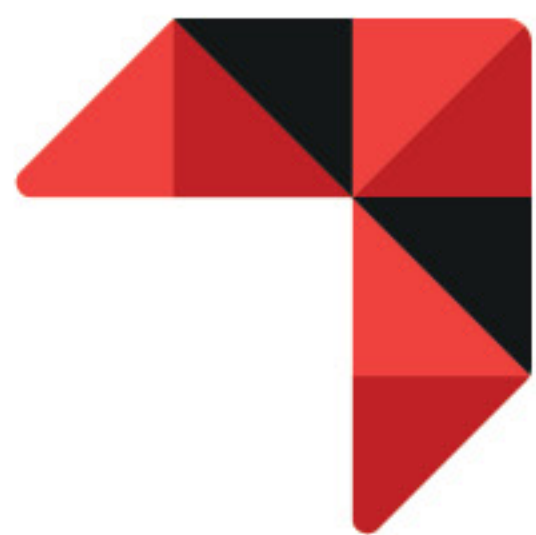




8 > Вадим КУЛИК
ВТБ
Банк как фабрика ИИ

28 > Василий ПИСКАРЁВ
Государственная Дума РФ
Атаки на систему
электронного
голосования
провалились



67 > Дмитрий
СЛОБОДЕНЮК
ARinteg
Искусство выбирать



84 > Александр ГАЛИЦКИЙ
ЭЛВИС-ПЛЮС
30 лет в море ИТ

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В БАНКЕ: ЭКСПЕРТИЗА ПРОБЛЕМЫ





УРАЛЬСКИЙ ФОРУМ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
ФИНАНСОВОЙ СФЕРЫ



IB-BANK.RU

15–18 ФЕВРАЛЯ 2022 ГОДА

Встречаемся на Урале!



Павел БЫЛЕВСКИЙ
шеф-редактор BIS Journal

Текущая ситуация и перспективы, преимущества и риски технологий «искусственного интеллекта» в финансовой сфере — главная тема этого номера BIS Journal. Для прагматиков-банкиров ИИ на основе BigData («больших данных») — не более чем новый перспективный функционал АСУ ТП (автоматизированных систем управления технологическими процессами). «ИИ» — просто новомодное название, очередной ребрендинг новых технологий автоматизации.

В банковской сфере ИИ открывает ряд конкурентных преимуществ: оптимизации, повышения эффективности, удешевления бизнес-процессов и клиентских сервисов. Значительно увеличивает продуктивность сбора, обработки и анализа данных о работе подразделений, о сотрудниках и клиентах.

К эффективным направлениям применения ИИ в банках относятся совершенствование корпоративных бизнес-процессов и клиентских сервисов, маркетинг и противодействие мошенническим операциям.

Как и прочим техническим новшествам, преимуществам использования ИИ в банковской сфере сопутствуют технические и гуманитарные риски. В том числе новые возможности недобросовестной конкуренции.

Аппаратные, программные, организационные ошибки и сбои могут снижать устойчивость бизнеса и оказания услуг, нарушать целостность и конфиденциальность информации, способствовать утечкам.

Среди социальных рисков ИИ — сокращение рабочих мест из-за автоматизации банкинга. К гуманитарным рискам банковского ИИ можно отнести возможности злоупотреблений данными клиентов: персональными, пользовательскими и биометрическими.

На основе ИИ могут создаваться инструменты так называемой «социальной инженерии», финансовых мошенников. Среди потенциальных новинок для злоумышленников — технология DeepFake, создание реалистичных поддельных фото и видео граждан.

В банковской сфере ИИ успешно применяется главным государственным регулятором отрасли — Банком России. Оставляя лиричным простоты размышления «может ли машина чувствовать и мыслить», прагматичные банкиры повышают инструментами ИИ эффективность и прибыльность бизнеса.

