комитет получил 16 заявок на 5 номинаций, и до последнего момента, до последнего голоса интрига конкурса сохранялась.

В итоге в номинации «Удостоверяющий центр года» победу одержал Региональный удостоверяющий центр Ямало-ненецкого автономного округа; «Организацией года» стало ЗАО «Аладдин Р.Д.»; «Продуктом года» назвали программно-аппаратный комплекс «Служба доверенной третьей стороны «Litoria DVCS», разработанный ООО «Газинформсервис»; а «Проектом года» — проект по модернизации личного кабинета налогоплательщика на сайте nalog.ru ФНС России; и наконец, «Экспертом года» в 2020 году в результате голосования программного комитета признан Иван Янсон, бизнес-партнёр по информационной безопасности ПАО «Сбербанк».

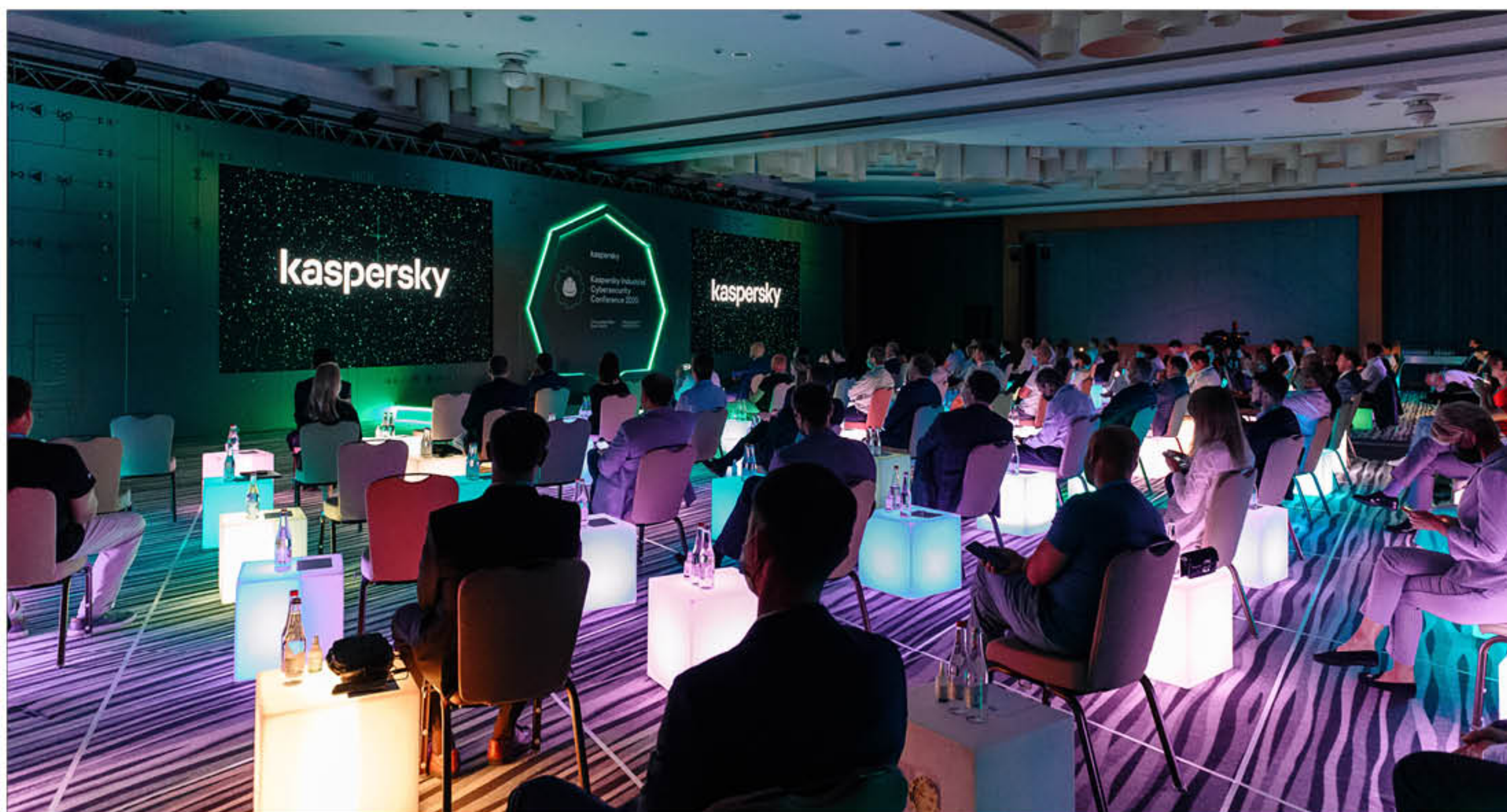


Фото: Kaspersky Events

KASPERSKY INDUSTRIAL CYBERSECURITY CONFERENCE

О КИБЕРБЕЗОПАСНОСТИ ПРОМЫШЛЕННОСТИ ОЧНО И В СОЧИ

В этом году осень принесла возрождение живых встреч. 2–4 сентября в Сочи прошла Kaspersky Industrial CyberSecurity Conference (KICC 2020). И хотя потенциальные иностранные гости так и не решились оставить свои убежища, российские участники не скрывали радости от возможности «почувствовать под ногами сцену».

ТЕРРА ИНКОГНИТА CYBERSECURITY

Из названия мероприятия можно догадаться, что конференция подготовлена «Лабораторией Касперского». Не столь очевидным оказалось содержание термина CyberSecurity. Признаки понятийного хаоса ощутились в ходе выступления представителя «Русатом автоматизированные системы управления», который сообщил, что в своих проектах по автоматизации АЭС он и его коллеги с готовностью и одинаково легко могут заниматься и кибербезопасностью,

и безопасностью информационной, и иными безопасностями, упоминаемыми в отечественной нормативной базе, рекомендациях МЭК и документах МАГАТЭ.

После чего Дмитрий Правиков из РГУ нефти и газа им. И.М. Губкина «усугубил» ситуацию, акцентировав внимание на том, что понятие кибербезопасности «так же неисчерпаемо, как атом»!

Стоит заметить, что представитель славной «Керосинки» представлял также молодой факультет комплексной безопасности ТЭК и ещё ряд некоммерческих организаций, избравших нелёгкую стезю формирования у общества системного взгляда на промышленную безопасность в цифровом мире. В ходе своего доклада «Гармонизация знаний и практик по информационной безопасности в энергетике» он не только заявил о наличии множества смыслов в представлениях о кибербезопасности, но и щедро поделился знаниями, уже наработанными

представляемыми им структурами, для понимания этих смыслов.

И жаль, что доклад этот оказался единственным в своём роде по широте и системности охвата проблем, возникающих в сфере кибербезопасности мира производств.

УНИФИЦИРОВАННЫЙ HANDMADE

В целом KICC 2020 отличал весьма высокий уровень организации при классическом подходе к формированию программы.

Приветствие мэтра, доклады сотрудников созданной мэтром компании, представление перспективных продуктов от Kaspersky Industrial CyberSecurity (флагманы — KasperskyOS и Единая платформа для мониторинга и анализа инцидентов ИБ), выступление партнёров компании (стоит отметить доклад «Как преодолеть глобальный дефицит компетенций промышленной кибербезопасности? Партнёрство

с UNIDO», сделанный Сергеем Коротковым, главой ЮНИДО РФ). И, конечно, «пленарка».

Но при всей унификации ход мероприятия подтвердил максимум «Бог в деталях!». По ходу конференции колоритных деталей, позволяющих разглядеть «лицо» отечественной CyberSecurity, было немало.

О «ПЛЕНАРКЕ»

Умело был сбалансирован состав спикеров «пленарки». Своими соображениями поделились реальные интересанты «отрасли» — так называл цифровую трансформацию модератор дискуссии. Часто «взаимно перпендикулярные» взгляды на разные аспекты CyberSecurity представили: Евгений Касперский — бизнес; Евгений Грабчак, Минэнерго России — промышленность; Андрей Раевский, НКЦКИ — регулятор; Сергей Коротков — повышение квалификации.

Начав с обсуждения темы «Победы и провалы отрасли, прогнозы на ближайший год», спикеры не сочли нужным упомянуть о каких-либо провалах. Но фразы в их ответах на вопросы и реплики по ходу ответов коллег заставили предположить, что отсутствие отдельных провалов — это следствие всё ещё балансирования на краю глобального провала. Балансирования из-за того, что лица, принимающие решения на уровне стран и глобальных корпораций, не определились с реальными возможностями цифровизации и, соответственно, с необходимостью цифровой трансформации. О переменах много говорится, но какие перемены нужны, как безопасно их осуществлять — непонятно.

В рассуждениях же о «частностях» было упомянуто и об отсутствии отечественных аппаратных платформ и элементной микроэлектронной базы для встраиваемых в промышленное оборудование компьютерных систем, и о невозможности безопасного перехода к широкомасштабной «цифровой трансформации» промышленности при опоре лишь на сторонние ЦОДы и коммерческий «телеком». Тогда как построение «проприетарных» отраслевых структур такого назначения входит в противоречие с так называемыми интересами

бизнеса — максимизацией прибыли и отказом от «непрофильных» активов.

Спикеры отметили проблемы, вызванные слабым присутствием на рынке отечественного системного и прикладного ПО для промышленных применений. При этом Евгений Касперский заявил, что создание такого рода продуктов и переход на них по объективным причинам может затянуться на пару десятков лет. И одна из причин — неготовность вендоров оперативно перейти от продуктов и решений, «генетически» связанных с унаследованными из XX века продуктами и платформами, для которых ИБ — это «щит», к новому их поколению, которое позволит строить промышленные объекты КИИ с естественным «иммунитетом» к киберугрозам.

Евгений Касперский также обратил внимание на необычайно возросший за последние годы уровень компетенций у сил, угрожающих промышленным объектам из киберпространства в собственных коммерческих интересах. И это в дополнение к давно существующим силам, вполне официально именуемым кибервойсками (такое название прямо указывает на их предназначение достигать политических целей).

О НЕКОТОРЫХ ДЕТАЛЯХ

Невозможно в коротком репортаже отразить содержание всех «детальных технических докладов», представленных на конференции, но уместно обратить внимание на некоторые мелкие штрихи этих докладов.

Например, на англоязычные тексты на слайдах ряда презентаций. С точки зрения развития внутреннего рынка — это нонсенс. Языковая среда — важнейший фактор для формирования общих подходов и взглядов, а у нас ещё и терминология не сложилась (то ли ИБ, то ли кибербезопасность...), так ещё и общаемся на смешении «французского с нижегородским».

Хотя, конечно, не приходится поступать важностью экспортной ориентированности, когда отечественная индустрия низведена до состояния, когда даже в условиях коронавирусного карантина экономике упасть некуда. И лишь экспорт позволяет удерживать на плаву отечественные разработки ПО и способствовать развитию немногих

ИТ-компаний, подобных «Лаборатории Касперского».

Кстати, это сам Евгений Касперский в ходе «пленарки» вскользь определил своё детище как ИТ-компанию. И эта «оговорка по Фрейду», как можно трактовать слова мэтра с точки зрения «ибэшных» экспертов, высвечивает большую проблему в сфере промышленной кибербезопасности.

На этот «рынок» ринулись, слегка подправив слайды презентаций, «ай-тишники» с шаблонами и стереотипами, сохранившимися ещё со времён «пузыря доткомов». Этаким своеобразный набег «ИТ-туристов» из мира сервисов на заповедник материального производства.

И очень важно, чем закончится встреча этих двух миров, в одном из которых системного администратора «просят», а в другом он, появившись на производстве, будет «должен» и «обязан». И не только в связи с «трудовой», но и в рамках именно осознанной технологической дисциплины.

Пока же по прослушивании части вендорских докладов сложилось впечатление, что ИТ-неофиты рассматривают консерватизм технологической дисциплины на производстве как тормоз на пути к светлому будущему цифровой трансформации.

СВЕТ В КОНЦЕ ТОННЕЛЯ

Ситуацию корректирует существование таких ИТ-компаний, как «Лаборатория Касперского», «ИнфоТеКС», и некоторых других «социально близких» к ним свободных игроков рынка. Начав свой путь в ИТ не на хайпах и быстром извлечении прибыли, но решая «рутинные» вопросы безопасности и надёжности сервисов ИТ для финансово-кредитной сферы, для компаний, занимающихся администрированием бизнеса, для населения, они научились проводить разработки, в которых ИБ стала функцией ИТ. Эта идеология выдерживается и вновь создаваемыми «дочками», специализирующимися на ИТ-поддержке крупных промышленных структур. Выступления представителей этих компаний вселяют надежду, что цифровизация промышленности может пойти по безопасному пути, пусть и неторопливо.

CISO ФОРУМ 2020

БОЛЬШАЯ ВСТРЕЧА КИБЕРДИРИЖЁРОВ НА ЛЕСНОЙ

Организаторы мероприятия «Музыка кибербезопасности» (именно так CISO Форум 2020 обозначил своё видение этой встречи) утверждают, что использовали весенний карантин в интересах дела. Шлифовали программу, а аудитория тем временем копила тоску по живому общению.

Невольно вспомнилась реплика о пользе «пожара Москвы».

«ПРОВАЛ ЛИССАБОНА И МЕССИНЫ» НЕ СОСТОЯЛСЯ

Эксперты, собранные Алексеем Лукацким на пленарном заседании, практически в унисон подтвердили, что внезапный переход на дистанционные технологии работы не вызвал катастрофических последствий для ИБ. А когда въедливый Лукацкий стал требовать конкретики, гости признались, что никакие силы так и не смогли заставить перевести на «удалёнку» работу с внутренним контуром ФинЦЕР Та

и АСУТПэшные контуры на производствах ЕВРАЗ и Северстали.

А для офисных сотрудников были найдены даже плюсы! Ведь бизнес, доселе терпевший ИБ как неизбежное зло, сам пошёл на поклон к CISO, чтобы не было как в фильме «Волга, Волга». Помните? «Совершенно секретно я кричать отказываюсь!» Хотя, по мнению участников «пленарки», действительно требующей защиты является лишь малая толика информации, обращающаяся в коммуникационных сетях российского бизнеса.

Для ИТ же ситуация вообще повернулась в сторону «куй железо, пока горячо!» Ноутбуки продавались как горячие пирожки на ярмарке, а ДИТ Москвы в срочном порядке заказал и развернул безопасную систему коммуникаций для самоизолировавшихся чиновников.

ГОВОРИТЕ, ПОЖАЛУЙСТА, ПО-РУССКИ

Центробанк, похоже, остаётся единственной госструктурой, проводящей

политику уравнивания представлений о важности прибыли и кибербезопасности в сознании руководителей финансово-кредитных организаций. Вполне естественно, что госучреждения держат нос по ветру государственного «комплаенса», а вот бизнес по-прежнему оценивает риски с вероятностью меньше 100% как маловероятные.

Зачином для оценки «стратегических» перспектив корпоративного ИБ послужил мастер-класс «Разговор с бизнесом» Рустэма Хайретдинова. По его авторитетному мнению, сегодняшний бизнес живёт по «планам» с перспективой менее года. А если учесть, что этот самый бизнес в значительной своей части совершенно бесстрашен по природе своего происхождения, то для сохранения его на плаву CISO должен быть не только ИБ-компетентным, но и обладать навыками межличностных коммуникаций не хуже, чем у Труффальдино.

И начинаться эти навыки должны с умения разговаривать с руководством



infor-media Russia
Контакты. Информация. Решения.



на простом русском языке, а не «птичьим» диалекте, в основе которого русифицированные англоязычные термины и аббревиатуры. Финалом же должна стать презентация для руководства. И в ней оценки угроз ИБ и рисков штрафных санкций должны быть приведены в виде финансовых метрик.

На этих двух посылах акцентировали внимание слушателей не только Рустэм Хайретдинов и Алексей Лукацкий (мастер-класс «Афиша для концерта: экономическая эффективность. Презентация ИБ для руководства»), но и Александр Свердлов на, казалось бы, сугубо технологическом мастер-классе по кибергигиене.

И если, называя Алексея Лукацкого, вспоминаешь Cisco и её великолепную ИБ, которую поддерживают 300 вышколенных сотрудников, сотни продуктов, процессов и технологий, то благодаря Александру Свердлову участники форума смогли пополнить копилку своих знаний тем, как небольшим числом сфокусироваться на тех 20% усилий, которые способны обеспечить 80% успеха при защите цифровой инфраструктуры организации, а бизнес (и это главное!) — спасти от убытков и потери прибыли.

Уместно заметить, что мастер-класс Александра Свердлова был проведён в дистанционном режиме, но с высоким качеством двухсторонней связи и возможностью диалога в реальном

времени, что выгодно отличало его от некоторых других примеров использования «удалёнки» в ходе форума.

КАК ПОГАСИТЬ ЗВЕЗДУ

На форуме также состоялась и «прокачка» идей в сфере формирования работоспособного коллектива службы ИБ: от выбора организационной модели до подбора и ротации кадров в условиях дефицита компетентного персонала.

В части организации службы ИБ Мона Архипова (Межрегиональный информационно-расчётный центр (МИРЦ)) и Алексей Плешков (представленный в качестве независимого эксперта, но мы-то знаем!) поделились своим опытом использования так называемых распределённых команд, причём операционный директор МИРЦ посвятил этому целый мастер-класс.

В части подбора и обучения персонала мысли высказывались революционные — звёзд на работу не брать; повышение квалификации проводить за счёт и на территории конкурентов! Над этим следует поразмыслить, хотя сразу возникает вопрос: откуда при таком подходе возьмутся звёзды?

ОБОСТРЕНИЕ ИЗВЕЧНОГО КОНФЛИКТА

На технологических докладах слушателям представили развитие методологии DevOps в сторону DevSecOps — безопасного программирования — и

рассказали о грядущем нашествии «контейнерных» технологий. Компания Palo Alto Networks привела цифры, характеризующие уровень угроз ИБ при использовании сторонних ресурсов программного кода при создании приложений на базе «контейнеров». Тут в качестве гамлетовского вопроса встанёт целый ряд проблем, связанных с тем, что базовой метрикой эффективности создания приложений остаётся «time to market», а конфликт между «do it faster» и «keep it stable» так и не разрешён.

В симфонии CISO Форума 2020 мощно прозвучала тема «комплаенса» в контексте рисков выявления контролирующими органами несоответствий требованиям регуляторов по локализации баз данных с персональными данными. Мастер-классы по защите персональных данных провели Алексей Мунтян и Максим Лагуткин. Тема эта, интересная сама по себе, также открыла новые для ряда слушателей лица экспертов.

Подводя итоги форума, можно сделать вывод о по-прежнему «мета-стабильном» положении CISO и курируемого им направления в организациях, не входящих в контур опеки финансового мегарегулятора. Дирижёры есть, и много. Дело за музыкой.

ВБА-2020

«КОГДА НАД ВАМИ БУДЕТ ЦБ, МНОГИЕ ЖЕЛАНИЯ ПРОПАДУТ!»

Слоган форума ВБА-2020 («Вся банковская автоматизация — 2020») — «Цифровая эволюция в финансах» — не позволяет в полной мере представить страсти, бушевавшие на мероприятии.

ВТОРАЯ ИГЛА

«Лидеры инноваций по версии Сколково». Что можно ожидать от доклада с таким названием, зная, что российский финтех «впереди планеты всей», а европейские банкиры жгуче завидуют высочайшему уровню автоматизации наших банков? Но между строк основной темы вдруг просачивается мысль о пересаживании страны с одной «иглы» — сырьевой — на другую — «иглу высоких технологий». И есть большая вероятность, что эта идея — о специализации страны на одной отрасли, а «остальное купим» — активно протаскивается в высокие кабинеты.

СБП УВОДИТ КЛИЕНТОВ

СБП, внешне благопристойная и добропорядочная, способна, оказываясь, дестабилизировать сложившуюся микросистему банка. Так считает целая группа экспертов. На форуме был представлен доклад «С2В. Только InHouse. Только Hardcore», в котором генеральный директор iD Systems обратил внимание на важность использования локальных технологических решений для взаимодействия с СБП при работе с «юриками». Это, как мыслится компании, позволяет минимизировать риски миграции корпоративных клиентов за пределы финансовой организации, возникающие при подключении банка к СБП.

ПРО ОНЛАЙН

Стоит отметить, что онлайн-аудитория форума, возникшая в этом году на коронавирусной почве, составила пусть и не основную, но вполне заметную часть слушателей и экспертов. И это наглядно продемонстрировало, что не все технологии и платформы дистанционной работы одинаково хороши. Что позволяет

добавить оздоровительную ложку дёгтя в бочку официального мёда о готовности общества к переходу на дистанционные форматы коммуникаций и обучения.

Чего, впрочем, нельзя сказать о ДБО. Платёжные карты и платёжные смартфоны, логины и пароли, фейсы и войсы, мессенджеры и чат-боты... Список достижений и предлагаемых технологий можно было бы продолжить, но и на солнце есть пятна!

Вряд ли можно говорить о «цифровой эволюции в финансах», если «цифровой профиль ждали три года, а сделали за месяц», «за последние 2 года сделано столько, сколько ранее укладывалось в десятилетний период, а темпы выхода обновлений приложений достигают еженедельной частоты». Это один из комментариев директора по инновациям СКБ-Банка на круглом столе «Цифровизация и автоматизация, финтех и инфраструктура — формула успеха в эпоху перемен». И если в мире Виталия Копысова релизы выходят еженедельно, то ежемесячный релиз системы ДБО — это действительно норма жизни.

По крайней мере, такой вывод можно было сделать после доклада «ДБО физюрика — как основной канал коммуникации клиента и банка», с которым онлайн выступил коммерческий директор компании «Информационные системы». Он представил систему ДБО isFront, фишкой которой было совмещение обслуживания частных и коммерческих счетов клиента, что позволяет ощутимо сократить стоимость содержания ДБО.

И хотя выступление коммерческого директора было дистанционным, стенд компании на выставке форума оказался вполне физическим. Как рассказали его хозяева, релизы у них выпускаются не только ежемесячно, но и индивидуально под каждого клиента компании.

РЕПЛИКА В СТОРОНУ

Но так ли богата наша страна интеллектуальными ресурсами, чтобы еженедельно/ежемесячно гонять пиксели по пользовательским интерфейсам, не

имея при этом #конкурентопобедившего и самое главное #импортокапризного независимого пакета ОС для того, что сегодня делается на #частноамериканской платформе?

ПРО КАЧЕСТВО ПО

Отдельная проблема — качество любых программных разработок. Но тут, похоже, ФСТЭК и ЦБ подводят сообщество вольных финтехеров к верному стилю работы. Об этом поведали доклады «Становление и развитие механизмов технического регулирования в области защиты информации и кибербезопасности для российских финансовых организаций» (от ТК-122 Банка России), «Практика соответствия требованиям ЦБ РФ» и «Подтверждение соответствия требованиям Профиля защиты ЦБ РФ» (от «НПО „Эшелон“»), пропитанные упоминаниями и ссылками на Положения 382/683/684-П и документы со всё более узнаваемыми цифробуквенными обозначениями ГОСТ Р 15408-3-2013, ГОСТ Р 57580, ГОСТ Р 56939-2019 и другие.

БОЛЬШИЕ НАДЕЖДЫ

Помимо жаркого обсуждения вала ИБ-вызовов, обрушившегося и планомерно, и аврально на банковскую систему страны, на финальной встрече форума нашлось время и для визионерских обсуждений ситуации на рынке финтеха. В качестве перспективных векторов были названы «стриминг данных» (рекомендательные сервисы для клиентов в режиме реального времени), персонализация предложений, СБП, развитие технологий управления ценными бумагами «для домохозяек». И нельзя не упомянуть о надеждах экспертов на то, что при всех пертурбациях нынешнего мира банки сохранят ядро своей деятельности в виде доверительного управления деньгами.

МНОГО ЛЮБОПЫТНОГО

Форум также продемонстрировал, что «лицом» эффективного банка должна стать дистанционная омниканальность,

поддержанная умными чат-ботами. Тем более что ни у кого из «говорящих голов» российского финтеха не вызывает сомнения, что голосовой помощник может быть умным. А в условиях пандемии — ещё и гигиеничным. «НейроДБО — тёплое голосовое общение согревает вас и вашего клиента — надёжная защита от пандемии», — так звучало название доклада, представленного компанией BSS.

А ЧТО НУЖНО ЛЮДЯМ?

Завершилась же работа форума дискуссией о том, должны ли «финтехи» строить финансовые экосистемы или

им стоит аккуратно следовать в русле процессов, возглавляемых регулятором, и проектов банковских топов.

При этом Елена Смышляева из ЦФТ сознательно оставила «за кадром» ответ на вопрос «зачем?» в своём докладе об участии компании в проекте «Маркетплейс». В результате консенсус в ответах на вопрос о «комунужности» маркетплейсов и нужности их как таковых так и не был достигнут, хотя спикеры финального круглого стола выказали большую эрудицию по части предположений о нуждах россиян в финансовых услугах и о нужде банков в населении

России. Единственного, «чего в этом супе не хватало», так это достоверной информации с мест о том, какой же банк нужен российской глубинке.

В целом форум ВБА-2020 продемонстрировал, что «доверенное» ядро российского финтеха сохраняет боевой раж, а его продукция востребована банками, которые активно ищут свою «формулу успеха» не только «в эпоху перемен», но и в условиях заботливого внимания Центробанка к устойчивости банковской системы. Что и дало основание для утверждения Виталия Копысова, вынесенного в подзаголовок репортажа.

MOBIFINANCE-2020

СКОРО КАЖДЫЙ ЧАЙНИК БУДЕТ ПЛАТИТЬ САМ ЗА СЕБЯ

— Ну и где здесь информационная безопасность? — спросил главный редактор. — Я её не вижу!

— Вот и я не вижу, — ответил корреспондент. — А она здесь есть!

Такой диалог состоялся в редакции после знакомства с анонсом программы конференции «Мобильные финансы — 2020» / MobiFinance-2020.

И оба оказались правы.

«ОСТАВАЙТЕСЬ НА ЛИНИИ!»

Специальной секции по информационной безопасности на конференции не было. И это указывает на то, что рынок «мобильных финансов» всё ещё не mature market. Хотя он «большой и привлекательный».