ОБЩЕСТВЕННЫЙ РЕДАКЦИОННЫЙ СОВЕТ

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

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Былевский П.Г. — шеф-редактор, кандидат философских наук
Велигура А.Н. — председатель комитета по банковской безопасности Ассоциации российских банков, руководитель комитета по безопасности НП «НПС», CISA, кандидат физико-математических наук
Виноградов А.Ю. — специалист Службы информационной безопасности КБ Максима (ООО)
Вихорев С.В. — советник генерального директора по информационной безопасности IT Expertise
Воробьева А.А. — руководитель интернет-проектов
Дзержинский Ф.Я. — независимый эксперт
Зубков А.Н. — генеральный директор ООО «Медиа Группа „Авангард“», директор Фонда содействия развитию безопасных информационных технологий (ФСРБИТ)
Курило А.П. — заведующий кафедрой международной информационной безопасности МГЛУ, кандидат технических наук
Левинов 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
Пазинин С.В. — заместитель начальника Управления по обеспечению ИБ Банка ВТБ (ПАО), кандидат физико-математических наук
Рачкова Е.В. — управляющий директор Управления по обеспечению ИБ Банка ВТБ (ПАО)
Филиппчук А.А. — технический директор ГК ЦРТ
Шумский Л.С. — руководитель службы информационной безопасности Яндекс.Банка
Янсон И.А. — бизнес-партнер по информационной безопасности, Департамент безопасности ПАО «Сбербанк России», кандидат физико-математических наук

ЭКСПЕРТНАЯ ГРУППА

Баранов А.П. — руководитель департамента информационной безопасности факультета информационных технологий Финансового университета при Правительстве РФ, доктор физико-математических наук, академик Академии криптографии РФ
Батранков Д.В. — 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 АО «Аладдин РД»
Сумманен К.Т. — директор по управлению проектами — вице-президент, Банк ВТБ (ПАО), кандидат физико-математических наук
Хайретдинов Р.Н. — директор по росту компании BIZONE

РЕДАКЦИЯ ЖУРНАЛА

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

УЧРЕДИТЕЛЬ-ИЗДАТЕЛЬ

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

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

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

Подписан в печать 09.11.2021. Тираж 5000 экз. Заказ № 1782021.
Цена договорная. Отпечатан в типографии «Московский Печатный Двор», 123298, г. Москва, 3-я Хорошевская 18, корп. 1, офис 201А

© BIS Journal, 2021



НОВОСТИ

5 Технологии, законодательство, криминал

ТЕМА НОМЕРА: ИИ В БАНКАХ

- 8 Вадим Кулик (ВТБ)
«ВТБ — не столько фабрика ИИ, сколько наука и практика, как единое целое»
- 12 Елена Покатаева (BIS Journal)
Куда стремится «умное» стадо?
- 20 Алексей Лукацкий (Cisco Systems)
Что надо знать, если вы решили применить машинное обучение при мониторинге угроз
- 24 Никита Ломов (Ассоциация ФинТех)
«Финансовые услуги нового поколения потребуют этического регулирования»
- 26 Елена Покатаева (BIS Journal)
Тот ещё субъект...



31

РЕГУЛЯТОРЫ

- 28 **Выборы**
Василий Пискарев (Государственная Дума)
«Причастные к кибератакам на систему электронного голосования должны понести заслуженное наказание»



12

БАНКИ

- 31 **Вредные советы**
Екатерина Рачкова (Банк ВТБ)
Цепляйтесь к словам и называйте вещи своими именами
- 34 **Нормотворчество**
Сергей Вихорев (ИТ-Экспертиза)
Везде есть плюсы и минусы, главное, чтоб не замкнуло...
- 35 **Нормотворчество**
Александр Бойко, Алексей Сабанов (Аладдин Р.Д.)
Не так страшен чёрт, как его малюют
- 37 **Нормотворчество**
Василий Окулесский (Банк «Возрождение»)
«Такие стандарты у нас не часто встречаются...»
- 40 **ФинТех**
Кирилл Кузьмин (Ассоциация ФинТех)
Открытые API: соединение установлено
- 42 **Локдаун**
Александр Виноградов (КБ «Максима»), Оксана Докучаева (Московский метрополитен), Анастасия Николаева (КБ «АРЕСБАНК»)
Не подстелили соломки...