Но, как говорил персонаж отечественной кинокомедии: «Если я большая, это не значит, что я доступная!» Действительно, одна из проблем приложений для мобильного доступа к финансовым услугам — это (простите за тавтологию) их доступность. Точнее, отсутствие оной, особенно когда она очень нужна. «Оставайтесь на линии! Ваш звонок очень важен для нас!» — эта фраза, звучащая в самый неподходящий момент, хорошо знакома всем россиянам.

Природа НЕдоступности мобильных финансовых приложений многолика. Например, в несоответствии возможностей ИТ-инфраструктуры обслужить

кусочек рынка, на который замахнулись бизнесмены. Но это лишь одна из угроз.

Ю. Божор (в мегарегуляторе он руководит экспертной группой Службы по защите прав потребителей и обеспечению доступности финансовых услуг) заострил внимание на другом. Он рассказал о проблемах людей с ограниченными возможностями. Далеко не единицы отечественных банков озабочены решением этой задачи. Но результаты разработок таковы, что некоторые из приложений для людей с ограниченными возможностями требуют физических возможностей вполне 100 %-х.

«Кряк, кряк и в продакшн!» Так охарактеризовал Юрий Божор доминирующую на рынке ИТ технологию разработки приложений. Под занавес конференции весьма ехидно прошёлся по методологии agile и независимый эксперт М. Митусов. Уже в связи с недуманными попытками быстро копировать сомнительный зарубежный опыт.

ФАНТАЗИИ И РЕАЛЬНОСТЬ

Многие нереализованные ещё идеи были озвучены на заключительной дискуссии «Ближайшие прорывы в мобильных финансовых сервисах. На что ставить и во что вкладывать?» Тут А. Колесников из iSimpleLab анонсировал готовность выйти за рамки смарт-

фонов и перейти ко всеобщей «финансовой мобильности» на основе «интеллекта» бытовой техники.

Смелую идею предложил К. Маркелов из АРБ. Он завёл речь о переходе от мобильного управления финансами гражданина в конкретном банке к дистанционному управлению некими обобщёнными финансовыми активами россиянина. Следует заметить, что зал весьма неоднозначно оценил эту инициативу.

Более жизнеспособным выглядело предложение выйти на зарубежные рынки и завалить их «лёгкими» банковскими приложениями, востребованными иностранными финансистами. И совершенно реальными выглядят перспективы, открывающиеся американскими санкциями в отношении компании «Хуавэй».

И ВОТ ОПЯТЬ

Финальная дискуссия не обошлась без обсуждения угроз ИБ, которые видны уже сегодня. И это не только приснопамятный agile. Это ещё и просто низкий профессионализм команд, набранных из «летунов», успешно перемещающихся по «высушенному» кадровому рынку. А ведь впереди триумф OpenAPI, который, образно говоря, откроет каждой кухарке дорогу к разработке финансовых приложений для банков.



Сергей ВИХОРЕВ
советник генерального
директора
ООО «ИТ-Экспертиза»

*Прежде чем выйти из кабины лифта...
Убедитесь, есть ли земля!
Доктор Алешин (Максим Алешин)*



ЦИРК УЕХАЛ, КЛОУНЫ ОСТАЛИСЬ

ЭССЕ О ТРУДОВЫХ ОТНОШЕНИЯХ, ПОСТПАНДЕМИЙНОМ
ПЕРИОДЕ И БЕЗОПАСНОСТИ ИНФОРМАЦИИ

ПАНДЕМИЯ И ТРУДОВОЙ КОДЕКС

Я не хотел бы, чтобы читатели воспринимали фразу, вынесенную в заголовок, в отрицательной коннотации. Давайте будем позитивными. Я вкладываю в неё примерно такой же смысл, как во фразу «дома новы, а проблемы стары».

А поговорить я хотел бы о нововведениях в Трудовой кодекс, толчком к которым послужила злополучная пандемия. Мы все выходим (и слава богу, успешно!) из этого испытания другими. И жизнь в постпандемийный период уже не будет такой, как раньше. Надо привыкать к новым реалиям. И одной

из таких реалий является необходимость и возможность удалённой работы сотрудников. После пандемии экономические, социальные, деловые и прочие связи изменяются до неузнаваемости. Большинство из тех, кто уже принял новую модель работы, не захотят возвращаться к офисному варианту. Мнения

об эффективности удалённой работы разные. Многие считают, что за счёт отвлекающих факторов и отсутствия самоконтроля эффективность «домашней» работы падает. Однако учёные Стэнфордского университета утверждают¹, что производительность труда в домашних условиях увеличилась на 13%. Но сейчас не об эффективности новой модели работы. Это удел хозяев бизнеса, которые, соизмерив KPI работников и экономию на аренде помещений и коммунальных услугах, будут оценивать эффективность удалёнки и необходимость перевода на неё своих сотрудников.

Сейчас вот о чём. На сегодня права работника в условиях удалённой работы не регулируются законодательством, в Трудовом кодексе фигурирует только понятие дистанционной работы. Авторы законопроекта, который внесли в парламент 16 июня, предлагают добавить понятия «временная дистанционная (удалённая) работа» и «комбинированная дистанционная (удалённая) работа». Это позволит работникам официально работать вне стационарного рабочего места, а переводить на такой режим сотрудников можно будет на основании как минимум трёх факторов — соглашения сторон, производственной необходимости или обстоятельств непредвиденного характера. Кроме того, для дистанционных работников предлагают, так же как и для обычных, закрепить режим труда. Они получают право не быть на связи с работодателем круглосуточно.

Предусмотрен и упрощённый порядок введения режима временной дистанционной (удалённой) работы, который должен предусматривать издание локального нормативного акта с установлением списков работников, переводимых с их согласия на временную дистанционную (удалённую) работу, а также порядок организации режима временной дистанционной (удалённой) работы. И при этом в этих локальных актах должны быть отражены в том числе и вопросы возмещения связанных с выполнением удалённой работы расходов: оплата электроэнергии, используемого

программного обеспечения, включая антивирусную защиту, использование работником личного оборудования, программно-технических средств, средств защиты информации и других расходов. Ну, к этому чуть позже.

Проектом изменений в Трудовой кодекс также предусматривается право работодателя устанавливать дополнительное условие об обязанности дистанционного работника использовать при выполнении им своей трудовой функции оборудование, программно-технические средства, средства защиты информации и иные средства, предоставленные или рекомендованные работодателем. А это уже важно с точки зрения безопасности информации.

ОТНОШЕНИЯ НОВЫЕ — ПРОБЛЕМЫ СТАРЫЕ

Вот и получается, новые производственные отношения возникли, а проблемы безопасности информации — остались старые. Я уже, раскрывая концепцию доверенной среды, как-то писал о ситуации, когда сеть работодателя находится в защищённом сегменте, к которому предъявляются особые требования по безопасности информации. И он подконтролен администратору безопасности, который следит за тем, чтобы были соблюдены правила доступа пользователей, чтобы всё программное обеспечение было доверенное, чтобы, не дай бог, не пролез какой-нибудь троян. Но в ситуации, когда исчезает само понятие «периметр», администратор безопасности ничего проверить не может: территория и зона ответственности — не его, он сюда доступа не имеет. Но есть жёсткое требование бизнеса — работать удалённому пользователю. Даже если удалённый пользователь прошёл все установленные процедуры идентификации — аутентификации — авторизации и у администратора безопасности нет, кажется, оснований не допустить пользователя в закрытую сеть, он не может быть уверен, что все эти требования по обеспечению безопасности информации на удалённом рабочем месте выполнены.

О ДОВЕРЕННОЙ СРЕДЕ

Проще говоря, возвращаясь к теме, работодатель (или его доверенное лицо — администратор безопасности) должен

иметь возможность контролировать, с помощью каких программно-технических средств и средств защиты информации сотрудник осуществляет свои трудовые функции. Мы должны быть уверены в лояльности всех элементов информационной системы, то есть доверять им. Если мы сможем быть уверенными в надёжности каждого элемента, в том числе удалённых рабочих мест, нам не обязательно изолировать их в замкнутой среде. Это и есть смысл концепции «доверенной среды».

Здесь появляется проблема оценки доверия к тому устройству, на котором пользователь проводит процедуру идентификации — аутентификации — авторизации. Чтобы минимизировать риски и обеспечить доверенную среду обработки информации, необходимо обеспечить постоянный мониторинг состояния удалённых рабочих мест. Администратор безопасности должен иметь инструмент, позволяющий в момент подключения рабочего места к информационной системе и в течение всего сеанса взаимодействия контролировать состав аппаратного и программного обеспечения удалённых рабочих мест, определять тип и состав зарегистрированных USB-устройств, проверять запущенные в операционной системе процессы и доступность сетевых сред, работу антивирусных средств, уметь регистрировать любые события, влияющие на безопасность рабочего места и, в частности, регистрировать любые изменения в аппаратной и программной среде, нарушения правил информационной безопасности. Такой инструмент должен позволять указать строгий перечень разрешённых к использованию удалёнными сотрудниками устройств и программного обеспечения и проводить отслеживание нежелательных изменений в реальном времени. Другими словами, оберегать удалённых сотрудников от небезопасных действий.

О РАСХОДАХ

А теперь о проблеме возмещения связанных с выполнением удалённой работы расходов. Сразу же соглашусь с оппонентами, которые могут сказать, что эта проблема не имеет отношения к безопасности информации. Да, это

¹ <https://zen.yandex.ru/media/cfo/kak-korona-virus-meniayet-otnoshenie-kompanii-k-udalennoi-rabote-5e8342248274cd4de920c1ca>

так. Но с другой стороны, Трудовой кодекс требует от работодателя для учёта расходов контролировать использование работником программного обеспечения, включая антивирусную защиту, личное оборудование, программно-технические средства, средства защиты информации. То есть работодатель должен иметь возможность контролировать, чем занимается работник на удалёнке. С технической точки зрения эта задача полностью аналогична задаче контроля доверенной среды на удалённом рабочем месте. А если это так, то зачем выдумывать велосипед? Почему же нельзя средства

мониторинга доверенной среды использовать и для целей контроля затрат на выполнение удалённой работы? Это, прямо как Head & Shoulders, два в одном.

ВЫХОД ЕСТЬ!

В заключение хочу сказать, что сейчас на рынке имеются средства мониторинга состояния безопасности информации. Но это, как правило, достаточно большие и дорогие комплексы, имеющие очень большой и зачастую избыточный перечень функций. Да и не всегда они «заточены» под решение озвученных проблем. Для их настройки и

эксплуатации требуются высококвалифицированные специалисты и постоянное обращение к специализированным мониторинговым фирмам, способным правильно выработать правила обнаружения инцидентов безопасности информации. Это не всегда по карману бизнесу, особенно если он входит в SMB-сегмент. Но есть на рынке и недорогие, простые в обслуживании и не требующие специально обученных людей системы, которые имеют гибкую настройку параметров контроля и создания правил контроля для каждого компьютера, позволяют визуализировать динамику результатов мониторинга.

Примером недорогой, но эффективной системы, позволяющей решить проблемы обеспечения доверенной среды обработки защищаемой информации в распределённых информационных системах, может служить программный комплекс «САКУРА» (Система Активного Контроля Удалённой Работы АРМ).

В чём отличие комплекса «САКУРА» от SIEM-систем? Любая SIEM-система является внешней по отношению к информационной системе. Это элемент апостериорной защиты. Её можно сравнить с томографом, который позволяет определить «болевы» точки в информационной системе и выработать тактику устранения проблем. В отличие от SIEM, комплекс «САКУРА» является неотъемлемой частью самой информационной системы, он находится внутри неё. Это своеобразный нерв информационной системы, который моментально реагирует на любые отклонения от установленных параметров и при необходимости блокирует проблемный участок информационной системы.

Комплекс «САКУРА» выполняет роль элемента априорной защиты, он позволяет получать актуальную информацию и историю изменения рабочих мест, контролирует все действия на удалённом устройстве, проверяет, какие

антивирусы и программное обеспечение установлены на рабочем месте, наличие обновлений операционных систем, анализирует «поведенческую модель» сотрудника, проводит аудит доступа к компьютеру, запрещает использование нежелательных программ и уведомляет о возможных рисках. «САКУРА» может автоматически отключить удалённого сотрудника от корпоративных ресурсов при выявлении нарушений, которые могут привести к краже конфиденциальной информации.

Комплекс «САКУРА» обеспечивает выполнение мер обеспечения безопасности информации, предусмотренных ГОСТ Р 57580.1 (БФО), Положением Банка России № 382-П (НПС), Приказом ФСТЭК России № 17 (ГИС), Приказом ФСТЭК России № 239 (КИИ).

Комплекс «САКУРА» имеет программную реализацию и построен на клиент-серверной технологии. При этом АРМ могут быть развёрнуты на операционных системах как Windows, так и Linux.

Узнайте подробнее о решении «САКУРА» и получите консультацию экспертов по информационной безопасности по телефону: +7(499) 450 2886 или на сайте компании «ИТ-Экспертиза» <https://it-expertise.ru/products/sakura>



В отличие от внешних систем диагностики, которые лишь дают основу для принятия решений, **САКУРА** – это интегрированный внутренний механизм, который **сразу устраняет** возможные угрозы



Ольга ЛИМОНОВА
психолог
ООО «Антифишинг»



Андрей ЖАРКЕВИЧ
редактор
ООО «Антифишинг»



«ОТДЕЛКА ЩЕНКА ПОД КАПИТАНА»¹»

ОРГАНИЗАЦИОННОЕ И ДОКУМЕНТАЦИОННОЕ
СОПРОВОЖДЕНИЕ ПРОЦЕССОВ ОБУЧЕНИЯ
И ТРЕНИРОВКИ НАВЫКОВ ИБ

Большая часть специалистов по информационной безопасности уже пришли к пониманию необходимости обучения и тренировки навыков сотрудников. Однако практическая реализация этих процессов во многих случаях представляет собой продукт «интуитивных» экспериментов, а также попыток добиться положительного результата методом проб и ошибок. Очевидно, что для получения нужного результата требуется другой подход — основанный на научных исследованиях и проверенных психологических методиках.

Мы начинаем публикацию цикла статей, который поможет ИБ-службам качественно организовать процессы обучения и тренировки. В них мы поделимся собствен-

ным опытом и универсальными наработками, которые легко адаптировать и использовать в собственной практике. Это позволит избежать типовых ошибок и предупредить множество неприятных рабочих ситуаций, начиная от разрешения конфликтов с отдельными сотрудниками и заканчивая необходимостью объяснить вышестоящему руководителю рациональность тех или иных мер и нововведений.

Первая статья посвящена тому, как организовать адаптацию сотрудников компании к процессу обучения и тренировки навыков в сфере информационной безопасности.

Вторая рассказывает о том, как справиться с возражениями сотрудников, по той или иной причине отказывающихся проходить обучение и тренировки навыков.

¹ Цитата из повести А. Грина «Алые паруса»

АДАПТАЦИЯ ПЕРСОНАЛА К ПРОЦЕССАМ ОБУЧЕНИЯ И ТРЕНИРОВКИ НАВЫКОВ ИБ

Проблема внедрения новых процессов в работу кажется вечной, особенно если это касается процессов обучения и тренировки навыков ИБ. Даже простое изменение платформы для обучающих курсов нередко приводит к тому, что сотрудники перестают соблюдать установленные правила. Когда же процессы требуется создать с нуля, сопротивление экспоненциально возрастает.

В этой статье мы поговорим о том, как использовать методы адаптации для процессов ИБ, чтобы систематизировать все необходимые действия и объединить их в единый план-программу.

ЧТО ТАКОЕ АДАПТАЦИЯ И ЗАЧЕМ ОНА НУЖНА?

Адаптация персонала — процесс «привыкания» сотрудников к новой деятельности в компании. HR-коллеги под «адаптацией персонала» понимают интеграцию в рабочий процесс и корпоративную культуру новых сотрудников и тех, кто перешёл на новую должность или в другой отдел.

Таким образом, адаптацию персонала к процессам ИБ можно рассматривать как начальное знакомство новых сотрудников с принятыми в компании правилами ИБ, первичное обучение и тренировку навыков ИБ, а также разъяснительную работу по новым процессам и инструментам ИБ, внедряемым в компании.

Можно выделить следующие преимущества, которые даёт компании система адаптации персонала к процессам ИБ:

- ♦ сохраняется необходимый уровень производительности труда при минимуме затрат временных, экономических и административных ресурсов со стороны сотрудника и компании;

- ♦ новый сотрудник быстрее получает доступ к информационным ресурсам компании;

- ♦ уменьшается риск серьёзных инцидентов безопасности;

- ♦ уменьшается число конфликтов, возражений и неожиданных увольнений;

- ♦ поддерживаются положительные отношения сотрудников с ИБ-отделом;

- ♦ снижается уровень стресса, тревожности и неуверенности сотрудников перед соблюдением правил ИБ, потенциальными ошибками в процессе обучения и тренировки навыков.

Чем качественнее проходит адаптация, тем меньше возникает в дальнейшей работе возражений, конфликтов, недопониманий и нарушений установленных норм. Для этого адаптация должна быть чётко организована и регламентирована, иметь ясную цель, понятную и логичную структуру. Добиться этого поможет индивидуальная корпоративная программа адаптации персонала к процессам ИБ в компании, содержащая основные этапы адаптации, инструменты реализации и взаимодействия с сотрудниками, временные рамки и критерии оценки эффективности/успешности адаптации.

Основные этапы адаптации персонала к процессам ИБ включают в себя:

- 1. Оценку уровня подготовленности.** Необходимо определить уровень текущих знаний и навыков ИБ сотрудника: какие у сотрудника есть знания в области личной цифровой безопасности, был ли опыт столкновения с мошенниками, проходил ли он обучение и тренировку имитированными атаками на предыдущем месте работы. Оптимальнее всего выяснить это на этапе собеседования или в течение первой недели работы нового сотрудника с помощью интервью, анкетирования или опросника.

- 2. Вводное информирование.** Включает в себя начальное знакомство со-

трудника с общими правилами ИБ в компании, кратким описанием обязательных процессов, в том числе обучением и тренировками, системой поощрения за правильные действия и наказания за неправильные. Этот этап важен, поскольку избавляет сотрудника от неприятных сюрпризов и формирует восприятие процессов ИБ как чего-то само собой разумеющегося и неизбежного. Лучше всего этот этап совместить с оценкой уровня подготовленности на этапе собеседования или в течение первой недели работы нового сотрудника.

- 3. Первичный инструктаж.** Первое полное ознакомление сотрудника со всеми регламентирующими документами по ИБ, непосредственно связанными с его работой. Оптимально проводить в течение первого месяца работы нового сотрудника в электронном или бумажном виде.

- 4. Первичное обучение.** Первый назначенный курс обучения в данной компании. Оптимально проводить в течение первого месяца работы нового сотрудника, совместив с проверкой знаний в виде тестирования.

- 5. Первичную тренировку навыков.** Первые три имитированных атаки, назначенные сотруднику, чтобы оценить качество усвоения теоретических знаний на курсе обучения и имеющиеся навыки распознавания цифровых атак. Эту проверку лучше провести в течение месяца после прохождения сотрудником первичного обучения.

- 6. Оценку успешности адаптации.** Этот этап представляет собой подведение итогов адаптации сотрудника. При этом сравниваются первоначальная и итоговая оценки подготовленности, определяется, все ли этапы были успешно пройдены, где возникли затруднения и т.д. Оптимально проводить спустя полтора-два месяца после приёма сотрудника или с момента окончания последнего этапа адаптации.

№	Инструмент	Описание
1	Инструктирование	Включает в себя вводное, первичное и повторное инструктирование по существующим документам в сфере ИБ. Может включать дополнительные инструкции по безопасному использованию каких-либо систем/программ, поведению с каким-либо контентом/ресурсом «здесь и сейчас»
2	Информирование	Представляет собой актуальные информационные рассылки, призванные поддерживать актуальные знания сотрудников об ИБ. Это может быть ИБ-аналитика, громкие инциденты, актуальные примеры атак и т.д.
3	Предупреждение	Вид информационной рассылки, носящий предупреждающе-остерегающий характер о потенциальных инцидентах, атаках на компанию и т.д. В отличие от информирования, содержащиеся в рассылке указания обязательны для исполнения
4	Оповещение	Вид информационной рассылки, отвечающий за оповещение сотрудников о происходящих в компании или конкретно с ним ИБ-процессах. Например, что с N периода начнётся массовая тренировка сотрудников / рассылка имитированных атак, что сотруднику назначен курс обучения или промежуточное тестирование и т.д.
5	Напоминание	Вид информационной рассылки, отвечающий за напоминание сотрудникам о необходимости совершить какие-либо обязательные действия в части процессов ИБ, а также напоминание сотрудникам, нарушившим сроки обучения или тестирования
6	Отчёт	Вид информационной рассылки, содержащий итоговые данные по процессам ИБ в компании, отдельном департаменте, отделе или конкретно по сотруднику. Носит важную мотивационную функцию

Таблица 1. Инструменты общения с персоналом

ИНСТРУМЕНТЫ ВЗАИМОДЕЙСТВИЯ С СОТРУДНИКАМИ ПО ПРОЦЕССАМ ИБ

Если технические инструменты, как правило, привычны и понятны, то инструменты поддержания коммуникации с сотрудниками, проходящими адаптацию, могут вызывать вопросы. Особенно если необходимо налаживать их регулярное использование, структурировать общение.

Рассмотрим некоторые инструменты, которые позволяют наладить взаимодействие с сотрудниками. Их использование не ограничивается адаптацией новых сотрудников. Получив начальные навыки, сотрудники привыкают в дальнейшем использовать их для повседневной работы.

Важный момент: внедрение новых ИБ-процессов часто вызывает раздражение и сопротивление у «костяка», состоящего из опытных сотрудников.

Чтобы этого раздражения избежать, нужно регулярно общаться со всем персоналом посредством следующих инструментов, перечисленных в табл. 1.

Поддержание всех перечисленных способов взаимодействия с персоналом — сложная задача, которая полностью находится в сфере ответственности специалистов по ИБ. Однако систематическое применение данных инструментов формирует стабильный и надёжный канал связи со всеми сотрудниками, создаёт положительное и ответственное отношение сотрудников к ИБ как к неотъемлемой части всех рабочих процессов.

Использование этих инструментов позволяет провести «рефрейминг», изменив отношение сотрудников с «безопасники мешают работать» на «компания снижает риски», «пользователи повышают свой уровень / устойчивость к мошенникам» и т.п. Для этого следует использовать позитивные формулировки,

избегать приказного тона, включать в письма элементы заботы, поддержки и понимания. Разумеется, необходимо помнить и о базовых принципах корпоративной этики: вежливости, краткости, ясности и своевременности.

ЧАСТОТА ВЗАИМОДЕЙСТВИЯ ПО ПРОЦЕССАМ ИБ

Регулярность взаимодействия с сотрудниками по процессам ИБ подразумевает наличие определённой периодичности и правил коммуникации, которые также должны быть прописаны в программе адаптации в виде плана-графика.

Мы рекомендуем придерживаться частоты и триггеров взаимодействия, перечисленных в таблице 2.

ВАЖНО! В зависимости от подготовки и опыта нового сотрудника, его психологических качеств и специализации срок адаптации к процессам ИБ может составлять от двух месяцев до полугода.

№	Инструмент	Триггер	Частота
1	Инструктирование	Появление нового сотрудника Появление новых процессов или инструментов ИБ, затрагивающих работу инструктируемого Внесение значимых для изменений в инструкции	Для нового сотрудника: от 3 раз в первый год. Для рядового сотрудника: от 1 раза в год + по мере появления новых инструкций
2	Информирование	Появление новой актуальной информации о мошеннических схемах, громкие кейсы и примеры атак	Не реже 1 раза в месяц
3	Предупреждение	Появление риска инцидента	По мере необходимости
4	Оповещение	Появление назначенных сотруднику актуальных задач по обучению, тренировке, тестированию и т.д.	Сразу после назначения задачи, не реже 1 раза в квартал
5	Напоминание	Повторное оповещение по прошествии N времени от основного срока задачи (например, в середине срока и за 5 дней до его окончания) Появление нарушения сроков выполнения назначенных задач	За 10 и 5 дней перед окончанием срока выполнения задачи; Сразу после нарушения срока выполнения задачи; По прошествии 5, 10 и N + 5... дней после нарушения срока выполнения задачи
6	Отчёт	По итогам процессов ИБ за N период	По мере необходимости, не реже 1 раза в год

Таблица 2. Рекомендуемые частота и триггеры взаимодействия

ОЦЕНКА АДАПТАЦИИ ПЕРСОНАЛА К ПРОЦЕССАМ ИБ

Как любой целенаправленный процесс, адаптация персонала в ИБ нуждается в подведении итогов, которое позволяет оценить эффективность реализации адаптации, а также выявить необходимость коррекции или доработки.

Результат адаптации показывает, насколько успешно сумел пройти все этапы, научился использовать все необходимые ИБ-инструменты. В качестве итога сотруднику может присваиваться статус адаптации (успешно/неуспешно), выставляться оценка на основании результатов тестирования и имитированных атак, составляться рейтинг успешности по компании и т.д.

По результату адаптации сотрудники делятся на следующие типы:

1. Неадаптивные. Сотрудник не разделяет корпоративных ценностей, не следует установленным нормам и

правилам. В процессе адаптации это может проявляться в виде игнорирования сообщений от специалистов по ИБ, непрохождении назначенных курсов обучения, злостном нарушении правил безопасности и т.п. Чаще всего такие сотрудники увольняются в первые месяцы работы или их увольняют за низкую производительность труда.

2. Адаптивные. Сотрудник целиком принимает и следует установленным правилам, выполняя все поставленные перед ним задачи. Данный тип сотрудников обычно представляет большую часть штата любой компании.

3. Ложноадаптивные. Сотрудник формально принимает установленные правила и следует им, выполняя все поставленные перед ним задачи, однако внутренне не согласен с данными процессами. В итоге он после испытательного срока начинает нарушать установленные процессы ИБ или увольняется, подобно неадаптивным коллегам.

4. Адаптивные индивидуалисты. Сотрудник целиком принимает установленные правила и следует им, выполняя все поставленные перед ним задачи, при этом сохраняя свою точку зрения и отношение к данным процессам, что выражается в активном соучастии в их преобразовании и доработке.

Адаптация персонала — одна из наиболее сложных задач, падающих на плечи специалистов по информационной безопасности. Тем не менее последовательное применение приведённых в статье инструментов позволяет решить эту задачу с приемлемыми затратами времени и ресурсов, но самое главное — сформировать фундамент корпоративной ИБ-культуры и создать у сотрудников целостное понимание важности соблюдения требований безопасности.