SOC-ФОРУМ

- 44 Алексей Лукацкий (Cisco Systems)
Разбегаются глаза. Какую модель функционирования SOC выбрать?
- 49 Александр Бодрик (BIS Journal)
DevSecOps. Пока не попал впросак
- 52 Алексей Юдин (Infosecurity),
Андрей Коняхин (ПАО «Норвик Банк»)
От непонимания до заключения контракта
- 54 Иван Мелехин (Информзащита)
Прозреть!
- 56 Тимур Зиннатуллин (ГК Angara)
SOC против pentest
- 58 Борис Осепов (Лаборатория Касперского)
Развиваете SOC? Мы знаем, как вам помочь
- 60 Антон Фишман (RuSIEM)
Берите крылышко!



УГРОЗЫ И РЕШЕНИЯ

- 63 **Удалённый доступ**
Дмитрий Михеев (АйТи БАСТИОН)
Серьёзный инструмент
- 64 **Антифрод**
Василий Окулесский
(Банк «Возрождение»)
Эти разные лица
- 67 **Интеграция**
Дмитрий Слободенюк,
Алексей Курских (ARinteg)
Искусство выбирать
- 70 **IAM-системы**
Валерий Куликов (BIS Journal)
One Identity Manager разрешает взлёт
- 72 **Технологии**
Илья Осадчий (Тайгер Оптикс),
Владимир Соловьёв (ДиалогНаука)
Ханипоты и Deception
- 74 **Обзор**
Наталия Казанькова
(Positive Technologies)
Специально на вас
- 76 **Нормативная база**
Евгения Колодина,
Алексей Велякин (ЦИБИТ)
Разбираемся в Приказе ФСТЭК России №77
- 78 **Аппаратно-программные комплексы**
Дмитрий Ларин
(Гарда Технологии)
От Москвы до Владивостока
- 80 **Импортозамещение**
Михаил Иванов
(С-Терра СиЭсПи)
«С-Терра СиЭсПи»: сделано в России
- 82 **Технологии**
Владимир Ульянов (Zecurion)
ДСАР, кап, кап

ИНФРАСТРУКТУРА

- 84 Юбилей**
Александр Галицкий (ЭЛВИС-ПЛЮС)
ЭЛВИС-ПЛЮС — 30 лет!
- 88 Деловые мероприятия**
PKI-Форум Россия 2021
- 94 Деловые мероприятия**
Марк Новодачный (BIS Journal)
CyberPolygon 2021
- 96 Деловые мероприятия**
Николай Кольский (BIS Journal)
ИнфоТеКС ТехноФест Москва — 2021
- 98 Деловые мероприятия**
Валерий Куликов (BIS Journal)
Банки России — XXI век
- 99 Деловые мероприятия**
Павел Никифоров (BIS Journal)
BIS SUMMIT 2021
- 100 Мобильная связь**
Владимир Дрелихов,
Игорь Купалов-Ярополк (Институт точной
механики и вычислительной техники
им. С.А. Лебедева РАН)
Проект «Конус» в действии



ОБРАЗОВАНИЕ И КАРЬЕРА

- 105 Мероприятия**
Артём Зубков (ФСРБИТ),
Всеволод Былевский (BIS TV)
«И не поверится самим...»
- 108 Киберполигон**
Сергей Нейгер (Перспективный мониторинг)
Киберполигон AMPIRE
- 110 Обзор**
Марина Бродская (BIS Journal)
Приёмная кампания — 2021
- 112 Киберобзор ИноСМИ**
МГЛУ — BIS Journal: диалог друзей
- 116 Семинар**
Сергей Романовский (МГЛУ)
Внимание, «я» — жертва!

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

- 118 Безопасная разработка ПО**
Андрей Жаркевич (Антифишинг)
На одном языке
- 122 Осведомлённость**
Александр Дворянский (Infosecurity)
Цифровая гигиена: правила игры

СУБЪЕКТЫ

- 124 История**
Борис Столпаков (историк криптографии)
«Я военный связист, я тяну провода...»
- 130 История**
Дмитрий Ларин (историк криптографии)
«Тора! Тора! Тора!»
- 134 Компании**
Александр Агаков (QIWI)
QIWI для бизнеса
- 136 Заметки безопасника**
Александр Бодрик (BIS Journal)
Как стать сильнее благодаря атаке

SIM-КАРТЫ С ФУНКЦИЕЙ УКЭП

Минцифры планирует выпустить SIM-карты с чипами усиленной квалифицированной электронной подписи (УКЭП) — она позволяет предпринимателям подавать отчётность в ФНС, подключаться к portalу системы маркировки «Честный знак», участвовать в электронных торгах и т.д.

В настоящее время УКЭП устанавливается на компьютер, а токен хранится на USB-накопителе или смарт-карте.

SIM-карта с УКЭП разработана в Институте точной механики

и вычислительной техники РАН им. Лебедева. В планах производить 100–150 млн экземпляров в год, сообщил гендиректор учреждения Александр Князев. В новых «симках» будут использоваться российские криптографические алгоритмы; в действующих же применяется зарубежное шифрование.

В составе рабочей группы проекта — ФСБ, мобильные операторы и научные организации. Их представители обсуждают реализацию, сроки и требования к разработчику (от этого всего будет зависеть объём инвестиций операторов).



У БОГА ТЕПЕРЬ ДВА ГЛАЗА

Евгений Антипов, создатель заблокированного Роскомнадзором бота «Глаз Бога», запустит в этом месяце похожий сервис, но уже для бизнеса — «Мобиус». Он будет ориентирован на руководителей компаний, отделы кадров, отделы закупок и корпоративные службы безопасности.

«Мобиус» позволит проверять потенциальных сотрудников на нарушение закона или членство в подозрительных сообществах. Проверка контрагентов будет включать их финансовую отчётность, информацию об участии в судах, госзакупках и т.д.

Новый сервис собирается использовать более 30 источников. Среди них — данные «СПАРК-Интерфакса», базы налоговой, Росфинмониторинга, судебных приставов и база розыска МВД.

Каждый запрос будет стоить 1–3 рубля. Для подключения к самому

сервису нужно внести минимальный депозит — 15 тыс. рублей. Оценка проекта — 5 млн рублей (в основном это контракты с поставщиками информации).



FACEBOOK СНОВА ОБВИНИЛИ

Интеграция сквозного шифрования в мессенджеры Facebook может привести к усилению слежки за пользователями со стороны спецслужб, считает бывшая сотрудница соцсети Фрэнсис Хауген.

С её слов, после запуска новой фичи в Messenger и Instagram материнская компания лишится возможности выявлять «вредоносные операции представителей спецслужб».

«Сквозное шифрование позволит Facebook устраниваться от модерирования контента и послужит оправданием для бездействия», — заявила Хауген.

В руководстве Facebook с этим не согласны. Там отметили, что введение сквозного шифрования в указанных сервисах наоборот направлено на защиту конфиденциальности пользователей — эта функция оградит их не только от иностранного наблюдения, но и от хакеров.

ГОСУСЛУГИ «ПОУМНЕЮТ»

Минцифры планирует запустить «умное» приложение «Госуслуги» в следующем году, сообщил глава ведомства Максют Шадаев на заседании комитета Госдумы по информационной политике, ИТ и связи.

«В следующем году мы планируем запускать большой супер-апп — мобильное приложение «Госуслуги», которое должно полностью подстраиваться под профиль пользователя, предлагая те услуги, которые ему положены, и те, которые ему могут быть интересны. В этом смысле проактивное оказание услуг для нас очень важная часть», — рассказал он.

А в этом году, добавил министр, появится новая веб-версия: «Надеюсь, до конца года мы старую версию портала отключим. Там очень много новых возможностей технических. Всё ориентировано на то, чтобы пользователь максимально быстро мог найти нужную услугу, заполнить необходимое заявление, используя для этого минимальное количество кликов».

ВЕРНУТ УКРАДЕННОЕ

В кулуарах Московского финансового форума заместитель директора Департамента финансовой политики Минфина Алексей Яковлев рассказал, что готовится законопроект о механизме возврата похищенных мошенниками средств.