РАБОТА С ВОЗРАЖЕНИЯМИ СОТРУДНИКОВ В ПРОЦЕССАХ ОБУЧЕНИЯ И ТРЕНИРОВКИ НАВЫКОВ ИБ

Работа с возражениями сотрудников по поводу любых нововведений в рабочие процессы — важная часть обучения и тренировки навыков ИБ у сотрудников. Опыт крупных компаний показывает, что специалисты ИБ просто не знают, как корректно реагировать на сопротивление со стороны неподконтрольных им коллег.

В этой статье мы рассмотрим основные виды возражений против обучения, их причины и формы проявления, расскажем, как реагировать на возражения сотрудников и прогнозировать их, поделимся краткосрочными стратегиями, которые помогут «здесь и сейчас», а также обсудим долгосрочные стратегии формирования позитивного имиджа отдела ИБ в компании.

ВОЗРАЖЕНИЯ КАК СИМПТОМ

Нововведения и возражения тесно связаны между собой, поскольку возражения представляют собой естественную, чаще всего бессознательную, реакцию человека на вторжение в его личное пространство. Прежде чем принять новшества, человеку требуется время на их критическое осмысление. Именно это и происходит с сотрудниками, когда им помимо основной работы приходится заниматься обучением и тренировкой навыков ИБ.

Неизбежность возражений не означает, что можно возложить всю ответственность на самих сотрудников и пустить процесс на самотёк, руководствуясь правилом «решаем проблемы по мере их поступления». Любой опытный менеджер по продажам подтвердит, что, если возражения вовремя снять, в дальнейшем они уже не будут возникать. Таким образом, возражения

можно рассматривать как показатель зрелости и проработанности способов внедрения новых процессов в существующую структуру компании и рабочие привычки коллег.

♦ Если вы только начинаете заниматься развитием навыков безопасного поведения сотрудников, начните с долгосрочных стратегий предотвращения возражений сотрудников.

♦ Если вы уже ведёте данные процессы и регулярно сталкиваетесь с сопротивлением и негативом со стороны коллег, вам пригодятся краткосрочные решения, от которых можно постепенно перейти к реализации долгосрочных.

Важно! Не стоит полагаться исключительно на краткосрочные решения. Используя их, необходимо в любом случае ориентироваться на долгосрочные решения, поскольку именно долгосрочные решения позволяют проработать положительную мотивацию сотрудников, а эффективность краткосрочных, как правило, проявляется в виде мотивации «избежание наказания».

ТИПЫ ВОЗРАЖЕНИЙ И ЧТО С НИМИ ДЕЛАТЬ

У каждого возражения может быть как рациональная причина, связанная, например, с неудобством выстроенного процесса, так и совершенно иррациональная причина, проявляющаяся в виде психологического сопротивления, которое нужно помочь преодолеть. Понимание причины возникновения возражения помогает выбрать оптимальный способ его преодоления.

Выявление корректной причины появления возражений — основная трудность для специалистов ИБ. В разборе возражений мы сделаем особый акцент на психологические аспекты и

«сигналы», которые помогут понять истинную природу возражений, а следовательно, выбрать правильный алгоритм работы с ними.

Будет ценно, если вы соберётесь всей командой ИБ и выпишете все возможные возражения, которые могут возникнуть именно у вас в компании с учётом внутренней специфики.

Мы выделяем 15 типов возражений сотрудников:

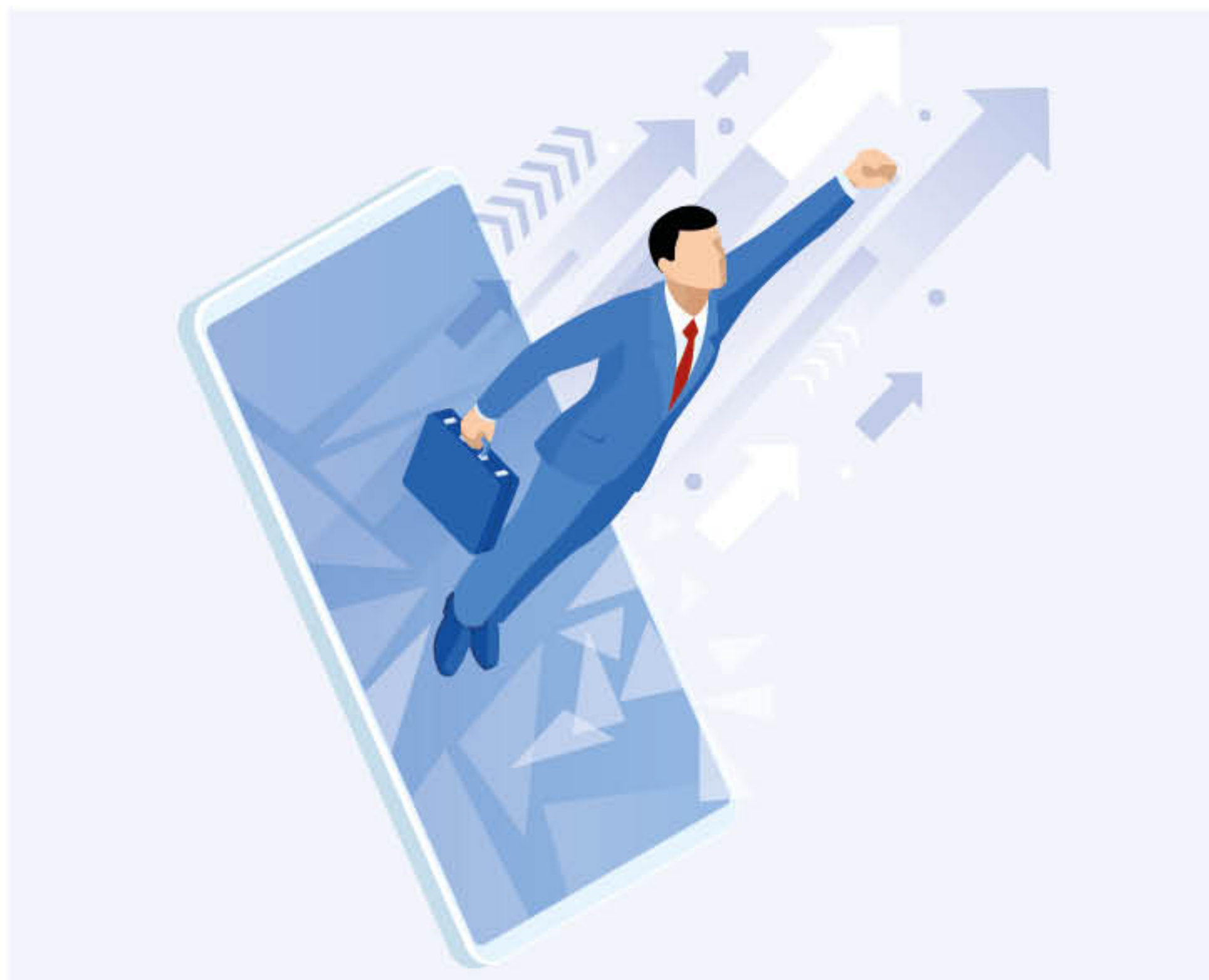
1. «Мне некогда проходить это обучение. Можно перенести на потом?»
2. «Я уже это проходил. Опять?»
3. «Я и так всё это знаю, отстаньте».
4. «Это слишком сложно».
5. «Это всё равно ничего не даст».
6. «На меня нет атак! Зачем меня кому-либо взламывать?»
7. «Извините, забыл».
8. «У вас там что-то глючит, всё поломано».
9. «Это не входит в мои должностные обязанности».
10. «Всё равно вы мне ничего не сделаете».
11. «А что мне за это будет?»
12. «Я уволюсь, если не отстанете».
13. «Мой начальник настаивает, чтобы я сначала сделал свою работу».
14. «Меня не предупреждали, не рассказали правила, я тут ни при чём...»
15. Полное игнорирование.

Рассмотрим эти возражения, их причины и способы их решения подробнее.

1. «МНЕ НЕКОГДА ПРОХОДИТЬ ЭТО ОБУЧЕНИЕ/ТРЕНИРОВКИ»

Причины

У сотрудника действительно может быть много работы и не хватать времени на прохождение обучения/тренировок. Но чаще всего подобную фразу используют как отговорку,



которая придаёт важности не желаемому проходить обучение сотруднику и позволяет скрыть лень или страх неудачи.

Как отличить одно от другого? Предложите сотруднику самому выбрать удобное время и день для прохождения обучения, при этом оговорив временные рамки, например, не позднее чем до конца квартала.

Если человек ссылается на то, что и тогда не найдёт 20 минут для обучения, скорее всего, сработает стратегия «утверждено начальством и является частью работы». Пытаться рационально объяснить полезность обучения в такой ситуации бессмысленно.

Проработка лени и страхов в данном случае возможна только с помощью долгосрочных решений, которые предполагают последовательное формирование у сотрудников фундаментального представления о данных процессах как об обязательных и абсолютно безопасных, что в процессе обучения можно ошибаться, это не вызовет последующего осуждения или каких-либо санкций.

Краткосрочные решения

♦ Предложите выбрать удобное время/день для прохождения обучения/тренировок:

«Добрый день, (коллега)! Принимая к сведению вашу рабочую нагрузку, предлагаем согласовать удобное вам время и дату прохождения обучения и тренировок. Будет ли вам удобно сделать это (в данный временной промежуток)?»

♦ Используйте авторитет вышестоящего руководителя: обратитесь к руководителю сотрудника, чтобы тот самостоятельно выбрал и назначил время/дату прохождения обучения/тренировок для данного сотрудника.

♦ Объясните, что данные процессы являются частью обязательной работы: *«Добрый день, (коллега)! К сожалению, данное обучение/тренировки невозможно отменить/перенести на столь отдалённый период. Они обязательны для всех сотрудников, включая руководителей, и в соответствии с п. XX трудового договора являются обязательной частью вашей работы.»*

Просим пройти назначенное обучение/тренировки до (указанного срока), иначе мы будем вынуждены (принять меры административного воздействия)».

Долгосрочные решения

♦ Для преодоления лени сотрудников закрепите обязательность соблюдения правил ИБ, своевременного прохождения обучения/тренировок в трудовом

договоре, должностной инструкции, регламенте/уставе работы.

♦ Для преодоления страхов сотрудников сформируйте «безопасную среду» для обучения и тренировки навыков ИБ: повсеместно и регулярно транслируйте мысль, что ошибки в обучении и тренировках неизбежны и ценнее их полного отсутствия, что ошибки в обучении и тренировках не влекут за собой наказания и ущерба по сравнению с реальными атаками, которые возможны.

♦ Чтобы снять рациональные возражения, обеспечьте изначальную гибкость графика обучения/тренировок, возможность выбора сотрудниками удобного для них времени обучения/тренировок.

2. «Я ЭТО УЖЕ ПРОХОДИЛ. ОПЯТЬ?»

Причины

Человеческий мозг так устроен, что не любит совершать бессмысленные повторяющиеся действия без очевидного профита, который может получить «здесь и сейчас». Это касается и изучения учебного материала, который сотрудник уже проходил.

Другой рациональной причиной может быть непонимание сотрудниками необходимости регулярно проходить обучение и тренировки ИБ. Для большинства пользователей новые угрозы неотличимы от старых, как и меры противодействия им. Технические детали различий остаются за границей понимания. Из-за этого люди не могут применить полученные теоретические знания для распознавания реальной киберугрозы.

Здесь эффективно работает обычное информирование, которое объясняет, почему необходимо регулярно проходить тренировки и обучение, в чём их отличия, как это влияет на работу и безопасность компании в целом.

Основными нерациональными причинами данного типа возражений являются лень и скука. И ошибочным решением здесь будет поспешить сделать обучение более лёгким, ярким, весёлым, анимированным. Лень и скука — психологический защитный механизм, который преодолевается обязательностью данных процессов. Всё, что кажется людям необязательным, рано или поздно

вызовет подобные эмоции, поскольку они служат эволюционным способом экономии собственных энергоресурсов на «ненужные, необязательные вещи».

Краткосрочные решения

- ♦ Объясните, что данные процессы являются частью обязательной работы.
- ♦ Объясните ценность регулярного обучения/тренировок.

Долгосрочные решения

- ♦ Формируйте у сотрудников представление о процессах ИБ как о системных и регулярных. Добавляйте эту информацию в начало всех учебных курсов, обеспечьте каждого сотрудника доступом к учебному плану, проводите промежуточную оценку актуальных знаний и навыков.

- ♦ Транслируйте ценность актуальных знаний ИБ: регулярно информируйте сотрудников о количестве атак, которые удалось детектировать с их помощью за период, поощряйте сотрудников за активное участие в этом процессе.

- ♦ Создайте систему рейтинга или нескольких рейтингов для постоянного вовлечения сотрудников в данный процесс. Рейтинг может представлять собой топ-10 сотрудников, чтобы привлечь индивидуалистов, или топ-3 отдела для командных игроков. Важно обеспечить понятные всем правила формирования данного рейтинга, а также постоянный открытый доступ к нему для всех сотрудников.

- ♦ Давайте сотрудникам возможность сравнивать свои предыдущие результаты обучения/тренировок с текущими. Для этого необходимо фиксировать имеющиеся результаты и накапливать данную статистику. Это позволит сотрудникам видеть свою динамику, улучшение или ухудшение результатов, а также послужит подтверждением того, что обучение и тренировка навыков требуют регулярности и систематичности.

3. «Я И ТАК ВСЁ ЭТО ЗНАЮ, ОТСТАНЬТЕ»

Причины

Этот тип возражений крайне редко бывает рациональным и к тому же является одним из самых сложных для обработки. Понять это помогает эффект Даннинга — Крюгера, который заключается в том, что умные/компетентные люди склонны больше сомневаться в

своей компетентности, в то время как люди, не отягощённые интеллектом, практически не способны осознать свою ограниченность. Как следствие, к таким возражениям чаще всего прибегают некомпетентные сотрудники с завышенной самооценкой.

Рациональный вариант этого возражения можно встретить, когда сотрудник искренне считает, что его образования, знаний или пройденного ранее разового обучения в сфере ИБ хватит на всю оставшуюся жизнь. К сожалению, среди этой аудитории часто попадают сами специалисты по ИБ.

Стратегия обработки данного типа возражений схожа с предыдущими, но включает в себя дополнительный обязательный элемент необходимости «приземлить» сотрудника путём назначения дополнительных сложных атак или внезапного тестирования знаний ИБ, а также наглядной демонстрации его результатов обучения/тренировок. Хорошо работает неформальное манипулирование самоуверенностью через спор «на слабо»: «если сдашь всё на отлично — можешь не обучаться». Однако такой неформальный тип общения подходит не для всех коллективов. По очевидным причинам это не сработает в

общении с oldschool-руководителями, которые требуют к себе особого отношения и уважения просто в силу занимаемой должности или большого опыта работы.

Краткосрочные решения

- ♦ Объясните важность поддержания актуальных знаний ИБ.

- ♦ Предложите пройти промежуточное тестирование как способ проверки того, что сотрудник действительно всё знает:

«Добрый день, (коллега)! В связи с вашим нежеланием проходить обязательное регулярное обучение/тренировки было принято решение пойти вам навстречу и провести итоговое тестирование ваших знаний ИБ: (ссылка на тест).

Просим пройти назначенное тестирование до (указанного срока). В случае если вы покажете отличный результат, подтвердив полноту и актуальность ваших знаний ИБ, дальнейшее обучение и тренировки будут для вас отменены и заменены коротким промежуточным тестированием».

- ♦ Назначьте сложную атаку с использованием новых мошеннических форм манипулирования и ярким нестандартным способом обратной связи



(индивидуальная финальная страница со скриншотом лица сотрудника и т.п.), чтобы эмоционально задеть и показать несостоятельность возражения сотрудника.

♦ Покажите сотруднику имеющуюся актуальную статистику по поведению сотрудников в компании (или его личную). Наглядные цифры — отличный аргумент, тем более когда отличников априори не может быть, ведь все рано или поздно ошибаются.

Долгосрочные решения

♦ Чаще тренируйте сотрудников и предоставляйте им обратную связь по итогам имитированных атак. Сделайте тренировку и проверку навыков привычной процедурой, которая позволяет выявлять слабости и уязвимости ваших сотрудников по разным техническим и психологическим векторам. Яркая и эмоционально затрагивающая обратная связь — отличный способ зафиксировать в сознании сотрудников понимание того, насколько они могут быть уязвимы независимо от их оценки собственных познаний в ИБ.

♦ Проводите промежуточное тестирование знаний ИБ у сотрудников. Это позволит сотрудникам адекватно оценивать свои текущие знания ИБ, а также наблюдать свой прогресс или регресс.

♦ Создайте систему рейтинга дляощерения конкуренции и наглядности личных успехов. Отлично подходит для аргументации фраза «Если ты всё знаешь, почему же ты не на первом месте?». А если без шуток, то для людей с завышенной самооценкой бывает очень болезненно терять свою корону, поэтому мотивация конкуренцией для них одна из самых сильных.

4. «ЭТО СЛИШКОМ СЛОЖНО»

Причины

Рациональная причина этого возражения состоит в том, что назначенный курс обучения, тестирование или имитированные атаки действительно слишком сложны для данного сотрудника, особенно если он сталкивается с ним впервые. Очевидно, что в такой ситуации учебные материалы нуждаются в адаптации по уровню сложности и категориям сотрудников, поскольку HR-специалисты в любом случае будут менее компетентны в вопросах ИБ, нежели сотрудники службы ИТ.

Если же это единичные возражения-отговорки, не связанные с уровнем сложности учебных материалов, истинная причина, скорее всего, состоит в страхе неудачи или банальной лени. Универсальное оружие против ленивых

сотрудников — обязательность. В случае низкой самооценки и страха неудачи сотруднику требуется дополнительное положительное подкрепление, подбадривание. Избегайте здесь негативных коннотаций и негативных мер мотивации «от наказания».

Краткосрочные решения

♦ Пойти навстречу и дать возможность пройти более лёгкое обучение/тренировки. Оптимальный вариант, если ваши учебные и тренировочные материалы разделены по уровням сложности.

♦ Объясните, что ошибки гораздо ценнее полного бездействия:

«Добрый день, (коллега)! Данное обучение/тренировки соответствуют вашему уровню знаний/навыков ИБ. Не бойтесь ошибаться, это неотъемлемая часть процесса. Чем больше ваша насмотренность в атаках и методах социальной инженерии, тем более вы защищены. Поверьте, лучше 10 раз ошибиться, чем ни разу не пройти обучение / тренировку навыков.»

Пожалуйста, пройдите назначенное обучение/тренировки до (указанного срока). (На первых этапах / первые месяцы) результаты обучения/тренировок ни на что не влияют и не несут за собой никакого (наказания/штрафа)».

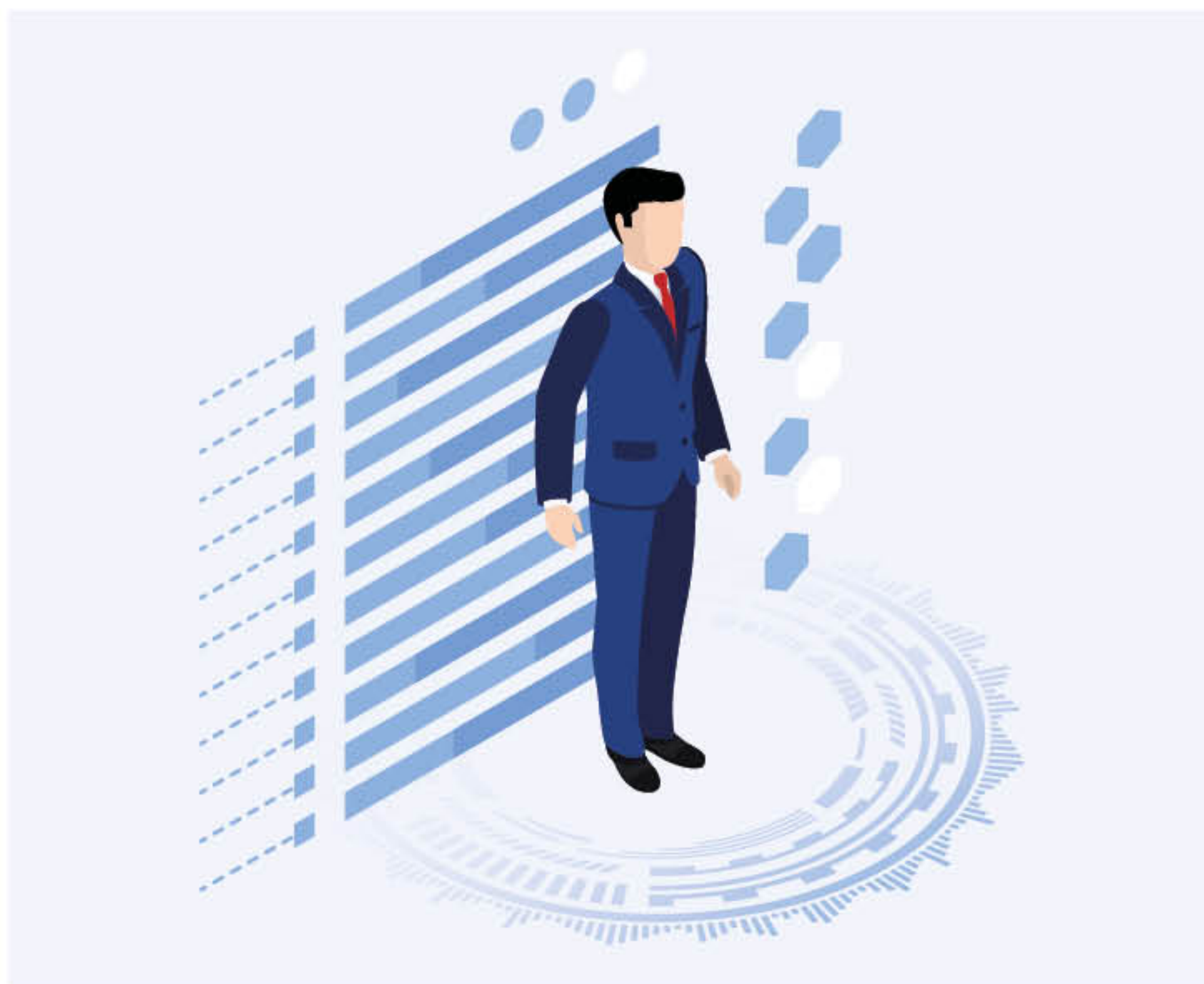
Долгосрочные решения

Разделите контент для обучения/тренировки по уровню сложности, если это ещё не сделано.

♦ Дайте возможность сотрудникам самим выбирать уровень сложности материалов. Это отлично работает, если сотрудник через личный кабинет может сам выбрать курс обучения, имитированную атаку и её сложность, а вам приходят уже оповещения и результаты данных процессов.

♦ Сформируйте «безопасную среду» для обучения и тренировок. Для этого транслируйте идею «безопасности ошибок» через курсы обучения и обратную связь. Идеально, если безопасную среду обучения удастся объединить с системой материальной мотивации, организовав её так, чтобы на начальном этапе обучения/тренировок ошибки не влекли за собой штрафы или другие взыскания.

(Продолжение в следующем номере)



СКАМ НА БАРАХОЛКЕ

ДИСТАНЦИОННОЕ МОШЕННИЧЕСТВО
НА ТОРГОВЫХ ПЛОЩАДКАХ ГЛАЗАМИ
АНАЛИТИКА SOC



Алексей ПЛЕШКОВ
эксперт BIS Journal

Просматривая в СМИ региональные дайджесты инцидентов и комментарии к ним от МВД, заметил: ежедневно совершаются мошенничества в отношении держателей банковских карт. К примеру:

♦ «30-летняя жительница Краснодара, увидев на сайте бесплатных объявлений заметку о продаже самоката, решила его приобрести. После длительной переписки с продавцом в мобильном мессенджере девушка перевела мошеннику 8000 рублей, но доставки товара так и не дождалась».

♦ «38-летний житель Красноармейского района Волгограда разместил на торговой площадке в Интернете объявление о продаже электрического счётчика. Спустя несколько часов ему пришло сообщение с предложением купить у него вышеуказанный товар. В процессе диалога со злоумышленником житель Волгограда получил ссылку на подставной сайт, на котором указал реквизиты, а также CVV-код от банковской карты. Выполнив все условия, мужчина обнаружил списание со своего счёта более 6 тыс. рублей».

В зоне риска оказались пользователи, продающие или покупающие товары дистанционно, в том числе с применением сервиса доставки или пересылки. В УМВД по г. Астрахань отмечают, что за первую половину 2020 г. в регионе зарегистрирован 631 факт мошенничества, 599 из них были совершены дистанционно. И это только те случаи, о которых заявлено в полицию. В масштабах РФ речь может идти о десятках тысяч таких случаев.