«Мы планируем в ближайшие два месяца внести его в правительство, чтобы оно уже в новый созыв Госдумы вынесло его на рассмотрение», — сказал он.

Со слов Яковлева, его ведомство рассчитывает, что новая практика позволит перехватить средства на том этапе, когда они ещё не были выведены на различные неподконтрольные счета.



БИОМЕТРИЮ АККРЕДИТУЮТ

Председатель Правительства Российской Федерации Михаил Мишустин подписал постановление об утверждении правил аккредитации организаций, обладающих биометрическими системами идентификации и аутентификации.

«Утвердить прилагаемые правила аккредитации организаций, владеющих информационными системами, обеспечивающими идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, и (или) оказывающих услуги по идентификации и (или) аутентификации с использованием биометрических персональных данных физических лиц», — гласит документ.

Аккредитация иностранных юрлиц, владеющих упомянутыми биометрическими системами, будет осуществляться с 1 марта следующего года. Сам документ вступает в силу с 1 января и будет действовать до начала 2028 года.

БАНКИ СТАНУТ БЛИЖЕ К НАРОДУ

Комитет Госдумы по финансовому рынку разрабатывает проект закона, обязывающего финансовые организации давать содержательные ответы на обращения потребителей (как это закреплено законом в отношении органов власти), сообщил глава комитета Анатолий Аксаков.

Есть мнение, что инициатива будет дисциплинировать банки, и финансовый рынок после её внедрения станет более прозрачным для пользователей. Однако, при этом важно оценить расходы для кредитных организаций, чтобы за нововведение не расплачивались их клиенты.

Руководитель проекта Народного фронта «За права заёмщиков» Евгения Лазарева отметила, что будет не лишним включить в ответы банков и рекомендации по эффективному решению проблемы: «На потенциальном заёмщике «висят» непогашенные обязательства, оформленные на него третьими лицами, о которых он не знал

или забыл. Было бы неплохо в таких ситуациях при отказе в оформлении кредита в его мотивационной части не только сообщать потребителю об этих фактах, но и рекомендовать проверить свою кредитную историю, завершить эти обязательства или сообщить в БКИ о существующей ошибке, исправить кредитную историю и обратиться к новому кредитору уже после этого».



ПО ТРЕБОВАНИЮ ФСИН

Мобильных операторов обяжут блокировать телефонные номера по требованию ФСИН в течение трёх суток, если они могут использоваться заключёнными для совершения

противоправных действий. Проект соответствующего постановления был внесён Минюстом.

«ФСИН России располагает информацией, что средства мобильной связи используются для оказания давления на свидетелей, координирования действий членов организованных преступных групп, находящихся на свободе, поставок запрещённых предметов, наркотических средств, а также в экстремистских целях», — сообщили авторы инициативы. Также в этот список добавляют преступления мошеннического характера.

Согласно предложенному Минюстом механизму, сотрудник ФСИН должен принять решение о необходимости блокировки номера в течение суток с момента обнаружения факта его незаконного использования и направить требование об отключении номера оператору связи. Операторы же по факту блокировки должны сообщить о ней не позднее, чем через 12 часов.



«ПОИГРАЕМ В КАЛЬМАРА?»

Эксперты из Proofpoint выявили новую вредоносную кампанию: хак-группа TA575 распространяет банковский троян Dridex с помощью писем на тему сериала от Netflix «Игра в кальмара». Атака происходит через SMS, соцсети, приложения для знакомств, мессенджеры, а также игры.

Тысячи сообщений отмечены такими фразами, как «Игра в кальмара» возвращается! Смотрите новый сезон раньше всех», «Приглашения клиента для доступа к новому сезону»,

«Предварительный просмотр тизеров нового сезона «Игры в кальмара» и т.д. В некоторых письмах потенциальной жертве предлагают роль в сериале, если она скачает и заполнит прикрепленный документ.

«Вложения представляют собой документы Microsoft Excel с макросами, которые при включении загружают партнёрский идентификатор банковского трояна Dridex 22203 из URL-адресов Discord», — пояснили в Proofpoint.



ДОБРАЛИСЬ ДО ОКЕАНИИ

Интегрированная система финансового управления (IFMS) Минфина Папуа — Новой Гвинеи подверглась атаке с использованием вымогательского ПО.

В результате оказались заблокированы сотни миллионов долларов иностранной помощи, и хакеры потребовали выкуп в биткойнах.

IFMS объединяет бюджет страны и отчетность для всех уровней и департаментов правительства, а также контролирует доступ властей к фондам. В системе нашлось несколько критических уязвимостей, которые и позволяют киберпреступникам взломать сети.

Известно, что департамент финансов сейчас занимается решением проблемы, но официальных комментариев не даёт.



АССОЦИАЦИЯ
БАНКОВ
РОССИИ

VII Банковская юридическая конференция

«Новые вызовы и возможности: регуляторные и правовые тенденции в банковской деятельности»

25-26 ноября 2021 года

Онлайн

Оргкомитет
Тел.: +7 (495) 785-29-93, +7 (495) 785-29-88
Электронная почта: event@asros.ru
asros.ru





Вадим КУЛИК
заместитель
президента-
председателя
правления ВТБ

«ВТБ — НЕ СТОЛЬКО ФАБРИКА ИИ, СКОЛЬКО НАУКА И ПРАКТИКА, КАК ЕДИНОЕ ЦЕЛОЕ»

НА ВОПРОСЫ BIS JOURNAL ОТВЕЧАЕТ
ЗАМЕСТИТЕЛЬ ПРЕЗИДЕНТА — ПРЕДСЕДАТЕЛЯ
ПРАВЛЕНИЯ ВТБ ВАДИМ КУЛИК

— Самое сложное — договоримся о терминах. Как вы относитесь к понятию и термину «Искусственный интеллект» (ИИ)? Как трактуют это понятие в ВТБ, какие термины используют?

— Для нас искусственный интеллект — набор технологий, который позволяет решать задачи за пределами возможностей бизнес-аналитики и классического программирования. В первую очередь технологии ИИ дают возможность понимать потребности наших клиентов на качественно новом уровне, быть максимально удобными для клиента, выстраивать партнёрства в части данных, быть операционно эффективными. Мы используем весь спектр направлений ИИ для этих задач — от компьютерного зрения и графовой аналитики до применения глубокого обучения в задачах оптимального размещения инфраструктуры банка. Важно отметить, что под ИИ в банке мы понимаем не только модели, которые без интеграции в бизнес-процесс не приносят ценности, но и весь жизненный цикл применения технологий ИИ: от данных и разработки модели до её внедрения и автоматического мониторинга качества.

— Где, на каких участках работы и в каких масштабах используют ИИ в ВТБ?

— ВТБ использует искусственный интеллект в большинстве процессов, в том числе при формировании предложений и принятии решений по кредитам, в голосовых помощниках, работе кол-центра, чат-ботах, в маркетинговых задачах. Технологии ИИ также применяются для распознавания и сегментации документов и защиты клиентов от мошенников. В рамках реализации цифровой трансформации ВТБ в 2020 году создал и запустил ИТ-платформу, которая позволяет унифицировать и упростить внедрение

технологий искусственного интеллекта в бизнес-процессы банка. В 2021 году ВТБ запустил в промышленную эксплуатацию новый продукт Фабрики искусственного интеллекта — систему управления моделями машинного обучения. Это ещё один этап в развитии и внедрении технологий искусственного интеллекта в бизнес-процессы банка. Кроме того, ВТБ одним из первых российских банков начал использовать искусственный интеллект при открытии и модернизации своих отделений и банкоматов. Банк разработал и внедрил модель машинного обучения, которая с помощью анализа Big Data позволяет прогнозировать спрос на банковские услуги в конкретных точках города. Реализация проекта позволит уменьшить среднее время доступности отделений ВТБ для клиента до 15 минут.

— Чей опыт по использованию ИИ ВТБ взял за основу своей модели?