АЛГОРИТМ МОШЕННИЧЕСТВА

Для аналитиков профильного ситуационного центра финансовой организации представленная картина выглядит достаточно прозрачно. Все случаи мошенничества на «Авито» и «Юле» происходят приблизительно по одному сценарию. А именно:

♦ жертва (продавец или покупатель) вступает в диалог с мошенником в чате по инициативе последнего (при этом товар, его стоимость и характеристики значения не имеют, так как товар — это всего лишь повод для начала диалога);

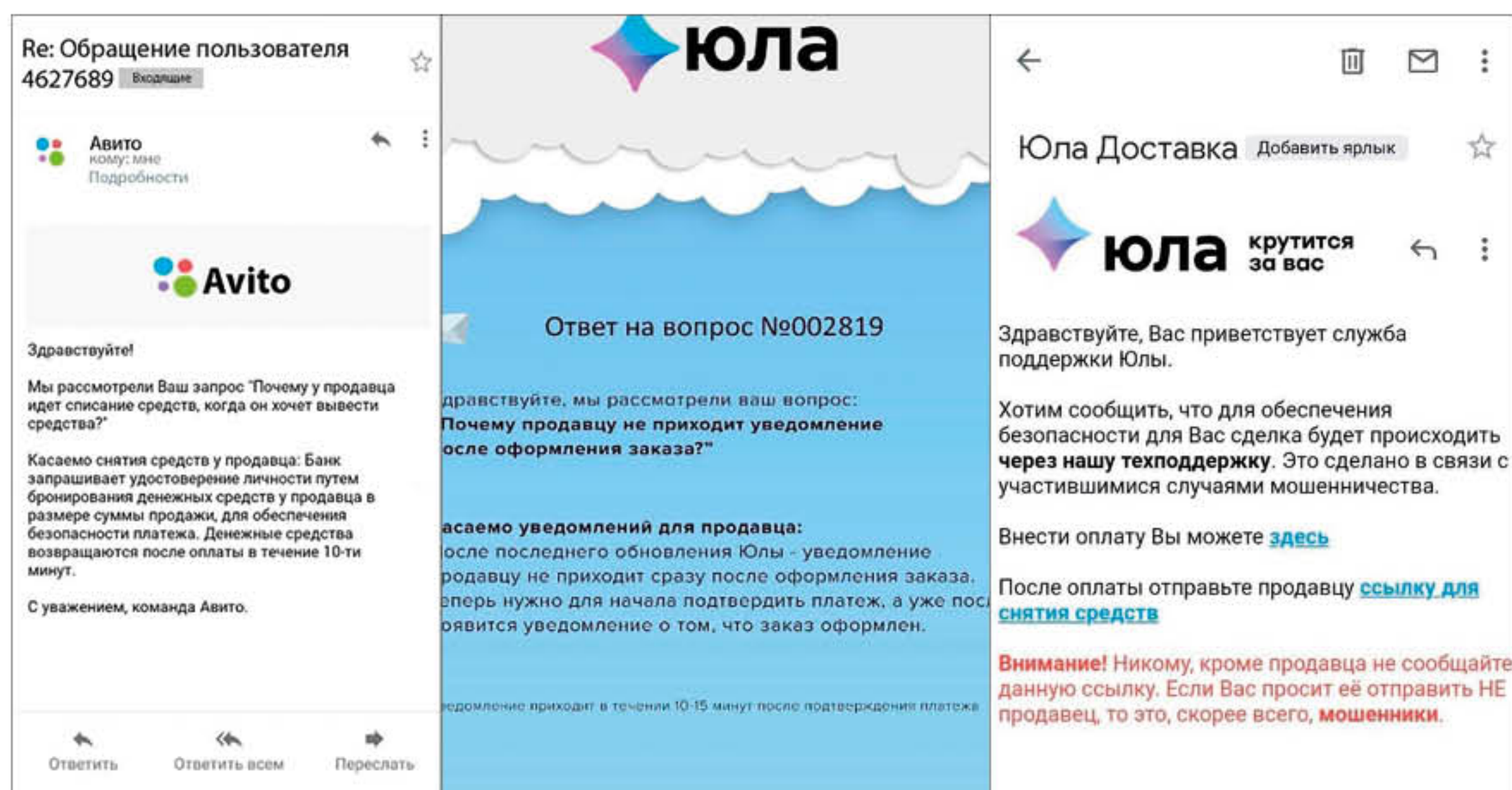


Рисунок 1. Примеры поддельных скриншотов общения с технической поддержкой

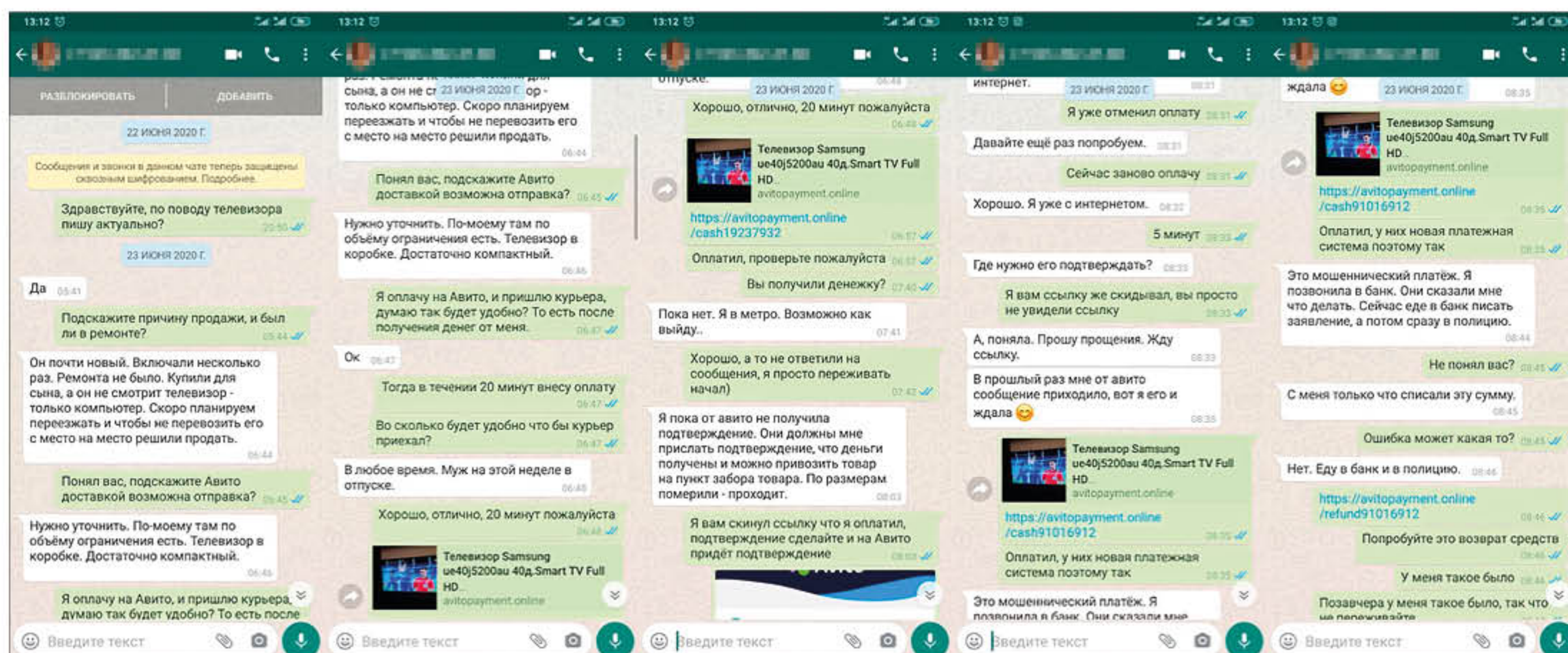


Рисунок 2. Коллаж, пример реального диалога жертвы с мошенником (вид со стороны мошенника), схема Авито 2.0. Жертва — продавец, мошенник выступает в роли покупателя товара

♦ после непродолжительного общения в чате торговой площадки (2–3 сообщения) мошенник под благовидным предлогом предлагает жертве уйти/перейти с торговой площадки и продолжить общение в «более удобном», но менее контролируемом внешнем чате (WhatsApp, Telegram, Viber, Mail.ru);

♦ обсудив во внешнем чате типовые детали сделки, мошенник выдвигает условия, которые требуют заказа сервиса доставки товара получателю;

♦ мошенник берёт на себя инициативу по оформлению сделки и доставки, после чего присылает жертве (по электронной почте или в чате) подготовленную специально для неё фишинговую ссылку на «новую» платёжную систему торговой площадки, подтверждая свои слова поддельным скриншотом своей переписки со службой технической поддержки (рис. 1);

♦ пройдя по ссылке, жертва получает предложение либо оплатить товар (схема 1.0), либо получить на свою карту полную сумму, временно заблокированную (со слов мошенника) на торговой площадке (схема 2.0) (рис. 2);

♦ жертва, введённая в заблуждение мошенником с применением методов социальной

инженерии и НЛП, указывает в форме реквизиты своей пластиковой банковской карты на поддельной странице и отправляет их злоумышленникам, которые совершают в автоматическом режиме р2р-перевод денежных средств на реквизиты карты дроппера; далее средства транзитом пересылаются по выбранной схеме обналичивания;

♦ если жертва начинает задавать вопросы в чат и что-либо подозревать, ей тут же предлагается оформить «возврат товара» и «получить деньги» обратным переводом, для чего мошенники создают новую фишинговую ссылку; пройдя по ней и повторно указав реквизиты своей пластиковой банковской карты, жертва ещё раз подтверждает р2р-перевод своих денежных средств на карту дроппера в стороннем банке (мошенники получают удвоенный доход).

ПРИМЕР СКАМА

Данная активность в интернете не нова. Она имеет устоявшееся название: скам (от английского SCAM — афера, мошенничество). В юридическом плане скам как вид мошенничества соответствует определению в статье № 159–3 УК РФ: хищение чужого имущества или приобретение права на чужое имущество путём обмана или злоупотребления доверия (мошенничество с использованием электронных средств платежа), включая завладение чужим имуществом или имущественными правами посредством блокировки, удаления, модификации или иного воздействия на средства хранения, передачи или обработки электронных данных либо информационно-телекоммуникационных сетей.

Если жертва начинает задавать вопросы в чат и что-либо подозревать, ей тут же предлагается оформить «возврат товара» и «получить деньги» обратным переводом, для чего мошенники создают новую фишинговую ссылку

Рисунок 3. Скриншот платёжного интерфейса страницы <https://p2p.chelinvest.ru>

Рисунок 4. Скриншот платёжного интерфейса страницы <https://card2card.ru>

СКРЫТАЯ ЧАСТЬ СКАМ-СХЕМ

Веб-интерфейсы для создания форм и реализации p2p-переводов в настоящее время предоставляют на коммерческой основе как отдельные финансовые организации, так и крупные порталы-агрегаторы. Техническая спецификация API размещена в публичном доступе (рис. 3–4).

По состоянию на август 2020 года описанные scam-схемы вышли за пределы РФ и успешно реализуются отечественными скамерами на торговых площадках, аналогичных «Авито» и «Юле», в странах Евросоюза, в Казахстане и Белоруссии.

СКАМ-КОМАНДЫ В ЦИФРАХ

Реализация и настройка скриптов, тестирование интерфейсов, администрирование хостинга, регистрация новых доменных имён, создание профильных каналов и сопровождение ботов в Telegram, поиск и обучение новых участников схемы (в терминах скама — worker'ов), взаимодействие с сервисами по обналаживанию денежных средств, ведение внутреннего учёта и взаиморасчётов с участниками операций — это только малый перечень ежедневных задач скамеров. Поэтому скамом злоумышленники промышляют в группах (командах). Скам-схема, пример которой приведён на иллюстрации выше, адаптирована под дистанционный формат взаимодействия. Строгая иерархия и точное понимание роли и функций каждого участника в scam-команде, а также мануалы и иллюстрации, содержащие примеры диалогов между скамером и реальной жертвой, позволяют scam-схеме более полугода развиваться на просторах RU-нет и привлекать в свои ряды новых участников.

В настоящее время в Telegram действует более 70 активных scam-команд. В scam-команду может входить до 1000 учётных записей пользователей Telegram. У каждой группы есть организатор, который чаще всего выступает в роли конечного бенефициара или технолога. Для сопровождения технической части в scam-команду привлекается специалист (саппорт). Для поиска и базового обучения новых участников предусмотрена роль кадровика/модератора/чекера. Остальные участники scam-команд — это worker'ы (кидалы, разводилы). В их задачу входит поиск и обман жертв на торговых площадках. По статистике, активных worker'ов в scam-команде не более 5–7% (рис. 5).

На примере одной из «молодых» scam-команд, созданной в начале июля 2020 года и работающей со схемами Авито 1.0/2.0, Юла 1.0/2.0, приведён экспресс-анализ и определены базовые экономические метрики схемы. Получены следующие цифры:

- ♦ время существования scam-команды (отчётный период): 14 дней;
- ♦ количество участников: 419 учётных записей;
- ♦ количество worker'ов, хотя бы раз совершивших обман жертвы: 19 учётных записей;
- ♦ количество совершённых мошеннических операций с подтверждённым результатом: 45 раз;
- ♦ наиболее популярная scam-схема мошенничества: Авито 2.0. (более 50% от общего количества);
- ♦ общая сумма похищенных за период данной scam-командой денежных средств: 204 624 рубля;

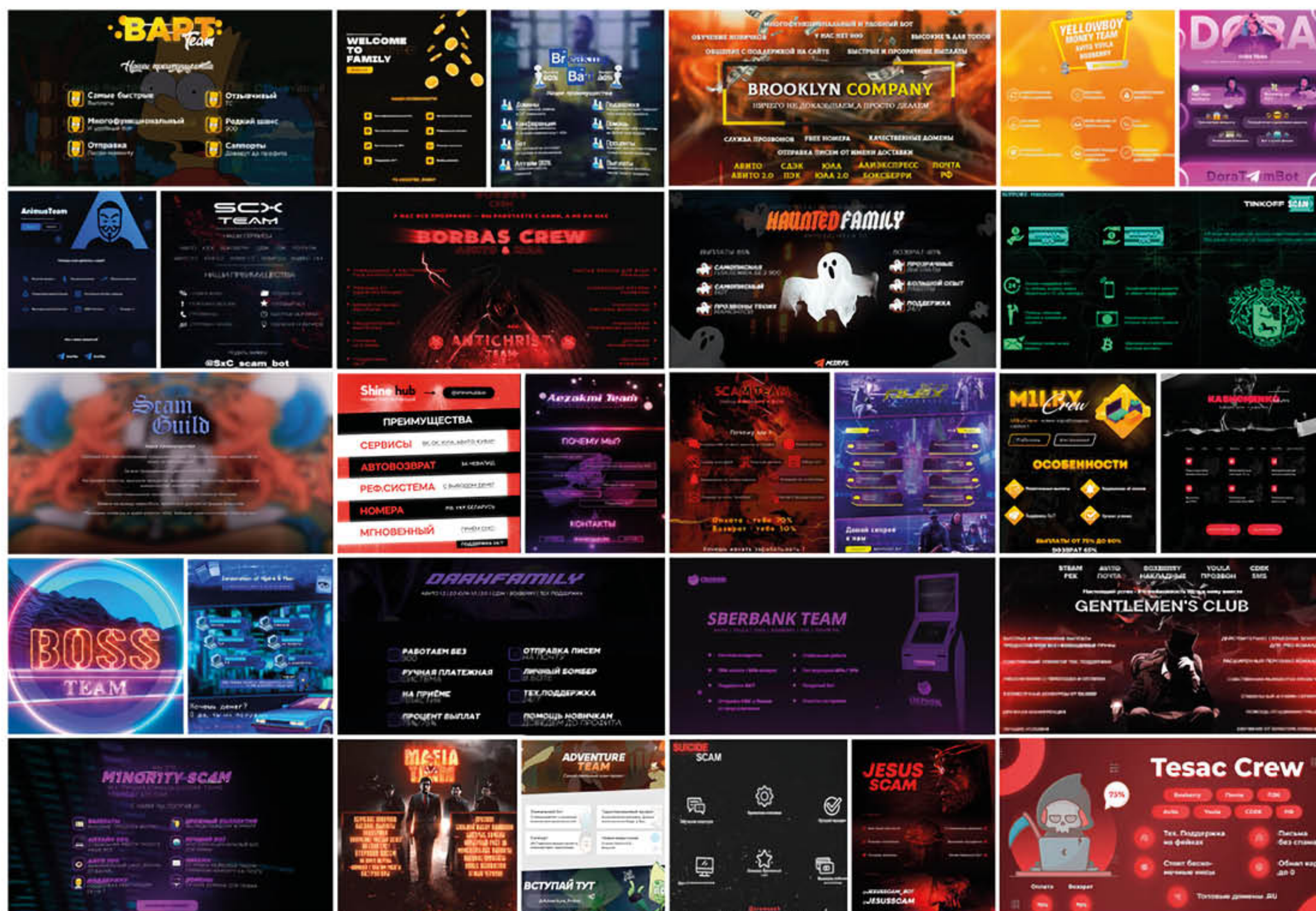


Рисунок 5. Коллаж из баннеров и объявлений от скам-команд о наборе новых участников, размещённых в telegram-каналах и на профильных форумах в darknet

- ♦ максимальный доход worker'a от одной жертвы за указанный период: 15 000 рублей;
- ♦ максимальное количество обманов жертв, совершённых одним worker'ом за период: 8 раз;
- ♦ максимальный «грязный» (до обнала и комиссий) доход worker'a за период: 31 840 рублей;
- ♦ прибыль организаторов от работы скам-команды за отчётный период составила: 43 478 рублей.

ПРИЗНАКИ СКАМ-СХЕМЫ

В процессе анализа материалов скам-схемы выявлены признаки, которые могут помочь участникам: явным (жертвы, торговые площадки) и неявным (банк-эмитент пластиковой карты жертвы) выявлять и не допускать дальнейшего развитие аналогичных схем мошенничества.

Топ-3 признаков скама с точки зрения жертвы на торговой площадке

Признак № 1. В диалоге о покупке/продаже вторая сторона предлагает продолжить общение во внешнем по отношению к торговой площадке чате. В сообщении умышленно искажается

форма написания email (вместо адрес@домен.ru пишется отдельно адрес собака домен точка ру) или наименование выбранного для продолжения общения мессенджера (вместо «WhatsApp» указывается «ВотсАпп», «В0тсап», «Вацап» и т.д.). Примеры таких сообщений:

«У меня муж хотел бы сейчас сесть за ноутбук. Можем продолжить обсуждение в вотсап в телефоне? *номер*. Спасибо!»

«Можно я Вам пришлю ГС (голосовое сообщение) в TG? Мне лень печатать».

Признак № 2. Вторая сторона по сделке в диалоге просит прислать email / номер телефона для передачи ссылки на оплату / получение товара. При этом поступившая ссылка отличается (частично или полностью) по внешнему виду и написанию от наименования торговой площадки, на которой происходит сделка.

Признак № 3. Вторая сторона по сделке просит прислать ей дополнительную информацию, которая поступает напрямую из банка или от торговой площадки (одноразовый пароль, секретный код, разгласить содержание полей в веб-формах или SMS-сообщениях) и не должна

раскрываться в процессе сделки, ссылаясь на собственный опыт и регулярно возникающие технические ошибки на площадке («я знаю, потому что так уже делал», «у меня так уже было вчера с другим», «это у них новые правила, мне тоже не всё понятно» и т.д.).

Топ-3 признаков скама с точки зрения аналитика ситуационного центра (на торговой площадке)

Признак № 1. Существенное (в количественном измерении, исходя из ранее определённых метрик, согласованных лимитов и существующей скоринговой модели) отклонение сценария работы от типового профиля пользователя торговой площадки.

Примерами таких отклонений являются:

- ♦ вход под существующей учётной записью с IP-адреса иностранного государства либо пула IP-адресов региона РФ, отличного от указанного при регистрации;
- ♦ после захода в профиль пользователя отключение всех уведомлений, настроек безопасности и каналов общения, кроме общения в чате на сайте;
- ♦ отключение в профиле учётной записи способа доставки товара гарантированными сервисами торговой площадки.

Признак № 2. При автоматическом анализе содержания диалогов между пользователями на торговой площадке могут быть выявлены паттерны, характеризующие попытку увода жертвы во внешний чат по ключевым словам/фразам (WhatsApp, Telegram и искажённые формы написания этих названий, такие как Вотсап, WA, WatsUp и пр.) в диалогах, а также на основе анализа ответов (указывается номер телефона — 10–11 цифр с разделителями, email — @, фразы «вот мой номер», «моя почта» и т.д.).

Признак № 3. Косвенным подтверждением факта реализации скам-схемы в отношении активного пользователя может являться появление «замерших» / неоконченных или внезапно завершённых на моменте передачи номера телефона / email диалогов в чате площадки.

Топ-3 признаков скама с точки зрения антифрод-офисера ситуационного центра банка-эмитента

Признак № 1. Попадание в чёрный список (ЧС) дропперов. При базовом r2r-переводе с пластиковой карты жертвы на пластиковую карту дроппера антифрод-система банка-эмитента может в режиме реального времени определить точные реквизиты получателя и сравнить их с данными из собственных ЧС (по картам, ранее использованным мошенниками для переводов).

При автоматическом анализе содержания диалогов между пользователями на торговой площадке могут быть выявлены паттерны, характеризующие попытку увода жертвы во внешний чат по ключевым словам

Признак № 2. Попадание в группы скомпрометированных виртуальных терминалов. Переводной интерфейс веб-сайта, который используется злоумышленниками для r2r-переводов, привязан к конкретному идентификатору клиента. В процессе ретроспективного анализа всех подтверждённых случаев мошенничества возможно установить перечень этих идентификаторов, привязанных к реальному или виртуальному терминалу (группе устройств), и либо взять все поступающие переводы с этих терминалов на ручной разбор, либо установить временные задержки (длительность определяется экспертно) на обработку приходящих с данного ID запросов на r2r-перевод.

Признак № 3. Соответствие профиля потенциальных жертв. Для группы клиентов, ранее не совершавших r2r-переводы в Интернете (лица пожилого возраста, жители в регионах и др. — профиль составляется на основе анализа подтверждённых случаев мошенничества), устанавливаются триггеры и дополнительные/временные дневные лимиты на совершение операций по коду «r2r-перевод» с пластиковой банковской карты.

* * *

Закончить статью я бы хотел словами обращения представителей МВД к потенциальным жертвам скамеров.

Уважаемые граждане! Будьте предельно внимательны при покупке товаров через сайты интернет-объявлений и популярные торговые площадки. Не разглашайте неизвестным лицам реквизиты своих банковских карт, а также иную контактную информацию. Помните, что добросовестные продавцы или покупатели товаров не будут запрашивать ваши персональные данные или убеждать вас совершать сомнительные операции. По факту совершения в отношении вас попыток мошенничества своевременно информируйте представителей МВД, службу безопасности финансовых организаций и торговых площадок. Будьте здоровы!



Владимир НИКОНОВ
председатель правления
ФСРБИТ



Борис СТОЛПАКОВ
историк криптографии

ГРАНЬ ПОБЕДЫ

ПРОЕКТ ФСРБИТ «КРИПТОГРАФИЧЕСКИЙ ФРОНТ
ВЕЛИКОЙ ОТЕЧЕСТВЕННОЙ ВОЙНЫ» ОТКРЫЛ ЮНЫМ
РОССИЯНАМ МАЛОИЗВЕСТНЫЕ СТРАНИЦЫ ИСТОРИИ

Ещё недавно часть исторических публикаций BIS Journal сопровождалась значками Фонда содействия развитию безопасных информационных технологий (ФСРБИТ) и Фонда президентских грантов. Эти статьи, посвящённые нынешнему юбилею Великой Победы, стали частью большого проекта «Криптографический фронт Великой Отечественной войны», осуществлённого ФСРБИТ при поддержке гранта Президента России в 2018–2019 гг., продолженного в 2020 году и призванного к сохранению народной памяти об одной из малоизвестных страниц войны — о весомом вкладе советских криптографов и радиоразведчиков в общую Победу.

Целевая аудитория была выбрана совершенно особенная. Это школьники средних и старших классов, проявляющие интерес и способности к

математике, физике и информатике. Не секрет, что школьники, увлекающиеся информационными технологиями, в большей степени подвержены влиянию западной культуры, а она формирует весьма одностороннее представление и о научных достижениях, и о технологических факторах, повлиявших на ход Второй мировой войны. В этой связи мероприятия проекта были направлены на повышение осведомлённости школьников о реальных событиях интеллектуального противоборства в годы войны, на их патриотическое и гражданское воспитание.

В рамках проекта были организованы тематические публикации в печатных и электронных СМИ с их продвижением к целевой аудитории через интернет-ресурсы, проводились лекции для школьников. Одновременно с этим готовились наглядные и методические материалы для использования в школах.

В привлечении целевой аудитории к мероприятиям проекта участвовали организаторы региональных и общероссийских олимпиад по направлению «Информационная безопасность», своё содействие и поддержку оказали более 20 образовательных организаций и СМИ.

Всего по тематике проекта в 2018–2020 гг. опубликованы 14 статей в журнале «BIS Journal — Информационная безопасность банков», ставшем главной площадкой проекта среди печатных СМИ. Их содержание наглядно демонстрирует самоотверженный труд и неоценимый вклад в общую Победу советских шифровальной и дешифровальной служб, криптографов из разведки, фронтовой радиоразведки и партизанских соединений.

На основе богатого фактического материала была организована серия мероприятий для молодёжи. Так, в школах Воронежа, Калининграда, Москвы,



Лекция в Президентском физмат лицее № 239, Санкт-Петербург



Лекция в школе №1568, Москва



Квест в галерее Александра Шилова

Санкт-Петербурга и Тамбова проведено 15 лекций, охвативших более 1300 человек. Записи некоторых из этих лекций опубликованы на сайтах школ.

Отобранные для проведения лекций информационные материалы послужили основой для создания наглядных пособий (стендов) «Успехи дешифровальной службы и принятие стратегических решений при обороне Москвы», «Вклад специальной службы в победу на Курской дуге» и «Академик В.А. Котельников и становление засекреченной телефонной связи», а также ещё трёх стендов с фотокопиями архивных шифрдокументов. Оригинал-макеты стендов доступны всем заинтересованным образовательным организациям для использования в военно-патриотической работе, в том числе для создания тематических экспозиций в школах. В сети Интернет размещена видеолекция, содержательно дополняющая эти материалы. К 75-летию Победы на сайте Фонда размещены интернет-версии стендов, адаптированные для отображения на различных платформах.

География реализации проекта в дистанционном формате охватила более 50 субъектов Российской Федерации, аудитория интернет-ресурсов — более 8 тыс. человек. Поскольку созданные в рамках проекта публикации и видеосюжеты размещены в открытом доступе, будем надеяться, что целевая аудитория ещё не раз ими воспользуется. По крайней мере, она демонстрирует такой интерес.

Проект «Криптографический фронт» динамично реализовывался и в нынешнем, юбилейном году. В Московской государственной картинной галерее народного художника СССР А. Шилова для учащихся прошли квест «Шифры Великой Отечественной» и научно-популярная лекция о создании и



Видеозадача про шифрование метеосводок на олимпиаде (май 2020 г.)

принципах работы шифраторов речи, использовавшихся для защиты телефонных и радиоканалов уровня Ставка — Фронт. Школьникам предложили поспорить в скорости и качестве выполнения заданий, основанных на архивных документах. А для победителей организаторы подготовили памятные грамоты. Их ребятам вручил действительный член Академии криптографии Российской Федерации Ю.И. Медведев. Мероприятия были приурочены к награждению московских дипломантов Межрегиональной олимпиады школьников им. И.Я. Верченко и прошли при поддержке компаний «ИнфоТеКС», «Линфо», «Перспективный мониторинг», «Код безопасности», ГК «Астра Linux», «Системы и технологии» и Медиа Группы «Авангард».

В ходе проводившейся Центром педагогического мастерства г. Москвы в мае интернет-олимпиады «Готов к жизни в умном городе» ученикам 2–9 классов предлагалась видеозадача по расшифрованию метеосводок, основанная на материалах военных архивов. Школьники — участники олимпиады проявили активность и в решении, и в разборе этой задачи, а число просмотров её видеоролика приблизилось к 100 тыс.

В дни юбилея Победы был использован и относительно новый формат популяризации знаний в молодёжной среде — интернет-викторины. Так, 7 мая прошёл специальный выпуск «Нашей игры», большинство вопросов которой

были посвящены «Криптографическому фронту». Запись трансляции, а также сам банк вопросов, размещённые в открытом доступе, дополнили копилку методических материалов проекта.

Экспозиция «Криптографический фронт» демонстрировалась в ходе отраслевых конференций «РусКрипто», «РКИ-Форум» и «СТ Сгурт — современные тенденции в криптографии» 2020 года.

Концепция проекта докладывалась на российско-белорусской конференции «Комплексная защита информации» в г. Витебске в мае 2019 года, а итоги реализации получили положительную экспертную оценку Фонда президентских грантов, проводившуюся летом 2020 года.

BIS Journal искренне рад тому, что охваченные проектом юные граждане России и их наставники яснее почувствовали, как каждый успех на незримом криптографическом фронте отзывался победами в реальных сражениях и сохранением жизней бойцов, в том числе жизней дедов и прадедов нынешних школьников.

Достойны благодарной памяти и победы на криптографическом фронте и наши выдающиеся криптографы, и организаторы промышленного производства шифровальной аппаратуры, оказавшейся не по зубам могучему противнику. Честь им и слава!



**Марина
БРОДСКАЯ**
обозреватель
BIS Journal

ВСТУПИТЕЛЬНАЯ КАМПАНИЯ — 2020: КОНКУРС ВЗЛЕТЕЛ

НО ЖЕЛАЮЩИХ УЧИТЬСЯ ИБ ЗА ДЕНЬГИ
МНОГО НЕ НАБРАЛОСЬ

2020 год ознаменовался 366-м днём в календаре, а также пандемией COVID-19, тотальным карантином, удалённой учёбой. Впервые были сдвинуты сроки сдачи ЕГЭ. Также впервые в число получивших право поступать вне конкурса попали все победители региональных этапов предметных олимпиад — заключительный этап Всероссийской олимпиады школьников отменили из-за угрозы заражения. Документы в колледжи и университеты принимали в онлайн-режиме. Чем ещё ознаменовалась вступительная кампания?

СИТУАЦИЯ С ПОСТУПЛЕНИЕМ

Главным вопросом для выпускников школ в конце мая стали сроки проведения ЕГЭ. Назвать точные даты поначалу не могли даже в профильном министерстве. Такая неопределённость, с одной стороны, привнесла нервность в ряды одиннадцатиклассников, с другой — школьники получили дополнительное время на подготовку. И к тому же могли подать заявление в вуз в традиционные даты, но до сдачи и тем более получения результатов ЕГЭ. Опять же ЕГЭ могли сдавать только те школьники, кто планировал учиться дальше. Остальным выдали аттестаты с итоговыми годовыми оценками. Выпускники девятого класса ОГЭ не сдавали и зачислялись в колледжи, если планировали туда перейти, по среднему баллу аттестата.

В итоге приёмная кампания в высших учебных заведениях началась, как обычно, 20 июня, но завершилась позже обычного — 18 августа, а её итоги были подведены в самом конце августа.

Впервые в истории страны кампания прошла в дистанционном режиме. Подать документы в 54 университета в экспериментальном режиме можно было через портал Госуслуг. Остальные вузы принимали документы через собственные онлайн-сервисы. Также документы можно было направить по почте или с доверенным лицом или принести лично. Предполагается, что в ближайшие годы документы будут подаваться через Госуслуги во все вузы страны.

Каждый абитуриент мог подать документы в пять вузов и на три специальности в каждом из них — итого 15 заявлений. Но в итоге заявленные цифры в десятки человек на одно бюджетное место снижались — об этом абитуриентов сразу предупреждали многие приёмные комиссии. Кто-то прислал неполный пакет документов, кто-то не сдал ЕГЭ по профильным предметам, кто-то не набрал требуемый для данного университета минимум или не прислал заявление о согласии на зачисление. В результате конкурс снижался в десятки раз. Вместе с ним падал и проходной балл.

ВНЕ КОНКУРСА

Заключительный этап Всероссийской олимпиады школьников 2019/2020 отменили, поэтому в число получивших право поступать вне конкурса попали все победители её региональных этапов. Более того, победители и призёры сохраняют особые права на поступление в течение четырёх лет.

Ещё одно изменение — увеличение доли мест с 25 до 27 % по сравнению с 2019 г. на целевое обучение за счёт федерального бюджета по направлениям «Компьютерная безопасность»

(10.05.01) и «Информационная безопасность телекоммуникационных систем» (10.05.02) согласно Распоряжению Правительства РФ от 4 марта 2020 г. Учиться за счёт бюджета с обязательным трудоустройством по окончании университета могут граждане, заключившие соответствующий договор с предприятием, куда в будущем пойдут работать. Этой лазейкой часто пользуются обладатели низких баллов или дети чиновников, что порою вызывает негодование общественности. Вопросы совершенствования системы образования обсуждаются в Федеральном собрании РФ, в частности, их поднимала на заседании рабочей группы по выработке предложений по совершенствованию структуры системы образования, повышению эффективности реализации целевого обучения и приёма председателем Комитета СФ по науке, образованию и культуре Лилия Гумерова.

На пресс-конференциях местным и федеральным СМИ ректоры многих университетов, подводя итоги кампании, отмечали увеличение числа абитуриентов и расширение географии их проживания. Одновременно выросло и число абитуриентов, имеющих право на преимущественное зачисление, — это те самые призёры и победители предметных олимпиад из регионов, которые получили статус победителей и дипломантов Всероссийской олимпиады школьников.

ПРО КОНКУРС И БЮДЖЕТНЫЕ МЕСТА

Если верить новостной ленте, то конкурс-2020 на самые популярные специальности побил все рекорды. 80, 90... 111 человек претендовали на одно

бюджетное место в Президентской академии в Санкт-Петербурге. Средний конкурс в СПбГУ — 30 заявлений на место, что на треть больше, чем в прошлом году. В университетах Москвы и регионов конкурс был высоким, однако о побитых рекордах никто не общал... Оценивая ситуацию, можно сказать, что Департамент образования Санкт-Петербурга отлично провёл пиар-кампанию.

Из положительных тенденций вступительной кампании — увеличение числа бюджетных мест, в том числе по интересующему нас направлению 10.0.0 — «Информационная безопасность». В феврале 2020 г. вице-премьер Правительства РФ Татьяна Голикова заявила, что число бюджетных мест, распределяемых между вузами России, увеличится в 2021 году на 18,8 тыс., а в 2024 — на 141,8 тыс. В абсолютных цифрах, приведённых в конце августа «Российской газетой», на 2020/2021 учебный год российским вузам было выделено почти 542 тыс. бюджетных мест. В 2021/2022 учебном году их будет уже более 576 тыс.

Более того, летом Министерство науки и высшего образования РФ выделило вузам дополнительные бюджетные места, в связи с чем во многих университетах был открыт дополнительный приём.

Если в московских университетах бюджетных мест по ИБ прибавило в одном вузе и тут же убавило в другом, то тенденция роста числа бюджетных мест в региональных вузах действительно есть, что не может не радовать. В сентябре дополнительный приём на бюджет был объявлен во многих регионах, например, ещё в сентябре можно было подать документы в Воронежский и Башкирский государственные университеты, а также в Уфимский государственный нефтяной технический университет. Принести документы могли как не прошедшие по конкурсу абитуриенты, так и все желающие. Отрадно, что в БашГУ появились дополнительные бюджетные места и по специальности «безопасность информационных технологий в правоохранительной сфере». В 2020 г. в Башкирии число бюджетных мест в вузах увеличено почти на 1,5 тыс. по

сравнению с прошлым годом, в 2021 г. планируется дальнейшее увеличение на 2 тыс. мест.

Учитывая рост числа победителей и призёров Всероссийской олимпиады школьников, которые поступают вне конкурса и порой занимают все бюджетные места, многие университеты открыли приём на места с обучением за счёт средств вуза. Так, за счёт НИУ ВШЭ добавлены места с расчётом, чтобы для поступающих по результатам ЕГЭ осталось не менее 25 % от количества бюджетных мест.

За счёт вузов могут учиться не только студенты «Вышки» или МИФИ. В университете ИТМО уже в третий раз прошёл набор по конкурсу индивидуальных достижений — ITMO.STARS. Программа позволяет талантливым абитуриентам обучаться за счёт университета. В этом году на конкурс через Личный кабинет абитуриента поступили 184 заполненные по форме заявки, из них на собеседование эксперты университета пригласили 42 человека. Требования к победителю просты: быть выпускником школы этого года, преодолеть минимальный порог баллов ЕГЭ (порядка 60 баллов по каждому предмету) и подтвердить знания и компетенции, для чего необходимо представить свои разработки в любой из сфер: программу или алгоритм, инновационный или бизнес-проект, научно-исследовательскую работу, новый прибор или устройство, социальный проект. По итогам собеседования эксперты и члены приёмной комиссии выбрали 15 человек, которые будут учиться в ИТМО за счёт университета.

ПРО ПЛАТНОЕ ОБУЧЕНИЕ

Об очевидном снижении платёжеспособности населения сегодня говорят не только экономисты. Во многих вузах отметили уменьшение числа желающих поступать на платные отделения и одновременный рост числа заявлений на бюджетные места. Ряд заведений, опираясь на опыт прошлых лет, сократил число платных мест с 30–50 до разумных 10–15. И, как показала вступительная кампания, в начале сентября далеко не все платные места были заполнены — приём заявлений для зачисления был продлён.

А по моему личному расследованию в ряде вузов, например МАИ, объявленные цифры приёма на платное отделение не сходились с числом абитуриентов в приказах о зачислении. Если это не техническая ошибка, то желающих учиться ИБ за деньги много не набралось.

Среди новшеств платного образования — рост числа желающих оплатить обучение из средств материнского капитала. В разделе «Платное образование» на сайтах ряда университетов уже появились инструкции, как это правильно сделать.

Многие вузы предлагают традиционно скидки за обучение на платном отделении для недобравших баллы по конкурсу. Но есть и новшества, например предложение пойти на платное тем, кто проходит по конкурсу на бюджет. Так, СибГУ предлагает до 50 % скидки имеющим высокие баллы абитуриентам, если они поступают на платной основе. «Заплати сегодня, получи скидку, вернём деньги при зачислении на бюджет», «Вы потеряете только на банковском переводе, но это копейки по сравнению с экономией, если будете платить потом по полной программе», — уверяют маркетологи университетов, предлагая скидку от 15 до 25 % тем, кто нервничает и сомневается, хватит ли ему баллов ЕГЭ для прохода на бюджет по конкурсу. Желание пополнить пустующий бюджет университета и воспользоваться ситуацией с одной стороны понятно, но с другой — в условиях угрозы коронавируса такой подход вызывает вопросы этического характера.

Один из самых дорогих вузов — ВШЭ — в этом году ограничил число платных студентов, таких было принято порядка 3,6 тыс. человек, хотя и поднял плату на традиционные для «Вышки» 10 %. Сократили число студентов на коммерческой основе и в МИРЭА.

ПРО ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

Начальные требования к абитуриентам у разных вузов разные. Одним достаточно минимальных баллов ЕГЭ по основным предметам, другие повышают планку до 40 баллов по отдельному предмету, а сильные университеты

Вуз	Спец. по ИБ*	Мест (бюд./пл.)	Заявлений (бюд./пл.)	Квоты на бюджет
ВШЭ	10.03.01 10.05.01	50/20/10 ино 40/75/5 ино	588/393 650/247	10 16
НИЯУ МИФИ	10.03.01 10.05.04 10.05.05	40/30 15/15 10/10	420/72 194/37 нд/2	4 2 1
МФТИ	10.05.01	10/5	310/85	4
МГТУ	10.05.03	28/51	924/нд	6
Калуга	10.05.03 10.05.01	29/10 18/39	191/нд 805/нд	10 6
МАИ	10.05.02 10.03.01	-/20 40/20	/85 1558/346	- 8
РГГУ	10.05.01.65	30/10	нд	3+3
МИИТ	10.03.01 10.05.01	25/35 25/35	742/189 457/79	6 11
МИРЭА	10.05.03 10.05.04 10.05.05 10.05.01 10.05.02 10.03.01	72/108 43/107 42/108 77/108 72/108 62/244	нд нд нд нд нд нд	8+18 5+4 5+4 8+40 8+32 7+6
МГЛУ	10.03.01	22/40	388/233	2+2
Оч.-заоч.	10.03.01	10/15	115/73	1+1
СПбПУ	10.03.01 10.05.01 10.05.03 10.05.04	36/20 41/20 41/20 24/10	591/115 530/77 809/162 487/94	нд нд нд нд
ЛЭТИ	10.03.01	60/25	742/174	2
СПбГУТ	10.03.01 10.05.02	50/88 27/44	нд нд	5 3
ПГУПС	10.05.02	15/35	470/74	2+3
РГГМУ	10.03.01	15/20	275/28	2+5
СФУ	10.05.01 10.05.03 10.03.01	20/12 20/12 25/40		3+5 2+4 6
АлтГТУ	10.03.01	45/6	464/	5+5
АГУ	10.03.01	50/8	367/29	5
ДВФУ	10.03.01 10.05.01	25/10 45/10	/43 /30	1 5+1
ВГТУ	10.05.01 10.05.02 10.05.03	28/10 28/10 28/10	336/нд 217/нд 292/нд	нд нд нд
КБГУ	10.03.01	25/5	нд	6
САФУ	10.03.01	30/13	213/29	2+2
НГТУ	10.03.01 10.05.03	35/70 30/70	1003/700 654/415	4+3 3+3
ЧГУ	10.03.01	25/5	211/21	3+3

* Специальности по ИБ: 10.03.01 — «Информационная безопасность», бакалавриат; 10.05.01 — «Компьютерная безопасность», специалитет; 10.05.02 «Информационная безопасность телекоммуникационных систем», специалитет; 10.05.03 — «Информационная безопасность автоматизированных систем», специалитет; 10.05.04 — «Информационно-аналитические системы безопасности», специалитет; 10.05.05 — «Безопасность информационных технологий в правоохранительной сфере», специалитет

Экзамены по ЕГЭ**	Проходной балл 2020 г.	Проходной балл 2019 г.	Стоимость 2020, тыс. р. (для сравн. 2019 г.)
МФР	253	288	440 (400)
МИР	278	292	440 (400)
МФР	нд/222	296	243,8–273,8
МФР	294/233	289	273,8
МФР	276/225	-/217	273,8
МФР	298/252	288/192	270 (290 иностр. гражд.)
МФР	261/211	269	302,533
МФР	177/нд	187/нд	154,230
МФР	271/164	288	302,533
МФР	нд	-/188	208,55
МИР	248/214	253/201	208,550 (249)
МФР	223/150	225/156	249 (215,2)
МФР	229/147	230/162	227,4
МФР	229/151	259/120	227,4
МИФ	236/140	246/нд	221,250
МИФ	235/142	243/нд	221,250
МИФ	237/139	247/нд	221,250
МФР	237/154	236/нд	221,250
МИФ	241/167	244/нд	221,250
МИФ	246/129	257/нд	221,250
М Иняз Р	262/196	265/180	270 (330)
М Иняз Р	249/160	-/126	160
МФР	190/164	264	191
МФР	176/161	250	191
МИР	246/184	256	191
МИР	257/183	260	191
МИР	244/нд	262	179 (166)
МФР	246/120	252/нд	204
МФР	242/132	240	204
МИР	213/140	198	212,9 (203,8)
МИР	174/146	/148	202
МИР	203/169	230/нд	170,622
МИР	201/186	219/нд	170,622
МИР	224/140	198/148	170,622
МФР	192/142	179/нд	109,5
МФР	173/нд	195/147	114,16
МФР	155/140	195	210
МФР	146/нд	178	210
МФР	нд	216	115,8
МФР	нд	202	115,8
МФР	нд	196	115,8
МФР	149/	188/159	103,1
МИР	195/173	185/133	103,1
МИР	229/140	239/134	136,6
МИР	236/167	227/134	136,6
МИР	171/164	163/нд	130

** Экзамены по ЕГЭ:

М — математика, И — информатика и компьютерные технологии,

Р — русский язык, Ф — физика, Иняз — иностранный язык

заранее отсекают «неудачников», желая видеть у себя как минимум уверенных хорошистов. Во многих регионах студентами часто становятся те, кого даже на порог не пустят в столичных вузах.

ИБ В МОСКВЕ

В ВШЭ требования к минимуму по ЕГЭ — 185 (60+60+65). Несмотря на конкурс более 11 человек на место, минимальный проходной балл на бюджет по направлению 10.03.01 («Информационная безопасность») составил 253, на 10.05.01 («Компьютерная безопасность») — 278. По «зелёной волне» (гарантированное зачисление при подаче всех документов) на бюджет могли пройти обладатели 270 и 278 баллов соответственно. По итогам первого курса вакансий на бюджете 2-го курса — 3 места, на платном отделении — 3 места.

В МИФИ можно было идти, имея от 183 или 191 балла по ЕГЭ в зависимости от выбранного направления ИБ — бакалавриат или специалитет. По направлению 10.03.01 («Информационная безопасность») все бюджетные места заняли призёры олимпиад и целевой приём (270 баллов), на специальности 10.05.04 («Информационно-аналитические системы безопасности») и 10.05.05 («Безопасность информационных технологий в правоохранительной сфере») прошли обладатели 294 и 276 баллов. Для сравнения, на платном отделении можно учиться, имея 222 балла и от 243 до 273 тыс. руб. в год.

Схожая ситуация в МФТИ. На 10 бюджетных мест, из которых 6 — это квоты и целевой приём, было подано 584 заявления. В конкурсе участвовали 310 заявлений, проходной балл составил 298. На платном отделении конкурс был 17 человек на место, проходной балл составил 252. Стоимость обучения — 270 тыс. руб. в год. Стоит отметить, что в МФТИ проходной балл по сравнению с 2019 г. вырос, а стоимость обучения упала.

В МГТУ им. Н. Баумана минимальные требования намного ниже конкурентов — всего 125 баллов по ЕГЭ. Видимо, поэтому на специальность 10.05.03 захотели поступить 924 человека, а на 10.05.01 — 805. В конкурсе на бюджетные места из них приняли участие 865 и 751 человек. Минимальный

проходной балл за последние годы снижается, в этом году на разные направления ИБ смогли поступить абитуриенты с 261 и 271 баллами по ЕГЭ. А в Калужском филиале, где на 19 бюджетных мест по конкурсу претендовали 191 человек, проходной балл составил всего 177. Правда, и стоимость обучения на платном отделении в Калуге ниже, чем в Москве, — всего 154 тыс. руб., в то время как в столице цена учебного года почти вдвое выше.

В МАИ на 40 бюджетных мест по специальности 10.03.01, из которых 8 — это квоты и целевой набор, было подано 1552 заявления. Несмотря на такой спрос на специальность, минимальный проходной балл составил 248, что на 5 ниже, чем в 2019 г. На 20 платных мест по направлению поступили всего 11 человек. А по направлению 10.05.02 («Информационная безопасность телекоммуникационных систем»), где, согласно контрольным цифрам приёма, открыты 20 платных мест и были поданы 85 заявлений, приказа о зачислении на сайте при подготовке обзора не обнаружилось. Стоимость года учёбы — от 208 тыс. руб.

Значительно изменились по сравнению с предыдущими годами контрольные цифры приёма в МИРЭА, где представлен наиболее полный список специальностей по направлению 10.00.00 «Информационная безопасность». Во-первых, выросло число бюджетных мест, даже с учётом квот. А во-вторых, по ряду специальностей на 10% сократилось число мест на платном отделении. Сколько из них реально оказались занятыми, сайт университета умалчивает. Проходные баллы из года в год остаются на уровне 235–245 в зависимости от специализации.

С каждым годом всё большим спросом пользуется направление ИБ в Московском государственном лингвистическом университете. Несколько лет назад, когда обзоры вступительных кампаний в нашем журнале только зарождались, университет принимал ограниченное число лиц на платное отделение. В этом году на очное и очно-заочное отделения по специальности 10.03.01 принимались абитуриенты как на бюджетной, так и на платной

основе. На 22 бюджетных места очного отделения претендовали 388 человек (в прошлом году на 19 мест было 414 желающих), а на 10 мест очно-заочного отделения подали заявления 115 человек. Проходные баллы на бюджет составили 262 и 249. Вместе с тем выросли минимальные баллы при зачислении на платное отделение. Если в 2019 г. на очно-заочное обучение были зачислены абитуриенты с 126 баллами, то в этом году минимум составил 160. При этом снизилась стоимость обучения — с 330 тыс. руб. до 270 тыс. руб. Для тех, кто дополнительно хочет учить китайский язык, стоимость обучения на очном отделении составит 305 тыс. руб.

ИБ В РЕГИОНАХ

Если рассматривать региональные вузы, то стоит отметить рост числа бюджетных мест по направлениям ИБ в 1,5–2 раза, а в ряде случаев, как, например, СПбГУТ, и в 3 раза — в этом году открыты 50 бюджетных мест, в 2019 г. их было всего 17. В Сибирском федеральном университете оценили спрос на специальности и увеличили не только число мест на бюджете, но и, порой кратно, число платных мест. Такая же ситуация в Дальневосточном, Северном Арктическом госуниверситетах и многих других. Например, максимальное число заявлений на бюджет в Астраханском госуниверситете было подано на специальность «информационная безопасность», проходной балл составил 203. ИБ вошла в тройку самых востребованных специальностей у абитуриентов Череповецкого государственного университета. Минимальный проходной балл второго этапа составил 171, максимальный первого — 245. А в Новосибирском государственном технологическом университете направление ИБ входит в число пяти популярных уже 10 лет.

Конечно, минимальный проходной балл в региональных вузах порой ниже порога отсека ВШЭ или МИФИ, однако радует сам факт — спрос на направление замечен, университеты и государство начали вкладывать средства в подготовку специалистов по информационной безопасности на местах.



ШКОЛЫ И УНИВЕРСИТЕТЫ ПОД ПРИЦЕЛОМ ХАКЕРОВ

НОВЫЕ РЕАЛИИ ОНЛАЙН-ОБРАЗОВАНИЯ ЗА РУБЕЖОМ¹

Злоумышленник перехватил управление в Zoom и показал непристойности во время урока — вот типичная новость этого года в западных СМИ.

КИБЕРАТАКИ БЫЛИ, НО ТЕПЕРЬ СТАЛИ ПРОБЛЕМОЙ

Не стоит думать, что инциденты стали открытием для учебных заведений с введением карантина. Хакерские атаки начались задолго до пандемии коронавируса и массового перехода на онлайн-обучение. Год назад школьный округ города Сан-Бернардино, штат Калифорния, стал целью атак вымогателей. Университет штата Юта и

Университет Калифорнии заплатили выкупы в размере \$457 тыс. и \$114 тыс. соответственно, чтобы получить доступ к своим системам.

Эксперты отмечают, что учреждения среднего образования (уровня ниже колледжа) являются наиболее уязвимыми для взлома. Кибератаки на школы обходятся преступникам дешево, но для их предотвращения или восстановления самим школам могут потребоваться миллионы долларов. У школьных округов просто нет ресурсов, как финансовых, так и кадровых, чтобы справиться с такими атаками.

Если кибератаки на компании и корпорации приносят хакерам прибыль, то целью нападений на образовательные и академические учреждения становятся исследовательские программы

или лёгкий грабёж. Некоторые университеты готовы заплатить выкуп за восстановление данных студентов или финансовых транзакций, только бы не оказаться втянутыми в судебные тяжбы со стороны пострадавших. Да и восстановление университетской компьютерной системы может занять несколько месяцев, что парализует не только дистанционное обучение, но и весь образовательный процесс в целом.

НЕХВАТКА ФИНАНСИРОВАНИЯ И КАДРОВ

Среди последних примеров — августовские атаки на школьный округ Риальто и Колледж Пустыни в Калифорнии. Дистанционные программы остановились, заражённые компьютеры

¹ По материалам зарубежных СМИ



и гаджеты были изъяты для проверки и замены. В Нью-Йорке злоумышленники перехватили управление во время пресс-конференции в Zoom мэра города и Объединённой федерации учителей. Во Флориде в школе Майами-Дейд после многодневных кибератак так и не смогли начать дистанционное обучение. По словам официальных лиц, многие атаки были совершены из-за пределов страны.

Согласно данным отчёта RiskBased Security QuickView за 2019 г., на сектор образования пришлось 7,2 % от общего числа обнаруженных кибератак. Это не много по сравнению со сферами здравоохранения (13%) или бизнеса (69%). Однако теперь всплеск атак отмечается именно в связи с массовым переходом на онлайн-обучение. Во многом успехи хакеров объясняются сокращением финансирования ИТ-сектора в университетах и колледжах (всего 4,4 % бюджетов), что создало серьёзные препятствия для модернизации классов и полноценного выстраивания дистанционного обучения.

По данным EDUCAUSE, на 1 тыс. штатных сотрудников в университетском кампусе приходится всего 0,26 штатной должности в отделе ИТ, включая ИБ. В результате университеты сейчас имеют большие проблемы при

построении цифрового доверия, дистанционного образования, управления процессом обучением и в социальных сетях.

ПОЛОЖИТЕЛЬНЫЕ ПРИМЕРЫ

Примером правильного подхода к вопросам кибербезопасности называют школьный округ долины Джурупа в Калифорнии. Программа ИБ работает тут шесть лет. Команда безопасников округа установила несколько уровней защиты (фильтры, межсетевые экраны) и ввела двухфакторную аутентификацию. Ответственность за кибербезопасность стала стандартной частью страхования ответственности школ ещё задолго до того, как получила массовое распространение.