— Крупные российские банки занимают передовые позиции в мире по применению и внутренней разработке ИИ-решений. В других странах драйверами такой разработки в финансовом секторе часто становятся финтех-компании, у нас же основной драйвер — крупнейшие игроки финансового рынка. Поэтому опыт ВТБ во многом уникален. Мы изначально ориентировались на централизацию функции ИИ в банке, в том числе с помощью создания специализированных платформ, которые позволяют эффективно применять ИИ в таких сложных областях, как геоаналитика, графовая аналитика, анализ неструктурированных и потоковых данных.

В этом плане мы похожи на крупнейшие мировые компании. Они также создают платформы, поддерживающие специализированные задачи ИИ, но не ограничивающие разработчиков в инструментах и области применения.

Уникальной особенностью в данном случае стала необходимость внедрения инноваций в условиях жёсткого банковского регулирования. Достичь баланса нам удалось за счёт централизованно выстроенного MLOps процесса (система управления моделями). Он поддерживает полный жизненный цикл моделей и обеспечивает как внедрение наиболее инновационных технологий, так и полное соответствие требованиям регулятора.

— **Какую пользу, эффект получает ВТБ от использования ИИ?**

— Все более-менее серьёзные игроки рынка так или иначе используют в процессах математические модели. Этим сегодня никого не удивить. При этом, чтобы выйти на принципиально новый уровень в условиях конкурентной борьбы за каждого клиента, необходим комплексный подход. Он предполагает, что ИИ становится частью повседневной реальности и пронизывает все без исключения бизнес-процессы и системы банка. Приоритет ВТБ — комфорт и удобство клиентов. Анализируя большое количество разнородных данных, мы лучше понимаем потребности потребителей, именно это позволяет постоянно улучшать клиентский опыт. Кроме того, ИИ позволяет снизить риски различной природы: от рисков мошенничества до операционных и технологических рисков.

— **Цена вопроса. Насколько выгодно использование ИИ в вашем банке?**

— Применение искусственного интеллекта в 2020 году позволило банку показать экономию в размере 1,2 млрд рублей.

— **Какие риски, проблемы наблюдаются (преодолены и ожидаются) от использования ИИ? Как они решаются?**

— Люди боятся, что их персональные данные станут доступны, им часто звонят злоумышленники. В этом мало приятного, и очень бы хотелось, чтобы крупные индустриальные игроки предпринимали какие-то действия. Сами игроки понимают, что новый этап конкуренции связан с производством продуктов на основе ИИ, требующих как можно больше различных классов Big Data. Получается противоречие: большой объём Big Data даёт возможность лучших предсказаний, но при этом растут риски. Власти начинают это регулировать, тем самым сдерживается прогресс. Такова общемировая тенденция.

На этом фоне стали появляться технологии, которые позволяют сохранить конфиденциальность первичных данных и при этом — после

По прогнозам экспертов, глобальный рынок решений в области ИИ будет расти на 40 % в год и к 2025 году составит более 300 млрд долларов. Этот глобальный тренд в полной мере ощущается и внутри банка

проведения определённых манипуляций — строить на них модели. Например, технология Data Fusion, где нейросеть «оборачивает» первичные данные, чтобы они были обрабатываемы для предсказательных моделей, но в то же время их дешифровка была бы практически невозможна. Такая технология отвечает интересам государств и физических лиц и позволяет корпорациям развиваться.

К примеру, мы уже провели тестирование технологии MPC (Multiparty computation) в рамках совместного мероприятия ВТБ и Ростелекома «Платформа больших данных». Особенность технологии MPC в отсутствии обмена исходными данными между компаниями: это даёт возможность пользователям сервиса реализовать подход Data Fusion.

— **Существует ли проблема кадров в сфере ИИ? Как она решается?**

— По прогнозам экспертов, глобальный рынок решений в области ИИ будет расти на 40 % в год и к 2025 году составит более 300 млрд долларов.

Этот глобальный тренд в полной мере ощущается и внутри банка. Сферы применения ИИ увеличиваются с огромной скоростью. Идёт активный процесс технологического замещения, который, в свою очередь, требует найма большого количества высококвалифицированных специалистов в этой области. Причём речь идёт не только о data science — командах, а также о специалистах по таким направлениям, как обработка/хранение/подготовка данных (data engineers), разработка/построение эффективной и надёжной CI/CD-инфраструктуры для внедрения алгоритмов ИИ и автоматизация рабочих процессов (DEV OPS, CI/CD, ML engineers).