С началом этого учебного года школьный округ Лагуна-Бич ввёл дополнительные уровни защиты своей компьютерной системы и цифровых устройств. При помощи Департамента образования округа Ориндж тут провели обширную проверку безопасности, в первую очередь — тестирование систем в реальном времени на выявление уязвимостей.

Власти Нью-Йорка тоже внесли свою лепту. С началом учебного года в местных СМИ проводится целевая информационная кампания: до населения настойчиво доводятся простые правила,

которые помогут защитить конфиденциальность ребёнка и обеспечить его безопасность. Например, рекомендации выключать веб-камеры и микрофоны компьютеров после онлайн-уроков, скрывать личную информацию ребёнка, не оставлять перед веб-камерой счета или выписки из банка, не использовать для дистанционного обучения устройство, с которого есть выход в банк, и т.д. и т.п.

Также предлагается остерегаться фишинговых сайтов и рекламных баннеров онлайн-магазинов. Из 35 тыс. новых доменов, зарегистрированных за последние три месяца, более 500 оказались злонамеренными, ещё 3400 отнесены к подозрительным.

ОПЫТ АРКАНЗАСА И ГОСПОМОЩЬ

В сельской школе Джексон штата Арканзас родители и учителя местного школьного округа прошли тренинг по онлайн-обучению. По данным Ресурсного центра государственных школ, округ входит в число 170 (из 263) округов штата Арканзас, школы которых используют систему управления дистанционным обучением, разработанную Lincoln Learning Solutions Inc. из Филадельфии. Администраторы системы объяснили собравшимся, как получить доступ к

цифровой учебной программе, как отправлять задания и как использовать службу видео-конференц-связи Zoom для общения с учителями и одноклассниками.

Этой осенью всего 10 % из 950 школьников этого округа учатся дома, в других округах штата эта цифра значительно выше. Школьные округа используют различные образовательные платформы для загрузки учителями видео, заданий и контента — Google Classroom, Schoology и Canvas.

Поставщики ПО предлагают готовые учебные программы, дополняющие или полностью заменяющие очные занятия. Большинство школ используют микс из учебных программ, разработанных их собственными учителями, и базовых цифровых контентов, которые легко объединяются с помощью платформы управления обучением.

Решение внедрить в штате систему дистанционного образования было принято Управлением начального и среднего образования Арканзаса, однако выбор платформ и решений для онлайн-обучения оставили на усмотрение округов. Многие школы уже несколько лет используют платформы для удалённого обучения, но в условиях пандемии пришлось внедрять новые системы или в авральном порядке приспособлять уже имеющиеся.

Департамент образования штата Арканзас в сотрудничестве с Lincoln Learning — некоммерческим центром ресурсов государственных школ — предлагает местным округам цифровой контент и систему управления обучением. Цифровой контент и ПО бесплатны — за всё платит департамент, выделивший \$2,4 млн по «Закону о помощи, поддержке и экономической безопасности в связи с коронавирусом (CARES)». До \$310 тыс. из этой суммы предназначено для помощи школам при внедрении ПО, а \$1,9 млн — для оплаты услуг Lincoln Learning, в том числе за систему управления обучением Buzz и цифровую учебную программу, которая включает основные и факультативные занятия.

ОБУЧЕНИЕ ВИРТУАЛЬНОЕ — ПОМОЩЬ РЕАЛЬНАЯ

Пример Арканзаса не единственный. Департаменты образования многих территорий США купили у компаний

виртуальные решения и бесплатно предлагают платформы и контент государственным школам. Особое внимание уделяется сельским районам с ограниченными ресурсами. Помощь варьируется от денег на оплату услуг до помощи учителям и администраторам в обучении и быстром создании контента для обучения на дому.

Платформ много. Кроме упомянутой Lincoln Learning, предлагаются разработки систем PowerSchool и Schoology, LMS Seesaw и пр. Например, в штате Техас подписано соглашение о партнёрстве с компанией PowerSchool, занимающейся онлайн-обучением, и предлагается платформа управления обучением Schoology — бесплатная в течение двух лет для всех школ штата.

БЕСПЛАТНЫЙ СЫР

Но за бесплатный сыр когда-то придётся заплатить, а сделает это государство или штат — пока неизвестно. Школьные округа в Арканзасе обеспечены инвестициями, которые им, возможно, придётся сделать в будущем для продолжения использования полученного бесплатно ПО. Представители Департамента образования Арканзаса и Ресурсного центра государственных школ заявили, что ещё не решили, будут ли они предлагать платформе бесплатно после весеннего семестра. Неизвестна и стоимость поддержки системы, если школы решат продолжить использовать её самостоятельно.

Поставщики ПО для дистанционного образования взимают плату со школьных округов, используя ряд показателей, например активность использования продукта и число пользователей. Поэтому онлайн-платформа может стоить округу от нескольких тысяч до более чем \$1 млн. Согласно отчёту консалтинговой и исследовательской компании 360iResearch, глобальный рынок систем управления обучением вырастет с \$9,5 млрд в 2019 году до \$29,9 млрд к 2025 г. Рост во многом связан с высокими темпами внедрения продуктов из-за пандемии.

В округе Граветт в северо-западном Арканзасе около 24 % из 1850 школьников этой осенью решили остаться дома. И директора школ хотят извлечь максимум пользы из ПО от Lincoln Learning.

А вот округ Литл-Рок, где 50 % из 25 тыс. учащихся выбрали дистанционное образование, отказался от Lincoln Learning из-за опасений по поводу будущих расходов.

Согласно обзору Департамента образования Арканзаса, 14 округов штата используют Schoology, в том числе школьный округ Форт-Смит, который подписал годовой контракт на \$52 825 с PowerSchool на использование платформы для 7750 учеников в шести средних и трёх начальных школах. Округ Форт-Смит тратит \$1,9 млн на цифровую учебную программу Pearson Connexus от британской Pearson Education. Школьный округ Фаунтин-Лейк заплатил в этом году \$2750 за использование Seesaw LMS в своей начальной школе, где учатся 1400 учеников. Учащиеся средних и старших классов используют бесплатный Google Classroom. Школьный округ уже потратил \$168 тыс. на финансирование CARES и почти \$300 тыс. на подготовку школ — закупку средств дезинфекции и цифрового контента от MyON, платформы, предлагающей ученикам цифровые книги.

По данным газеты Democrat-Gazette, округ Литл-Рок заплатил PowerSchool более \$165 тыс. за использование системы управления обучением Schoology для дистанционного обучения детей с детского сада до 12-го класса в 2020/2021 учебном году. Это первый платёж в рамках трёхлетнего договора. Округ также заплатил компании Seesaw Learning Inc. более \$20 тыс. за использование системы LMS Seesaw в дошкольных учреждениях в течение двух лет. Для покрытия расходов в этом учебном году округ использовал финансирование CARES, но как будет оплачиваться платформа в будущем — не очень понятно.

Что касается бесплатной платформы Google Classroom, то она удобна, полезна и широко используется. Однако школьные чиновники заявили, что у неё есть ограничения. В качестве альтернативы предлагается совсем не дешёвая Schoology, позволяющая учителям создавать классы и архивировать их из года в год, а школьным администраторам обмениваться информационными ресурсами со всем округом.

ЭФФЕКТИВНО ЛИ ОНЛАЙН-ОБУЧЕНИЕ?

Исследования эффективности онлайн-обучения проводились во многих штатах. Эксперты считают, что иногда виртуальные классы полезны, но в целом очное обучение всё-таки лучше. Хотя факторов успеха множество: квалификация учителей, качество образовательной платформы, отношение к онлайн-программе районной администрации, выраженное в финансировании... Если, как говорится, все эти звёзды сходятся, что случается нередко, то всё складывается отлично. По результатам тестирования учитель может увидеть проблемы у конкретного ученика и провести с ним дополнительные онлайн-консультации и занятия. Но, если оценки промежуточного обучения нет, возникают проблемы.

По мнению Пола Ревия, профессора Высшей школы образования Гарвардского университета, онлайн-образование имеет «огромный потенциал», но качественную онлайн-программу невозможно создать в одночасье. Для этого нужно время и активная совместная работа школ, составителей учебных программ и разработчиков образовательных платформ. Необходимо также и усилие учителей в овладении технологиями виртуального класса, чтобы «лошадь слушалась хозяина», а не наоборот.

Опрос исследовательской компании в области образования Upbeat показал, что только 60% учеников регулярно участвовали в онлайн-занятиях во время карантина. В районах с высоким уровнем бедности онлайн-классы посещают всего 50% учеников. А уверенность самих учителей в успехе урока упала с 96% при очной работе до 73% в режиме онлайн. Многие учителя уходят из профессии, что создаёт сложности в сельских районах. Так, руководители округа Марвелл-Элейн (Арканзас) серьёзно обеспокоены потерей преподавателей.

ДВОЙНОЙ УДАР ПО УНИВЕРСИТЕТАМ

Университет Редлендса (Калифорния) усиливает меры кибербезопасности с момента начала дистанционного обучения весной 2020 г. Департамент ИБ

получил внутренний грант для обучения дополнительных стажёров и был реорганизован, что позволило большему числу сотрудников сосредоточиться исключительно на сетевой безопасности.

Но гранты дают не везде. Что советуют эксперты учреждениям, которые недофинансированы или недоукомплектованы персоналом? Все как один утверждают, что важнейший шаг — базовое обучение пользователей. Именно конечный пользователь представляет самую большую угрозу безопасности.

Руководители служб безопасности университетов считают, что в первую очередь необходимо обучить студентов и преподавателей защите данных. Но принципы ИБ часто противоречат академическим традициям свободного обмена информацией. Например, при оценке исследований и связанных с ними практик предполагается открытый доступ к информации, что полностью противоречит политике информационной безопасности. Решением проблемы становится выбор правильной платформы для обмена сообщениями и обучение студентов и преподавателей методам обеспечения ИБ, принципам работы хакеров и типам кибератак.

Эксперты также отмечают, что университеты, участвующие в исследованиях, связанных с Covid-19, подвергаются особому риску. Даже если хакеров не интересуют научные данные и интеллектуальная собственность, они стремятся получить доступ к огромным массивам конфиденциальной личной информации, хранящейся в этих университетах. Майкл Дафф, главный специалист по ИБ Стэнфордского университета, отмечает рост числа фишинговых атак с начала пандемии, и большинство схем имеют финансовую мотивацию.

А системы Университета Ньюкасла (Великобритания) пострадали из-за двойного воздействия — коронавируса и кибератаки. С одной стороны, на них давили новые санитарные нормы, с другой — хакеры. В конце августа киберпреступники взломали компьютерную сеть университета, украли данные и зашифровали исходники с помощью вредоноса DoppelPaymer. Университет

не смог распределить студентов первого курса по общежитиям в автоматическом режиме, в результате сотрудники вручную регистрировали более 1000 студентов-медиков. Число таких регистраций вырастет, поскольку все учащиеся должны получить доступ к студенческим кредитам.

Хакеры выложили несколько украденных документов из базы данных университета, угрожая массовой утечкой личных данных студентов. Студенты стали возмущаться, что университет не информировал их об инциденте и не сделал публичного заявления о попытке выкупа. На момент подготовки обзора сотрудники университета вели работы по восстановлению системы, пытаясь установить, какие из её 1500 серверов заражены, и проводили переговоры с правоохранительными органами. По данным Sky News, ущерб от взлома систем для сотрудников и студентов может быть значительным, поскольку хакеры получили доступ к паролям, хранившимся в виде простого текста. Если будет установлено, что университет небрежно защищал личную информацию, ему грозит значительный штраф в соответствии с Общими правилами защиты данных.

Справедливости ради стоит заметить, что Управление комиссара по информации Великобритании исторически не решается назначать штрафы за нарушения безопасности в высших учебных заведениях. Скорее всего, не решится и в этот раз.

ЧТО ДЕЛАТЬ?

Поскольку высшая школа вступает в беспрецедентный учебный год, западные эксперты тотально заняты выявлением общих проблем в кибербезопасности онлайн-обучения, их причин и способов устранения. Предлагаем познакомиться с советами по снижению основных рисков в онлайн, гибридном и дистанционном обучении, которыми делится сетевое издание EdTech: Focus on higher education.

1. Построение цифрового доверия. Учитывая, что высшее образование, возможно, никогда не вернётся к традиционной форме, важным моментом является построение цифрового доверия. Способность организации



защищать цифровую информацию имеет решающее значение в новом учебном году, поскольку основное взаимодействие будет осуществляться в сети.

Поставщики платформ для онлайн-обучения должны обеспечить безопасность и конфиденциальность своих приложений и методов взаимодействия с пользователями: необходимо понять, кто и как будет работать с ПО, какие данные будут вносить, как будут ими пользоваться и распространять. Университеты должны отдавать приоритет контрактам с нулевым доверием, предоставляя доступ только доверенным сотрудникам кампуса и студентам. Важно знать, кто, как и с какой целью собирает данные и где они будут их использовать.

2. Управление доступом. Системы дистанционного обучения должны быть готовы решать вопросы кибербезопасности. Ключевым моментом тут является управление доступом. Поскольку многие студенты получают доступ к системам электронного обучения из разных мест, университетам нужны решения, которые могут оценивать как текущие, так и старые запросы доступа,

отклонять или утверждать вход в систему, автоматизировать отчёты об инцидентах и разрывать соединения.

3. Системы управления обучением изначально должны обеспечивать безопасность и конфиденциальность данных. Часто проблема кроется в обеспечении безопасности надстроек, обеспечивающих совместимость средств обучения, в безопасных переходах по ссылкам, которые дают преподаватели. Также стоит рассмотреть инструменты оценки уязвимости, которые могут выявить потенциальные проблемы системы до того, как она будет массово применяться в процессе обучения.

4. Защита социальных сетей. Всё больше преподавателей обращаются к социальным сетям, чтобы привлечь студентов во время онлайн-обучения. Это влечёт за собой риски кибербезопасности, поскольку открывает двери вирусам и вредоносным программам. Основные меры безопасности — последние обновления и резервные копии важных данных — могут значительно снизить большинство рисков. Необходимо регулярно проводить

обучение сотрудников и студентов. Простейшие меры значительно снизят потенциальный риск заражения.

5. Защита сервисов сторонних поставщиков. Речь о сторонних сервисах, обрабатывающих данные для университетов, и растущем количестве устройств промышленного Интернета вещей в кампусе.

Тут требуется как первоначальная оценка сети, так и развёртывание новой инфраструктуры, способной поддерживать подключение к Интернету вещей в любом масштабе. Важно иметь возможность выявлять приложения и сервисы, которые содержат потенциальные точки взлома, использовать облачные технологии, работающие с подключением разнообразных устройств.

6. Кибербезопасность онлайн-классов университетов и колледжей становится важной задачей для ИТ- и ИБ-отделов университетов. Тут в первую очередь необходимо восполнить кадровый голод и уделить максимум внимания вопросам кибербезопасности, описанным выше. И тогда дистанционное обучение принесёт желаемые результаты.



Дмитрий ЛАРИН
кандидат технических наук,
АО «Лаборатория СКАТ»

БОЛЬШАЯ ТРОЙКА: ТЕГЕРАН — ЯЛТА — ПОТСДАМ

ОРГАНИЗАЦИЯ ШИФРОВАННОЙ СВЯЗИ ВО ВРЕМЯ ВСТРЕЧ ЛИДЕРОВ СОЮЗНЫХ ГОСУДАРСТВ В 1943–1945

ТЕГЕРАН-43

Тегеранская конференция проходила с 28 ноября по 1 декабря 1943 года, в ней участвовали Иосиф Виссарионович Сталин, Франклин Рузвельт и Уинстон Черчилль. Встреча стала важным этапом в развитии международных и межсоюзнических отношений, на ней был рассмотрен и решён ряд вопросов войны и послевоенного устройства мира.

Перед специалистами отдела правительственной связи (ОПС) НКВД СССР была поставлена крайне сложная задача. Шла война, И. В. Сталин был не только лидером государства, но и Верховным главнокомандующим Вооружёнными силами СССР, и было необходимо обеспечивать его правительственной связью всюду, где бы он ни находился.

Основным способом правительственной связи в то время была голосовая шифрованная высокочастотная (ВЧ) связь, именно её и предстояло организовать на территории Ирана нашим связистам.

Оперативная группа под руководством И. Я. Воробьёва и П. Н. Воронина выехала в Тегеран за месяц до начала конференции. По прибытии сотрудникам ОПС стало понятно, что им предстоит преодолеть серьёзные проблемы. Во-первых, до войны проводной связи с Тегераном у СССР не было. Во-вторых, из Тегерана

требовалось организовать связь не только с Москвой, но и со всеми фронтами и армиями.

В ходе работ были использованы последние достижения как в техническом отношении, так и в области организации правительственной связи. Для шифрования голосовой связи был использован шифратор новейшей конструкции «Соболь II», разработанный под руководством выдающегося учёного В. А. Котельникова. Для шифрования текстов использовались шифрмашинки с наложением гаммы и роторные шифраторы.

Советская делегация должна была разместиться в Тегеране в здании советского посольства, поэтому место развёртывания станции ВЧ-связи было очевидным. Кроме того, специалисты ОПС организовали передачу информации из иранского города Сари сразу по двум направлениям — на Баку и на Ташкент. Таким образом, удалось обеспечить и делегацию, и прежде всего И. В. Сталина устойчивой правительственной связью на весь период работы конференции.

Следует отметить, что в Тегеране впервые с начала ВОВ засекреченная телефонная связь в звене Ставка — фронт — армия была организована с использованием участков постоянных воздушных линий, арендованных у иностранного государства. Этот опыт оказался очень полезным и использовался

в дальнейшем при проведении следующих встреч глав союзных государств в Ялте и Потсдаме.

ЯЛТА-45

Очередной встречей лидеров Большой тройки стала Ялтинская конференция, проходившая в Крыму с 4 по 11 февраля 1945 г. Помимо глав трёх союзных держав — Сталина, Рузвельта и Черчилля — в конференции принимали участие министры иностранных дел, начальники высших штабов и другие представители органов госуправления.

Серьёзным успехом советской разведки накануне конференции стало получение копии шифрованной телеграммы Черчилля Рузвельту. В ней английский премьер предлагал американскому президенту соображения, как совместными усилиями обыграть Сталина в Крыму.

В ходе конференции советским специалистам необходимо было обеспечить Верховному главнокомандующему не только связь со всеми действующими фронтами и тыловыми районами, но и внутреннюю засекреченную связь с членами нашей делегации. Связистам была поставлена следующая задача: необходимо обеспечить два устойчивых канала связи с Москвой и наличие не менее трёх-четырёх каналов связи с основными объектами в Крыму (Сарабуз, Саки, Севастополь, Ялта), а также внутреннюю защищённую телефонную



Рисунок 1. Встреча лидеров «большой тройки» в Тегеране

связь основного объекта (Ливадийского дворца) в количестве 335 абонентских точек. Для организации правительственной связи непосредственно на объектах Крымского полуострова с Москвой, а также между ними туда в течение 8–22 января прибыли 11 отдельных рот войск правительственной связи (ВПС).

Основным средством шифрования речевой связи по-прежнему был «Соболь II», применялись и другие системы шифрования речевых сообщений. Для шифрования текстовых сообщений использовались шифраторы, упомянутые выше.

Ливадийский дворец, где происходили основные события конференции, был главным узлом связи. Он получил кодовое наименование «Долина». Работы по организации связи там начались ещё до прибытия в Ялту линейных подразделений ВПС. Силами связистов местного погранотряда уже в первых числах января была организована связь «Долины» с Симферополем, а через него и с Москвой, а также обеспечена местная связь первым трём абонентам, заранее прибывшим на объект.

С прибытием 8 января 942-й роты ВПС началось окончательное оборудование узла связи и прокладка абонентских телефонных линий.

Вот что об этом пишут российские историки: «На объекте «Долина», а также на близлежащих объектах «Восточный» и «Западный», в течение двух дней от Ливадии до Севастополя был проложен американский кабель типа «гуппер» для нужд делегации США».

Американскую делегацию поместили в бывший царский дворец в Ливадии, где проходили основные переговоры. Это было связано с тем, что президент США Ф. Д. Рузвельт уже не мог передвигаться самостоятельно.

Английскую делегацию разместили в 20 минутах езды — в Воронцовском дворце в Алушке. Советская делегация расположилась в Юсуповском дворце в Кореизе. Во всех дворцах были организованы узлы связи, позволявшие связаться с любым участником конференции, кому был предоставлен телефонный номер. Для обеспечения бесперебойной работы ко всем станциям в дополнение к американским и

английским специалистам были прикреплены сотрудники НКВД, знавшие английский язык.

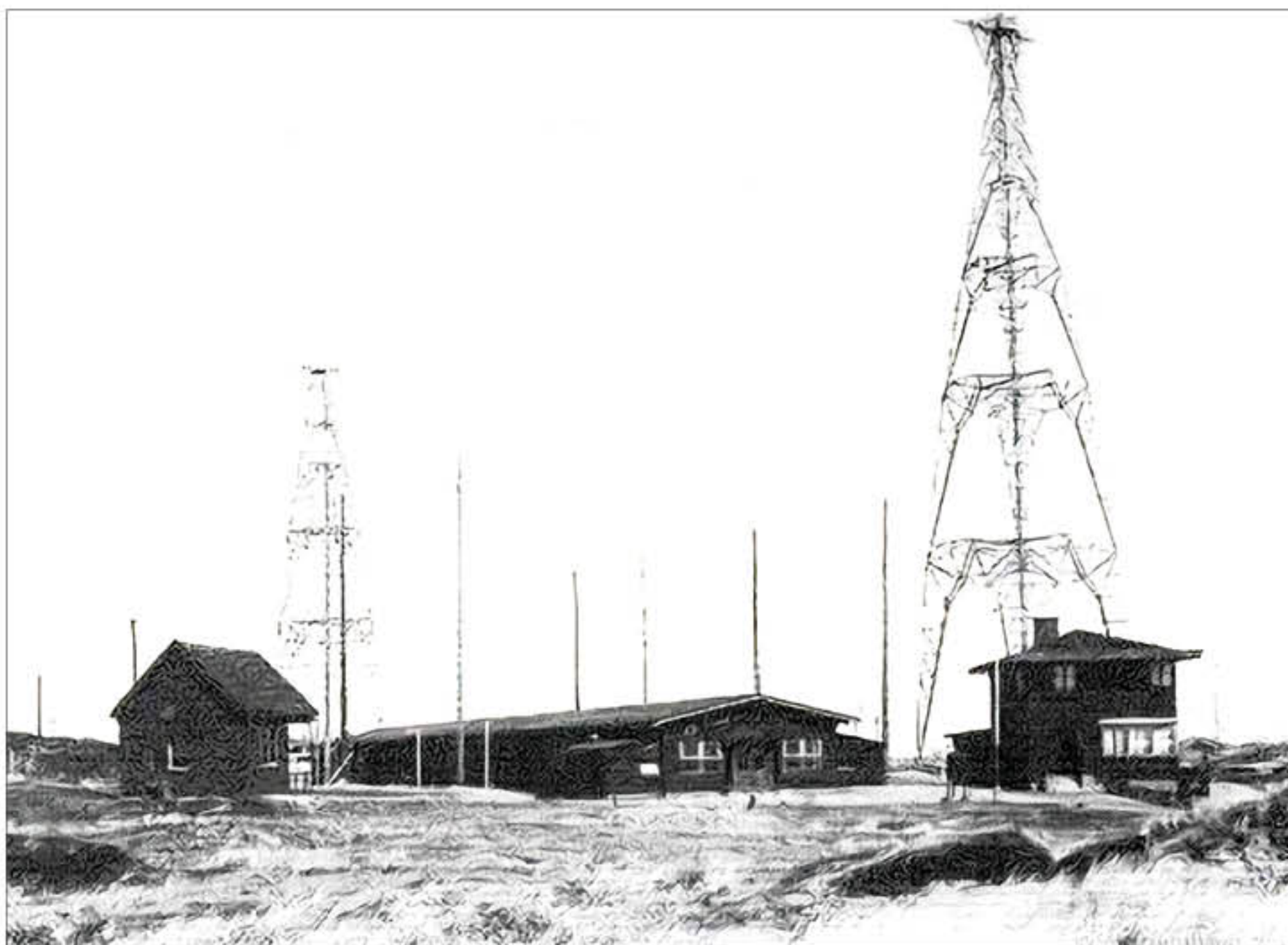
При этом английская и американская резиденции были оснащены системами подслушивания. Вот что об этом пишет сын Л. П. Берии Серго Лаврентьевич, непосредственно принимавший участие в установке подслушивающих устройств: «Как и в Тегеране, в Ялте оборудовали подслушивающей аппаратурой все помещения, которые занимали участники конференции, но этим дело не ограничивалось. Новая аппаратура позволяла нам вести постоянную запись разговоров не только в зданиях, выделенных для американской и английской делегаций, но и, скажем, в парке с помощью направленных микрофонов. Если интересующий нас объект находился на расстоянии 50–100 м, проблем здесь не возникало».

Как отмечается в некоторых источниках: «Американцы, похоже, вообще не принимали никаких мер предосторожности». Однако это не так. В Ялте шла настоящая «война прослушек», американские и английские сотрудники спецслужб не только проводили



Рисунок 2 (вверху). В. Онезгорге

Рисунок 3 (справа). Станция перехвата на побережье Нидерландов, с помощью которой перехватывались переговоры на линии связи Вашингтон — Лондон



мероприятия по выявлению советской аппаратуры (далеко не всегда успешные), но и пытались установить свою прослушивающую аппаратуру практически везде, куда они имели доступ. Наши чекисты эффективно выявляли такие жучки. При этом никаких официальных заявлений не делалось, и мы, и союзники предпочитали не ссориться, понимая, что разведка есть разведка и каждая сторона хочет иметь информационное преимущество.

При организации работ по оборудованию главного узла связи в Ливадийском дворце особое внимание уделялось их качеству. Так, наиболее значимые кабельные линии на объектах «Восточный» и «Западный» подвешивались по столбам на колышках каждый отдельно, а кабельный шлейф на 16 цепей от резервного столба до ВЧ-станции был подвешен на роликах. Более того, на всех важных направлениях узла прокладывались по 1–2 резервных линии, которые по первому требованию включались в работу. В результате хорошей работы советских связистов необходимости в ремонтных и профилактических работах практически не возникало, за исключением отдельных случаев, связанных с гололёдом и штормом, который трижды прошёл по южному побережью Крыма с 24 января по 7 февраля. В частности, был длительным и интенсивным

гололёд на участке Ленинск — Керчь 1–2 февраля 1945 года. Это метеорологическое явление привело к массовым обрывам проводов и разрушениям столбов, на которых они крепились. В результате этого перерыв связи по данной цепи составил 23 часа 45 минут. В ходе повреждения связь с Москвой осуществлялась через Мелитополь и Херсон.

SIGSALY

Интересно отметить, что американцы для обеспечения секретных переговоров своей и английской делегаций (в первую очередь Рузвельта и Черчилля) разместили в Севастополе уникальный аппарат шифрования речевой связи гарантированной стойкости SIGSALY, использовавший оцифровку речевого сигнала. Расскажем о нём подробнее.

Необходимость в срочной разработке и изготовлении аппаратуры такого класса возникла уже в начале Второй мировой войны в связи с успехами немецких специалистов во главе с доктором В. Онезгорге в практическом дешифровании межконтинентальных телефонных переговоров высших должностных лиц США и Великобритании, которые проводились с использованием аналогового шифратора типа «А-3» с динамическими частотными перестановками (1941 г.). Немецкие специалисты перехватывали и дешифровали

десятки, если не сотни телефонных разговоров, зашифрованных системой «А-3», поскольку такая техника была первоначально разработана немецкой фирмой Siemens в первой половине 1930-х годов.

За годы войны была постепенно создана правительственная система закрытой радиотелефонной связи США на основе вокодерных станций SIGSALY (известных также под названиями X-ray, Project X, The Green Hornet). Терминалы этой системы связи начиная с 1943 г. располагались в Вашингтоне, Лондоне, Алжире и Австралии, позднее в Париже, Северной Африке, Гавайях, Гуаме, Маниле, и после войны — в Берлине, Франкфурте и Токио. Один из терминалов был установлен на 250-тонном океанском лихтере OL-31, обеспечивавшем связь генералу Д. Макартуру во время войны на Тихом океане. Таким образом, первый мобильный телефон с гарантированной защитой от подслушивания представлял собой огромный теплоход!

SIGSALY была самой большой из когда-либо построенных криптомашин. Каждый терминал содержал более тридцати стоек высотой свыше 2 м оборудования общим весом 55 тонн, занимал три больших помещения с кондиционированным воздухом (так как электронные лампы терминала потребляли 30 кВт электроэнергии)



Рисунок 4. Реконструкция терминала SIGSALY из экспозиции музея АНБ США

и обслуживался шестью операторами, которые не имели возможности прослушивания переговоров. Вместе с тем при сохранении режима секретности осуществлялись магнитные записи и стенографирование всех переговоров. К оценке криптографической стойкости шифратора привлекался легендарный Алан Тьюринг, принимавший участие в дешифровании немецкого шифратора «Энигма» (операция «Ультра»). В ходе этой операции под руководством Тьюринга был создан один из прототипов первого в мире «протокомпьютера». То есть первый настоящий компьютер Colossus был создан английскими инженерами 75 лет назад и предназначался для дешифрования немецкого шифратора Lorenz SZ 40/42, стоявшего на самых секретных линиях Третьего рейха. По причинам чрезмерно больших размеров, сложности и дороговизны эксплуатации терминалы SIGSALY были вывезены из мест дислокации и выведены из эксплуатации в 1946 году.

Скорость линейной передачи спектрально-полосного вокодера терминала SIGSALY составляла 1650 бит/с, что было на пределе возможностей модемов «узкополосной» радиосвязи тех лет. При такой скорости кодирования разборчивость расшифрованной речи неизбежно оказывалась очень низкой. К тому же полностью отсутствовала узнаваемость голосов абонентов. В связи с этим нередко руководители США и Англии созванивались по открытым каналам связи и договаривались о том, что сейчас они будут говорить по SIGSALY.

Шифрование осуществлялось сложением с оцифрованной речью специальной ключевой последовательности (гаммы), а на приёмном конце соответственно проводилось её вычитание. Интересно отметить, что ключ (гамма) был записан на грампластинках, которые после сеанса связи уничтожались.

В связи с высокой секретностью оборудования все терминалы были физически уничтожены, а грифы секретности



Рисунок 5. Корабль OL-31 — первый мобильный телефон с гарантированной защитой от подслушивания



Рисунок 6. Грампластинки — носители ключевой гаммы

патентов, положенных в основу разработки, сняты только в 1976 году. В начале XXI века один образец терминала SIGSALY был воссоздан заново для постоянной экспозиции в Национальном криптологическом музее США.



Рисунок 7. Делегации «Большой тройки» во время переговоров в Потсдаме

ПОТСДАМ-45

Теперь рассмотрим организацию правительственной связи в ходе Потсдамской (пригород Берлина) конференции, проходившей с 17 июля по 12 августа 1945 г. В ней участвовали И. В. Сталин, новый президент США Г. Трумэн и У. Черчилль. В ходе конференции, 28 июля, У. Черчилля сменил вновь избранный премьер от партии лейбористов Клемент Эттли, но Черчилль остался в составе английской делегации и принимал активное участие в переговорах.

В Потсдаме обсуждались проблемы устройства послевоенной Европы, а также условия вступления СССР в войну против Японии. Основную работу по организации правительственной связи на основном узле, получившем условное название «Пальма», проводили специалисты ОПС НКВД под руководством заместителя начальника ОПС И. Я. Воробьева.

Средством шифрования были всё те же «Соболь II» как основной шифратор речевых сообщений и другие речевые и текстовые шифраторы, о которых упоминалось выше. Американцы и англичане использовали для передачи секретной информации берлинский терминал SIGSALY и другие средства.

В Берлине и непосредственно в Потсдаме все работы по строительству линий связи с нашей стороны производились личным составом 55 и 115 ОРПС. Подвеску всех типов кабелей и монтажные работы по телефонизации

зданий также осуществляли военные связисты. Кроме того, для работ по прозвонке, расшивке и пайке освинцованных кабелей была привлечена специально созданная бригада кабельщиков. Поскольку все вышеперечисленные работы были выполнены качественно и в срок, связь объекта «Пальма» с Москвой во время всей конференции работала устойчиво.

ПРО АТОМНУЮ БОМБУ

Самая важная для президента США зашифрованная телеграмма пришла накануне конференции 16 июля 1945 г. Из-за особой её важности помимо шифрования был применён условный язык. Дело в том, что в эти же дни завершилась подготовка к испытанию первой атомной бомбы, и Трумэн с нетерпением ждал сообщения о результатах.

Испытания проводились на базе ВВС в Аламогордо. Административным руководителем проекта «Манхэттен» по созданию атомной бомбы был генерал Л. Гровс. На испытания был направлен личный представитель президента Гаррисон. Сопровождавший Г. Трумэна министр обороны Г. Стимсон (тот самый, что в 1929 году, будучи госсекретарём, с фразой «Джентльмены чужих писем не читают» закрыл дешифровальную службу внешнеполитического ведомства США) держал руку «на пульсе».

И вот 16 июля Стимсон получил от Гаррисона телеграмму примерно такого содержания: «Доктор только

что вернулся, исполненный энтузиазма и уверенный, что мальчик оказался таким же шустрым, как и его старший брат. Свет его глаз достигал отсюда Хайхольда, и я мог слышать его вопли на моей ферме».

Гаррисон и Стимсон были друзьями и хорошо понимали намёки друг друга. Содержание телеграммы в общих чертах описывало результаты успешных испытаний. При этом под «доктором» следует понимать Л. Гровса (подчинённые нередко называли его доктором); старший брат — испытанная ранее бомба; младший брат — вторая бомба, предназначенная уже для военного применения; Хайхольд — ферма Стимсона; ферма Гаррисона была расположена в сорока милях от Вашингтона. Поэтому Стимсону нетрудно было вычислить расстояния, на которых наблюдалась вспышка и был слышен звук взрыва. Г. Трумэн был в восторге от этих данных.

После получения этой информации Трумэн заявил своему окружению: «Наконец-то я получил хорошую дубинку для этих ребят». Речь, разумеется, шла об СССР. Американский президент поделился радостью с Черчиллем, решено было на следующий день рассказать об этом событии Сталину. Вопреки ожиданиям союзников И. В. Сталин весьма сдержанно отреагировал на это сообщение и лишь поблагодарил за информацию. Лидеры союзников даже подумали, что Сталин не понял, о чём его проинформировали. На самом деле советский лидер отлично знал о ходе работ по атомному проекту в США, и в Москву тут же полетела зашифрованная телеграмма с предписанием резко интенсифицировать работы по созданию нашей атомной бомбы.

В заключение отметим, что опыт работы советских криптографов и связистов при организации связи во время встреч лидеров «большой тройки» оказал существенное влияние при создании регулярных зашифрованных линий связи с советскими загранучреждениями (посольствами, консульствами и т.д.) и группировками войск, располагавшимися за границей в послевоенный период.



Борис СТОЛПАКОВ
историк криптографии,
кандидат физико-
математических наук



Здание МИД в Петербурге,
архитектор К. И. Росси. Фото К. К. Буллы

ПЕРВЫЕ ЛИЦА ОТРАСЛИ

ШТРИХИ К ПОРТРЕТАМ ГЕНЕРАЛОВ КРИПТОГРАФИЧЕСКОЙ СЛУЖБЫ РОССИЙСКОЙ ИМПЕРИИ

Перед нами судьбы нескольких ведущих криптографов Министерства иностранных дел Российской империи. Они много лет возглавляли шифровальное и дешифровальное направления деятельности криптографической службы МИД. Хотя наши герои имели гражданские чины, но ранг их званий был генеральский. Уже это обстоятельство делает эти персоны заслуживающими внимания. Помимо житейского разнообразия, в событиях жизни их самих и близких им людей запечатлелось время: начало XX века и революционные перемены.

ВЛАДИМИР ВАСИЛЬЕВИЧ САБАНИН

Он родился в 1853 г. в Симбирске. В 1876 г. окончил Петербургский университет со званием кандидата права и поступил на государственную службу в

Правительствующий Сенат, а в следующем году перешёл в Министерство внутренних дел, в его хозяйственный департамент.

Согласно сословным традициям, Владимир Васильевич сочетал чиновную службу с общественной деятельностью. Её Сабанин начал в 1879 г. как делопроизводитель Постоянной комиссии по техническому образованию при Императорском техническом обществе. Благодаря своей энергии он уже вскоре стал товарищем, т.е. заместителем, председателя комиссии. Довелось ему потрудиться и мировым судьёй в Симбирской губернии.

Начало криптографической карьеры

В 1885 г. Сабанин перешёл в Министерство иностранных дел и с 1 декабря был зачислен в дешифровальную экспедицию, отделение при канцелярии

министерства. Его успешное освоение на новом поприще подтверждают ведомственные поощрения. Так, в 1892 г. Сабанин получил крупную премию — 800 руб. — за вскрытие генерального шифра правительства Великобритании для связи с посольствами в Санкт-Петербурге, Тегеране и Константинополе, действовавшего с декабря 1890 г. Не удивительно, что в 1893 г. он занял освободившуюся должность старшего чиновника и возглавил отделение. Согласно документам, за 1899–1902 гг. В.В. Сабанин сумел прочесть 3175 шифротелеграмм, больше всех среди чиновников своего отделения.

Заметен в общественных делах за пределами МИД

При немалой служебной занятости он находил время для активного участия в общественных делах за пределами МИД.



Иллюстрация 1. В. В. Сабанин

Среди них — организация I съезда по техническому и профессиональному образованию в 1889 г. Там Сабанин потрудился и как член организационного комитета, и в качестве руководителя секции ручного труда. В 1893 г. его избрали в товарищи председателя Общества для распространения коммерческих знаний. В 1896 г. Владимир Васильевич возглавил комиссию по исследованию кустарной промышленности в России.

К середине 90-х годов утвердился его интерес к развитию российской печати. В 1895 г. Сабанин принял участие в организации первой выставки печатного дела в качестве почётного секретаря, а в 1899 г. его избрали председателем Русского общества печатного дела.

В весьма сложное время, с 1901 г. по 1906 г., Владимир Васильевич занимался налаживанием деятельности Российского телеграфного агентства как его директор-распорядитель. К этому времени он уже приобрёл широкую известность. 25-летию его общественной деятельности была посвящена статья, опубликованная в популярном иллюстрированном российском журнале «Нива» в 1901 г. Разумеется, о служебных занятиях Владимира Васильевича там не было упомянуто ни слова. Благодаря известности в 1906 г. его избрали депутатом Санкт-Петербургской городской думы.

«Неустанная, энергичная деятельность...»

Из такого перечисления вполне понятно, что Сабанин обладал широким кругозором. Добавим, что он любил музыку, сам нередко исполнял музыкальные произведения, свободно владел английским, французским, немецким и итальянским языками. Его интересовала история изящных искусств. Как отмечено в «Ниве», «кроме своей неустанной, энергичной деятельности в области печатного дела и технического труда он сотрудничал в нескольких органах печати. Его перу принадлежит много статей по техническому образованию, кустарной промышленности, по печатному делу, археологии и библиографии».

У истоков Петербургского телеграфного агентства

Похоже, что Сабанину было тесновато в пределах МИД. Его активная натура искала и находила всё новые поприща для приложения своей недюжинной энергии на благо Отечества. Вовсе не случаен был его интерес к печати и делам телеграфного агентства. Он диктовался заботой о защите правдивой информации о жизнедеятельности Российского государства от её намеренного искажения. Надо сказать, что руководители МИД поддерживали начинания Сабанина. Например, газетная экспедиция МИД была преобразована в Бюро печати, а заведующий Бюро с 1906 г. одновременно стал директором Петербургского телеграфного агентства, так оно официально стало именоваться. Возглавлявшие министерство В. Н. Ламздорф и А. П. Извольский стремились к тому, чтобы МИД стал основным источником информации по внешнеполитической тематике.

Безусловно, основное внимание Владимира Васильевича было обращено на руководимое им подразделение МИД. В 1905 г. В. В. Сабанина пожаловали в действительные статские советники.

Шести чиновникам в основном удавалось ладить...

Как можно судить по документам, атмосфера в маленьком чиновничьем коллективе дешифровального отделения была достаточно спокойной. Шести

чиновникам и их помощникам в основном удавалось ладить и совместно решать свои сложные задачи. Они постоянно были рядом и на службе, и в быту, поскольку все жили в министерском доме на Большой Морской, 20.

Но всё же иногда возникали конфликты. Например, в 1903 г. испортились отношения между В. В. Сабаниным и младшим чиновником А. А. Долматовым. Хотя вместе они трудились уже 16 лет, и из них 10 Сабанин был начальником Долматова. В марте Сабанин неожиданно обратился к начальнику канцелярии министерства А. С. Волкову с предложением назначить Долматова на одну из консульских вакансий. Тот якобы «давно уже ходатайствует о назначении за границу» и при этом отличается низкой работоспособностью — «за последние четыре года расшифровал только 391 телеграмму». Сабанин обосновывал своё предложение тем, что уход Долматова «не только бы не нарушил правильного строя... работы, но наоборот устранил бы довольно серьёзные ненормальные стороны настоящего положения вещей в экспедиции». Однако такое предложение не получило поддержки начальства. Сабанину и Долматову пришлось работать вместе до мая 1907 г., когда В. В. Сабанин неожиданно и скоропостижно скончался от заражения крови.

АЛЕКСАНДР АЛЕКСАНДРОВИЧ ДОЛМАТОВ

Именно А. А. Долматов в июне 1907 г. получил должность старшего чиновника и возглавил дешифровальное отделение после 20 лет своей службы в нём. Сын надворного советника, что равнозначно подполковнику, не особенно родовитый, он начал чиновную карьеру после окончания университета в 1883 г. Криптографическую должность младшего чиновника второй, дешифровальной, экспедиции при Канцелярии МИД А. А. Долматов получил 7 января 1887 г., а покинул это отделение лишь спустя 30 лет, летом 1917 г.

Регулярно получал премии за вскрытие иностранных шифров...

В сохранившихся документах нет свидетельств о его ярких достижениях. Вместе с тем Долматов, как и другие

криптографы, регулярно упоминался в ведомостях Цифирного комитета на выдачу премиальных денег за вскрытие иностранных шифров. Так, в 1892 г. он получил в общей сумме 600 руб. за участие в коллективном разборе четырёх шифров, в том числе трёх германских двузначных кодов. К началу столетия особенной специализацией Долматова стали ключи Бельгии и Испании.

Ответственность за работу отделения с 1907 г. стала его постоянной заботой. Безусловно, с приближением ко времени Первой мировой войны объём криптографической работы всё возрастал, она усложнялась и требовала согласованных действий развивавшихся тогда ведомственных криптографических служб. Труды А. А. Долматова получили достойную оценку, и в 1910 г. он достиг чина действительного статского советника.

Семейная трагедия

Добавим, что в 1913 г. Долматов пережил тяжёлую семейную трагедию. Его сын, А. А. Долматов, окончивший Училище правоведения и тоже служивший в МИД, стал азартным игроком. По этой причине в конце 1912 г. Долматов-младший был уволен из министерства. Уже вскоре, 6 февраля 1913 г., он был арестован за убийство, совершённое им из корыстных побуждений вместе с другом, бароном В. В. фон Геймаром. В итоге Долматов-младший был приговорён к семнадцати годам каторги.

БАРОН КОНСТАНТИН ФЕРДИНАНДОВИЧ ФОН ТАУБЕ

Константин Фердинандович родился в 1854 г. в Петербурге. Обучался в престижном Императорском Александровском лицее и после выпуска в мае 1877 г. высочайшим приказом был определён на службу в МИД.

В 1880–1882 гг. начинающий дипломат работал за границей: первые полгода — вторым секретарём российской миссии в Мадриде, затем его перевели в Брюссель. По возвращении в Петербург барон фон Таубе стал вторым секретарём канцелярии МИД. В сферу ответственности этого подразделения входило ведение политической переписки, в



Иллюстрация 2. Барон К. Ф. фон Таубе с дочерью Софьей в 1902 году

основном шифрованной. Шифрованием и расшифрованием депеш занималась, прежде всего, дипломатическая молодёжь, вроде Таубе. Но и канцелярское начальство нередко брало на себя работу с особенно важной корреспонденцией.

«Сочинением шифров» в МИД он занимался 35 лет!

При канцелярии действовали две отдельные экспедиции, первая занималась созданием шифров для засекречивания собственной переписки с посольствами за рубежом, а вторая — дешифрованием перехваченных телеграмм иностранных миссий. Именно первая сфера деятельности и привлекла Константина фон Таубе, «сочинением шифров» в МИД он занимался 35 лет!

А тогда, в 1882–1883 гг., серьёзные изменения произошли и в личной жизни молодого чиновника — он женился на дочери тайного советника Марии Николаевне Замятниной, родились дети — дочь Софья (1883–1907) и сын Константин (1887–1940).

В формулярном списке фон Таубе 1883 и 1887 годы отмечены премиями в 800 и 1000 рублей за успешную разработку шифров. В мае 1887 г. он был произведён за отличие в коллежские советники и назначен управляющим 1-й экспедицией при канцелярии МИД.

«Не от мира сего»

По свидетельствам современников, Константин Фердинандович, постоянно погружённый в мир шифров, был человеком «не от мира сего». Его семейный союз оказался непрочным. По просьбе супруги в 1891 г. он дал ей своё согласие на развод и больше не женился.

Тем не менее карьера барона продвигалась вполне успешно. В 1896 г. К. Ф. фон Таубе принимал участие в торжествах в Москве по случаю коронации Николая II. Такие события обычно сопровождалась раздачей монарших милостей, и глава «сочинителей шифров» стал действительным статским советником.

Барон К. Ф. фон Таубе и в июне 1901 г. был лично отмечен императором, ему пожаловали 800 рублей «за труды по составлению нового секретного шифра». Среди специалистов Константин Фердинандович по праву считался и считается крупным систематизатором криптографического наследия и организатором широкого применения кодов в шифровальной практике.

Предложение об объединении службы

В 1907 г. в МИД была учреждена комиссия по реорганизации министерства под председательством товарища министра тайного советника К. А. Губастова. Авторитетнейший член Цифирного комитета и управляющий первой экспедицией, т.е. отделением разработки собственных шифров, барон К. Ф. Таубе 24 мая 1907 г. предложил сосредоточить всю шифровальную деятельность в одном подразделении.

В ответ старший чиновник А. А. Долматов, только что заменивший умершего В. В. Сабанина на посту руководителя второй экспедиции (дешифровального отделения), представил докладную записку от 28 июня, в которой категорически возражал против соединения двух отделений, имеющих дело с шифрами, в одно целое. Он заявлял, что его отделение «благодаря духу соревнования, материальным выгодам и отсутствию рутинности, продолжает самостоятельно и успешно работать, несмотря на чрезвычайные затруднения», в то время как первая экспедиция «живёт трудами посторонних лиц», её цель — создание шифров и с политической направленностью работы МИД ничего общего не имеет.

Заметим, что Долматов немного лукавил, отметив труды посторонних лиц только в интересах первой экспедиции. Ему и самому приходилось использовать такие труды. Так, согласно ведомостям Комитета по шифрам, он и Е. И. Ловягин, профессор греческого языка Санкт-Петербургской духовной академии, в равной степени разделили успех «в разборе сербского шифра» в 1892 г., оба получили в качестве премии по 300 руб.

Неформальное единство криптографов нерушимо

В свою очередь, барон фон Таубе 19 сентября снова обратился к Губастову, доказывая, что объединение будет благом для всех цифирных экспедиций, поскольку криптография едина и важно взаимодействие всех частей шифровального дела. Он предлагал собрать в одном подразделении три экспедиции: первую — для изготовления шифров, вторую — для дешифрования и третью — для шифрования и расшифрования всех текущих документов.

Всё же Таубе и Долматов продемонстрировали и единство в своих предложениях по реформированию министерства: оба выразили пожелание увеличить штаты первой экспедиции и повысить оклады её чиновникам. В результате всех обсуждений дешифровальная экспедиция сохранила свою самостоятельность.

Осуществление объединительных замыслов

Как бы в утешение и в знак уважения его четвертьвековым трудам на криптографическом поприще в 1907 г. барон получил орден Св. Станислава I степени, на ленте через плечо, с орденской звездой. В 1913 г. барон фон Таубе был произведён за отличие в тайные советники, т.е. в чин, равный армейскому генерал-лейтенанту. А в июле 1914 г. при реорганизации министерства Константин Фердинандович добился наконец осуществления своих объединительных замыслов.

Он получил назначение управлять Цифирным отделением при 1-м политическом отделе МИД, возглавив, таким образом, криптографическую службу российского внешнеполитического ведомства. Цифирным отделением Таубе руководил до лета 1917 г. Тогда завершились его 35-летняя служба на поприще криптографии и 30-летнее руководство «сочинением шифров».

НЕМНОГО О ДЕТАХ

Воздержался от сотрудничества

Барон Константин Фердинандович фон Таубе скончался в 1919 г., в Петрограде, в обстановке Гражданской войны.

Его сын, Константин Константинович фон Таубе, также трудился на дипломатическом поприще. В годы Первой

мировой войны он служил вторым секретарём российского посольства в Тегеране. Иран был тогда прифронтовым государством: с его территории войска Антанты, включавшие российский контингент, вели наступление на турецкую Месопотамию. В конце 1917 г., как и многие «старорежимные» дипломаты, К. К. фон Таубе воздержался от сотрудничества с Советским правительством и предпочёл эмиграцию.

«Без него мы бы не справились»

По-иному сложилась судьба его ровесника, сына В. В. Сабанина Андрея Владимировича Сабанина. Он родился в 1887 г., в Петергофе. В 1904–1905 гг. изучал восточные языки в Петербургском университете, но в 1908 г. окончил Императорский Александровский лицей с золотой медалью. Тогда же А. В. Сабанин поступил на дипломатическую службу в Министерство иностранных дел.

В 1920–1937 гг. А. В. Сабанин работал в Наркомате иностранных дел СССР, с 1931 г. заведовал там Правовым отделом. Он участвовал в дипломатических переговорах и международных конференциях, готовил проекты договоров. В апреле 1922 г., во время Генуэзской конференции, он по поручению руководителя делегации Г. В. Чичерина сумел наладить контакт с начальником Русского отдела МИД Германии. Это стало прологом подписания советско-германского договора в Рапалло «О восстановлении дипломатических отношений, взаимном отказе от претензий и торгово-экономических связях».

Нарком Иностранных дел Г. В. Чичерин так отзывался о Сабанине: «У него совершенно исключительное, единственное знание практических вопросов, которые ежедневно возникают с другими государствами. Такие вопросы всегда точно и хорошо известны Сабанину; без него мы бы не справились».

Андрей Владимирович занимался также преподавательской деятельностью в московских вузах. В 1937 г. А. В. Сабанина арестовали, обвинили в шпионаже и вскоре расстреляли в посёлке Коммунарка Московской области.

БУДУЩЕЕ КРИПТОГРАФИИ СОЗДАЁТСЯ УЖЕ СЕГОДНЯ¹

С ЗАБОТОЙ О ЗАВТРАШНЕМ ДНЕ КРИПТОГРАФИИ

При всём разнообразии литературы по информационной безопасности специалистам и педагогам заметна недостаточность публикаций, интересно и ненавязчиво ориентирующих старшеклассников на выбор ИБ-специальностей. Особенно важен для отрасли выбор жизненного пути тех из школьников, кто уже участвовал или пока только собирается принять участие в олимпиадах по криптографии и информационной безопасности.

Профессиональную аудиторию, особенно родителей, несомненно, заинтересует информация о новом издании. В настоящее время готовится к печати книга Н. В. Никонова и Б. В. Столпакова «Просто о важном. Экскурсия в криптографию без формул». Издание осуществляется при поддержке НКО «Фонд содействия развитию безопасных информационных технологий» (ФСРБИТ).

По замыслу авторов, книга предназначена для, возможно, первого знакомства с криптографией, ныне ставшей важнейшей частью той сферы человеческой деятельности, что именуется защитой информации.

Небольшая по объёму книга задумана авторами как экскурсия в перспективную область приложения интересов и умений современного молодого человека. Авторы видят своей целью показать на небольшом числе наглядных примеров (без формул!) исторический путь криптографии и

доступно продемонстрировать её обширные возможности в современном мире.

В историческом разделе нашли своё достойное место и материалы уже ставшего известным проекта «Криптографический фронт Великой Отечественной войны», реализованного ФСРБИТ в 2019 г.

Несомненный интерес для целевой аудитории, прежде всего старшеклассников может представлять знакомство с плодотворными идеями, обеспечившими широкое применение криптографии. Среди них — идеи криптосвязи с открытым ключом и электронной подписи. Предусмотрено и доступное ознакомление с технологическими особенностями современной криптографии, прежде всего с хранением и распространением по сети открытых ключей, хранением закрытых ключей.

Наибольший интерес, вероятно, вызовет подробный рассказ о криптографии, сопровождающей нас в повседневной жизни. Здесь и криптография, обеспечивающая безопасность наших финансовых интернет-операций, и методы криптозащиты от незаконных транзакций.

Авторы постарались доступно ознакомить возможных читателей с перспективными идеями блокчейн-технологий и работ в таинственной квантовой области применения криптографии.

Вниманию читателей журнала, заинтересовавшихся информацией о книге, предлагаем одну из её глав.

Наша страна активно участвует в мировом процессе «цифровизации» экономики и всей общественной жизни, неотделимом от глубокого развития и внедрения информационных технологий. Уже сегодня сложные информационные технологии не могут обойтись без криптографических механизмов обеспечения их эффективности и безопасности. Со временем эта зависимость будет только усиливаться.

Давайте подробнее рассмотрим два перспективных технологических направления, напрямую связанных с криптографией: системы

распределённого реестра (или блокчейн) и квантовые технологии. Первое из них, вероятно, будет использоваться так же повсеместно, как и сеть Интернет, создавая её надстройку, а второе, может стать, полностью изменит нынешние представления о компьютерных вычислениях и способах организации безопасной передачи данных на расстоянии.

КРИПТОГРАФИЯ В БЛОКЧЕЙНЕ

Удивительно, как, начиная с публикации в 2009 г. небольшой статьи анонимного автора под псевдонимом Сатоши Накамото, стало решительно формироваться и развиваться новое направление общественных интересов прежде всего в финансовой области.

Направление, уже вскоре собравшее гигантские ресурсы на решение множества задач, связанных с блокчейн-технологией (от англ. Blockchain — цепочка блоков).

Представим себе ситуацию, при которой две не доверяющие друг другу стороны желают совершить сделку в электронном виде через Интернет. Известно, что честное взаимодействие при недоверии друг другу невозможно без наличия третьей доверенной стороны. Сейчас такой стороной является банк или какая-либо другая, как правило, государственная организация. Этот посредник, взимающий оплату за предоставленные услуги, например, по реализации честной сделки, одновременно в какой-то степени может контролировать её.

¹ Глава из книги «Просто о важном. Экскурсия в криптографию без формул», Н. В. Никонов, Б. В. Столпаков.



Иллюстрация 1. Варианты кошельков для криптовалют

Latest Blocks				Latest Transactions			
Рост	Добыто	Майнер	Размер	Хэш	Время	Сумма (BTC)	Сумма (USD)
640726	25 секунд	F2Pool	1 502 488 bytes	8663dd0430999aae9862...	13:59	0.00460248 BTC	44,13 \$
640725	13 минут	Unknown	1 697 901 bytes	2f1e7c044f6cd8854bd78...	13:59	0.00301292 BTC	28,89 \$
640724	16 минут	Unknown	1 644 999 bytes	3b25a7b52b529dfee9ba2...	13:59	0.03088797 BTC	296,19 \$
640723	19 минут	Unknown	1 351 121 bytes	641b89156bbb66ff1d519...	13:59	0.43889235 BTC	4 208,68 \$
640722	26 минут	AntPool	1 322 149 bytes	f910bd3e07c27c16fb2170...	13:59	0.07015426 BTC	672,73 \$
640721	30 минут	Poolin	1 393 454 bytes	ecd95932a9c3fc38ecba6...	13:59	1.01244900 BTC	9 708,70 \$

Иллюстрация 2. Таблица блоков блокчейна и необработанных транзакций

Блокчейн-технология предлагает на роль третьей доверенной стороны сам блокчейн — электронную конструкцию, не нуждающуюся в централизованном управлении и обслуживании. При этом, если речь идёт о финансах, валютные активы представляются в электронном эквиваленте — криптовалюте. Сейчас их много разных — Bitcoin (BTC), Monero (XMR), Zcash (ZEC), Ethereum (ETH) и др., все они торгуются на бирже и имеют свой текущий эквивалент в реальной валюте. Криптовалюта, как и обычные деньги, должна где-то храниться, и для неё тоже есть кошельки, но только они электронные, и доступ к вашим кошелькам должен быть защищён вашим закрытым ключом. Можно завести такой кошелек для хранения различных криптовалют у себя на мобильном

устройстве (Mobile wallets), компьютере (Desktop wallets) или аппаратном носителе (Hardware wallets). Легко найти сайты, где это возможно сделать, там вам предложат различные варианты кошельков в зависимости от операционной системы (см. илл. 1).

Как и в случае с электронной подписью, безопаснее всего электронный кошелек создать на аппаратном носителе, доступ к которому защищён PIN-кодом. Вне зависимости от типа кошелька важно не потерять к нему закрытый ключ — его потеря равноценна потере ваших электронных денег без возможности их восстановления. И в этом, пожалуй, заключается неудобство и важное отличие от традиционной финансовой структуры — отсутствие возможности возмещения потерянных средств. Правда, можно

с этой целью использовать различные онлайн-сервисы для хранения своей криптовалюты, но в этом случае получается так же, как и с подписью в облаке: вы снова полностью полагаетесь на какую-то третью сторону, от которой будет зависеть безопасность вашей информации и цифровые активы.

У каждого электронного кошелька есть адрес — фактически это ваш открытый ключ, на илл. 1 — это строка чисел и букв, правее — представление его в виде QR-кода. Если вы хотите перевести часть своих электронных денег, необходимо выбрать адрес кошелька получателя и создать транзакцию, подписав её своим закрытым ключом.

Сама транзакция имеет входы, связанные с адресами кошельков, откуда поступают электронные деньги, и

Block Transactions 			
Хэш	40ec9db3c07067b0b7c4822a4f5ee17d40c10a1fba82122360c2a22...	2020-07-25 13:59	
	COINBASE (Вновь Созданные Монеты)	1KFHE7w8BhaENAswwryaocDb6qcT6DbYY	6.86288920 BTC 
		OP_RETURN	0.00000000 BTC
		OP_RETURN	0.00000000 BTC
		OP_RETURN	0.00000000 BTC
Комиссия	0.00000000 BTC (0.000 sat/B - 0.000 sat/WU - 377 bytes)		6.86288920 BTC
			1 Подтверждения
Хэш	9b7effd9ed54d40dc4c71fd703fb79c7d6d004bea7c627b1327a5d4...	2020-07-25 13:54	
	17A16QmavnUfCW11DAApiJxp7ARnxN5pGX	6.21250393 BTC 	35S8YcFFcMkVSQMmHXjbk4Bc5KPiym6tCL
			0.00438556 BTC 
			3Mr6Bv9iAGHSj3vSoGspizyVrJCzJLBGy2
			0.01835282 BTC 
			17A16QmavnUfCW11DAApiJxp7ARnxN5pGX
			6.18854491 BTC 
Комиссия	0.00122064 BTC (425.310 sat/B - 106.328 sat/WU - 287 bytes)		6.21128329 BTC
			1 Подтверждения

Иллюстрация 5. Транзакции в блоке блокчейна

так, чтобы блок добавлялся в блокчейн примерно раз в 10 минут). Вы уже знаете, что найти такое PrevHash' непросто, так как обратить хеш-функцию очень сложно. Поэтому майнеру приходится кропотливо перебирать значения специального параметра Nonce', чтобы найти подходящее хеш-значение. Вот почему для этого процесса строят целые вычислительные фермы — у кого больше вычислительных мощностей, тот и будет быстрее находить требуемое значение Nonce' и добавлять блоки в блокчейн. А за каждый добавленный блок предусмотрен механизм вознаграждения майнера определённой суммой биткойнов, также майнер получает комиссионное вознаграждение от инициаторов обработанных им транзакций.

Давайте рассмотрим блок с номером $i+1=640726$, обработанный майнером под именем F2Pool (именно его биткойн-адрес приведён на илл. 1). Видим, что ему потребовалось около 13 минут, чтобы создать новый блок после блока с номером $i=640725$. Нажмём на него и приведём некоторые поля этого блока, о которых было сказано выше (время бежит вперёд, и порождаются все новые блоки, поэтому, чтобы найти этот блок у себя в браузере, воспользуйтесь кнопкой View All Blocks) (илл. 4).

Ниже на илл. 5 можно увидеть сами обработанные транзакции (в разделе Block Transaction, их всего 2009). Первая транзакция (с хеш-значением 40ec...) — транзакция-вознаграждение (coinbase-транзакция) в размере около 6,8629 BTC за созданный блок и обработанные транзакции, а следующие транзакции связаны с переводом биткойнов с одних адресов на другие. Например, во второй транзакции (её хеш-значение равно 9b7e...) с адреса 17A16... совершается перевод примерно 6,2125 BTC на три адреса: 0,0044 BTC на 35S8Y...; 0,0184 BTC на 3Mr6B...; 6,1885 BTC на исходный адрес — это сдача, возврат непотраченных биткойнов. За обработку этой транзакции её инициатор заплатил майнеру около 0,0012 BTC.

Блокчейн обеспечивает анонимность сторон транзакций. Так, в блокчейн-сети криптовалюты биткойн трудно по биткойн-адресам выяснить, кто на самом деле за ними скрывается. Кроме того, имеются встроенные механизмы использования одноразовых адресов — новых для каждой совершаемой транзакции, а также способы запутывания входов/выходов транзакций и самих транзакций между собой. Однако существуют подходы по выявлению абонентов блокчейн-сети для биткойна, несмотря на предусмотренные выше

механизмы анонимности. Это стимулирует разработчиков на внедрение более надёжных криптографических методов обеспечения анонимности. Такие способы реализованы, например, в блокчейн-сетях криптовалюты Monero и Zcash.

Важно, что применение блокчейн-технологии выходит далеко за рамки и анонимного перевода электронных денег друг другу, и всего оборота криптовалют, ведь они могут и не прижиться в нашем мире. Развитие этой технологии уже сегодня позволяет решать сложные задачи по заключению финансовых сделок в электронном виде через выполнение так называемых смарт-контрактов (англ., smart — умный), организации регулярных поставок в торговых сетях, а также проводить электронное голосование, результаты которого невозможно изменить или подделать, и т.п.

КРИПТОГРАФИЯ В КВАНТАХ. РЕАЛЕН ЛИ АБСОЛЮТНО СТОЙКИЙ ШИФР?

Все слышали о квантовых компьютерах и квантовой передаче данных. Это не просто что-то новое, это смена привычных представлений. Трудно в полной мере представить, как квантовые технологии изменят наш мир, в какие области повседневной жизни они

внедряются, но с уверенностью можно сказать, что изменятся способы передачи информации, сами принципы компьютерных вычислений, другой станет и криптография.

Если в традиционном канале связи передаются биты (0 или 1), то в квантовом канале аналогом битов являются кубиты, не имеющие, к сожалению, простых и наглядных образов.

В основе квантовой передачи данных и квантовых вычислений лежит понятие кванта, который имеет и материальную, и волновую природу. Квантовые компьютеры пока ещё перспективные вычислительные устройства с не близкой практической реализацией, но с потенциально колоссальной производительностью за счёт распараллеливания процессов, требующих перебора, например, ключей.

Это проявится в возможности эффективно решать на квантовых компьютерах сложные для классических вычислений задачи дискретной математики, на которых основана стойкость современных асимметричных криптосистем. Они позволят быстро решать задачи разложения числа на простые множители и вычисления дискретного логарифма, чем подорвут основы применения криптосистемы RSA и алгоритмов электронной подписи. Безусловно, многие широко используемые методы шифрования не выдержат взлома с помощью квантового компьютера. Но это лишь в перспективе, в замыслах физиков и математиков. Тем не менее уже сейчас криптографы размышляют о постквантовой криптографии и формируют арсенал надёжных средств защиты информации. При любом исходе событий будущие криптографы окажутся среди самых востребованных специалистов.

Наряду с новыми подходами к пока что гипотетическому вскрытию многих используемых шифров, квантовые технологии приближают нас к техническому воплощению идеального, недоступного взлому шифра. Ещё в конце первой половины XX века благодаря исследованиям В. А. Котельникова и К. Шеннона в математике и криптографии сложилось чёткое и строгое понимание условий, которым должен удовлетворять такой абсолютно стойкий шифр:

- ◆ ключ известен только его законным пользователям;
- ◆ длина ключа в битах не меньше длины сообщения;
- ◆ ключ (цифровой) составлен случайным образом;
- ◆ ключ используется только один раз.

В этом случае зашифрованное сообщение становится статистически независимым от исходного сообщения и не даёт информации о нём. Вновь мы убеждаемся в важности решения проблемы передачи секретных ключей между удалёнными друг от друга пользователями. И ещё раньше уже известной нам идеи открытого ключа возникла мысль об использовании квантов при передаче ключей. Ведь с точки зрения классической физики любой другой вид физического сигнала, применённого при передаче ключа, может быть подслушан без оставления следов, а значит, не способен гарантировать секретность ключа при его доставке. Если же передавать ключи с помощью квантовых состояний, то возникает принципиально другая ситуация: невозможно скопировать неизвестное квантовое состояние, т.е. вмешаться в канал связи и не оставить следа. Так открылась перспектива передачи ключей с помощью квантовых состояний, секретность при этом гарантируется фундаментальными законами природы.

КВАНТОВЫЕ КРИПТОСИСТЕМЫ И ПРОТОКОЛЫ

В 1984 г. Ч. Беннетт и Ж. Brassar предложили первый значительный криптографический протокол для квантовой передачи — BB84 (первый квантовый протокол), с ним и связывают возникновение квантовой криптографии, занимающейся именно распределением секретных ключей между удалёнными друг от друга законными пользователями. Протокол BB84 позволяет зафиксировать любые попытки подслушивания в канале связи. Подслушивание, а значит, изменение (возмущение) передаваемых состояний фотонов будет неизбежно изменять статистику результатов измерений на приёмном конце канала связи по сравнению со статистикой результатов измерений на невозмущённых состояниях.

Роль состояний фотонов (значений кубитов) в этом протоколе играют их поляризации, которые условно можно изобразить следующим образом:

В протоколе BB 84 вместо «0» и «1» передаются фотоны с соответствующими, произвольно выбранными из двух, поляризациями (см. илл. 6). Состояние фотона нельзя просто увидеть — его можно только измерить, применив специальные фильтры. Известно, что такие фильтры могут достоверно измерять состояния фотонов только с ортогональными (перпендикулярными) поляризациями, поэтому такие фильтры обозначают так, как показано на илл. 6.

Для формирования общего ключа одна сторона выбирает последовательность из нулей и единиц и передаёт другой стороне по квантовому каналу связи фотоны с соответствующими поляризациями. Другая, приёмная сторона, выбирает произвольно фильтры и

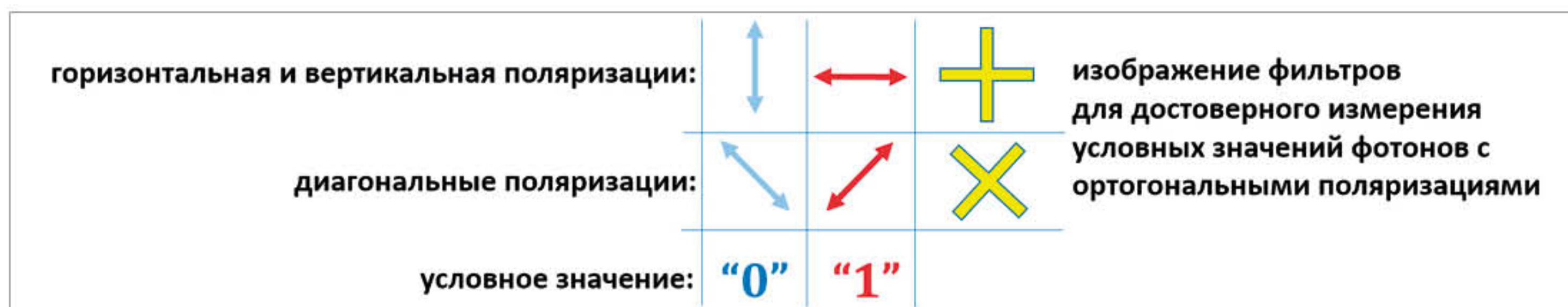


Иллюстрация 6. Поляризации фотонов и их условные значения

измеряет состояния полученных фотонов. Понятно, что примерно у половины фотонов состояние будет измерено неверно. Чтобы оставить только достоверные измерения и получить из них общий ключ, информация о верно выбранных фильтрах согласуется со стороной-отправителем по обычному каналу связи (см. пример на илл. 7).

Из описания этого протокола (и его известных модификаций) следует, что кроме квантового канала (как правило, оптоволоконного) необходимо наличие обычного открытого канала связи. Он требуется законным пользователям для контроля статистики результатов измерений и коррекции ошибок в первичном ключе, переданном по квантовому каналу связи. В реальных условиях для защиты обычного канала необходима процедура аутентификации и контроля целостности данных, что является существенным недостатком этих протоколов.

Позже в России был обоснован качественно новый подход на основе квантового запутывания и предложен протокол АКМ2017 (от авторов Ф.К. Алиев, А.В. Корольков, Е.А. Матвеев), позволивший отказаться от отдельного обычного канала связи. Отметим, что воздействие на один из предварительно квантово запутанных объектов немедленно скажется на другом квантовом объекте, на каком бы расстоянии они ни находились друг от друга.

Несмотря на все сложности, уже в начале 2000-х годов появились коммерческие прототипы квантовых криптосистем, и их возможности постепенно возрастают. Одной из подобных криптосистем является квантовый телефон, точнее, телефон с квантовой доставкой ключей для защиты связи. Российская разработка такой аппаратуры впервые была представлена для коммерческой реализации совместно компанией «ИнфоТеКС» и Центром квантовых технологий МГУ в 2019 году (илл. 8).

Кто-то из наших читателей, вероятно, в недалёком будущем продолжит череду этих успехов своими полезными новинками.

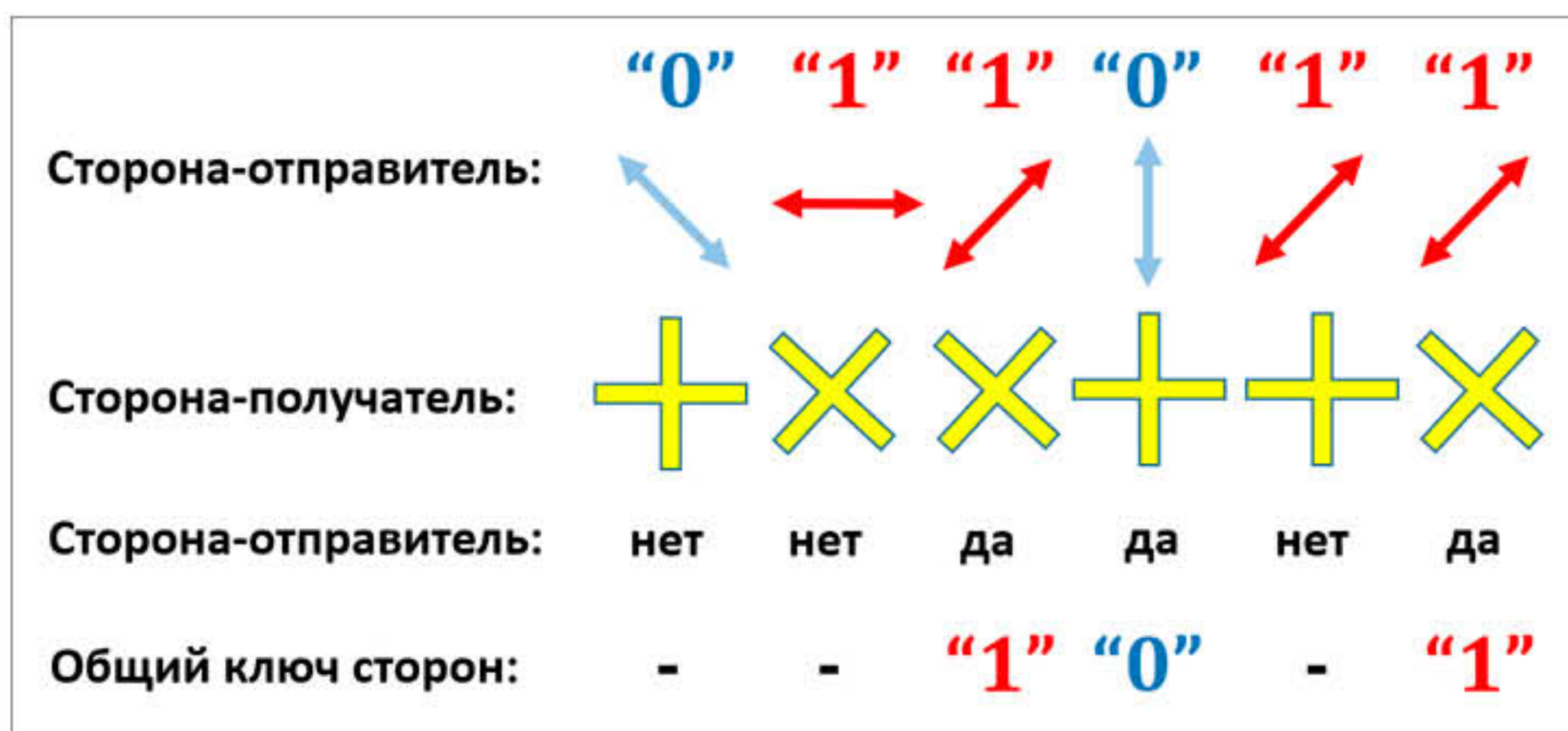


Иллюстрация 7. Пример формирования общего ключа по протоколу BB84



Иллюстрация 8. Телефон с квантовой доставкой ключей для защиты связи. Фото со стенда компании «ИнфоТеКС» в демозоне РКН-Форума Россия 2020

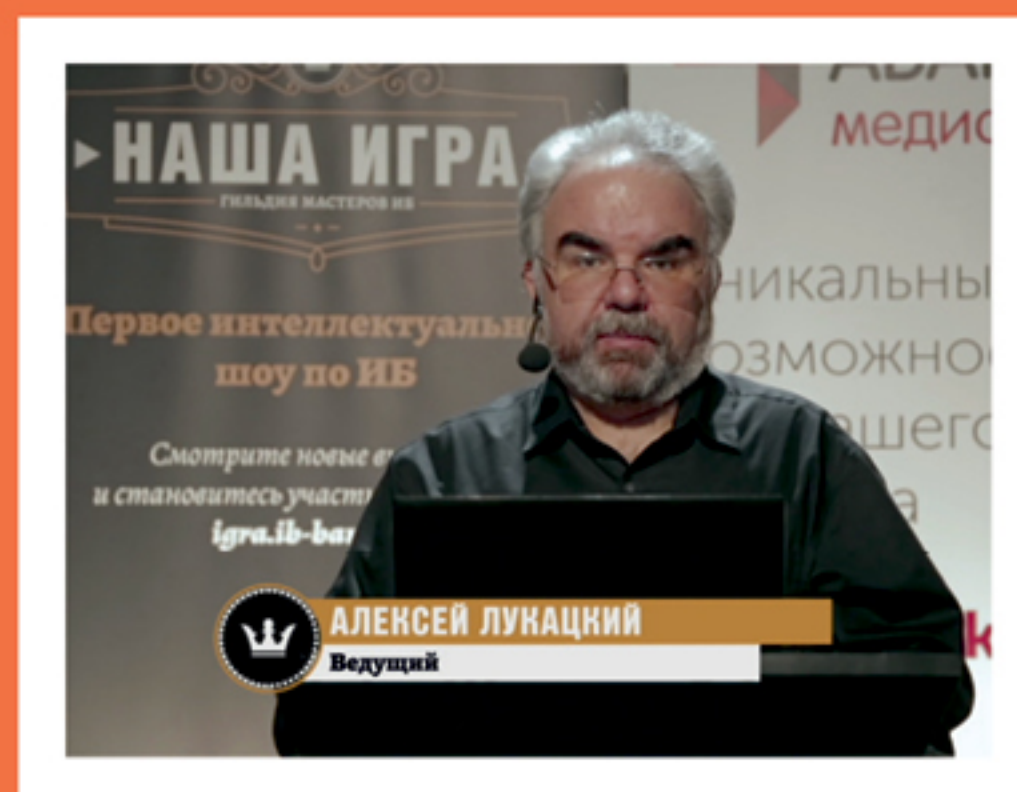


ОСВЕЩАЕТ ГЛАВНЫЕ МЕРОПРИЯТИЯ
ОТРАСЛИ И ПРОИЗВОДИТ
ВИДЕОКОНТЕНТ ДЛЯ ВАШИХ ЗАДАЧ:



На деловых мероприятиях:

- Яркие видеоотчёты
- Развёрнутые обзоры
- Интервью с участниками



Видео для ваших целей:

- Динамичные промовидео
- Серия тематических интервью
- Презентация продуктов
- Имиджевый ролик



В студии:

- Ток-шоу об ИТ и ИБ
- Телевикторина
- Специальные ТВ-проекты



BIS TV — фокус на безопасность



ib-bank.ru/bistv



SOC
ФОРУМ **LIVE**

ib-bank.ru/soclive

1 декабря 2020

10:00 (МСК)

начало

< Дистанцированы, но не сломлены!

Впервые SOC-ФОРУМ полностью
в онлайн – экспрессом в один день

Всё самое актуальное о центрах мониторинга
и противодействии **КИБЕРАТАКАМ!**



< БОЛЬШЕ _ НАСЫЩЕННЕЕ _ БЕЗОПАСНЕЕ >

ПАРТНЁРСКОЕ И СПОНСОРСКОЕ СОТРУДНИЧЕСТВО:

Екатерина Коденцева

Тел.: +7 (962) 947-46-32, E-mail: ekodentseva@avangardpro.ru