На рынке труда наблюдается дефицит специалистов в области машинного обучения и ИИ. Финансовые институты и финтех-компании находятся в активной конкуренции за высококвалифицированные кадры. Мы не ожидаем изменения данной тенденции в течение ближайших лет. Одним из решений данной проблемы может

быть разработка внутренних программ обучения новых талантливых сотрудников для повышения их квалификации.

— **Насколько правильно работает ваш ИИ? Как влияет на внутреннюю операционную устойчивость организации на разных участках и в целом?**

— В банке действует система внутреннего контроля, которая опирается на концепцию трёх линий защиты, в том числе для управления модельным риском ИИ. Первая линия — это непосредственно разработчики моделей, вторая — независимое подразделение валидации и управления модельным риском, осуществляющее независимый контроль и проверку разработанных моделей ИИ, третья линия — независимое подразделение внутреннего аудита, контролирующее соблюдение внутренних стандартов со стороны первой и второй линии защиты. Правильность работы моделей ИИ помогает отслеживать действующая автоматизированная система мониторинга моделей, внутренний учёт разработанных моделей ведётся в системе управления моделями, а правила и процесс взаимодействия подразделений регламентируются утверждённым стандартным жизненным циклом моделей. Модельный риск использования ИИ не оказывает значимого влияния на операционную устойчивость организации в силу действующих организационно-технологических мер по управлению модельным риском.

— **Какие нейросети используются в ваших системах?**

— Мы уделяем большое внимание совершенствованию используемых практик в сфере машинного обучения (machine learning) и глубокого обучения (deep learning), так как часто даже небольшое улучшение в качестве используемых моделей приносит существенный финансовый эффект. Специалисты регулярно изучают лучшие международные практики, принимают участие в конференциях, обмениваются опытом. Важно, что для создания коллаборации между научным сообществом и практиками data science в 2021 году была создана международная площадка — конференция Data Fusion.

Непосредственно нейронные сети используются для анализа транзакций, для поддержания диалога с клиентом в голосовом ассистенте, анализа графов и создания рекомендаций. В настоящее время активно развиваются решения на основании компьютерного зрения (Computer Vision) для верификации пользователей, контроля и регулирования деятельности

дополнительного офиса и борьбы с мошенниками. При выборе архитектуры нейронных сетей в ряде случаев мы используем разработанное нами совместно с научным сообществом решение по нейронному поиску архитектур (Neural Architecture Search), которое позволяет рассматривать большее количество архитектур нейронных сетей и ускоряет поиск наиболее подходящей. Пока это применимо в основном к рекуррентным и полносвязанным архитектурам, в дальнейшем планируем распространить это решение и на сверточные сети.

— **Какие перспективы для ИИ в ВТБ вы видите? Какие новые шаги планируете?**

— Мы активно работаем над совмещением науки и практики, считаем это направление перспективным. В апреле ВТБ и Московский физико-технологический институт (МФТИ) договорились об открытии на базе МФТИ совместной лаборатории, цели которой: развитие технологий Big Data, искусственного интеллекта в банках, содействие научно-исследовательской деятельности и поддержка профессиональных кадров. Банк совместно с МФТИ создаёт прикладные разработки приложений и сервисов распознавания речи для улучшения клиентской поддержки ВТБ. Ещё одним направлением совместной работы в новой лаборатории являются исследования и проекты в области определения психоэмоционального состояния персонала банка с помощью нейросетей. Кроме того, ВТБ и МФТИ будут разрабатывать математические модели для повышения эффективности работы банка, а также технологии для бизнес-партнёров ВТБ.

— **Видите ли вы конкурентов в сфере ИИ? Или, наоборот, считаете, что в этой сфере необходимо делиться опытом и двигаться вперёд сообща?**

— С точки зрения развития ИИ как фундаментальной науки, безусловно, необходима кооперация специалистов. При этом практическое применение технологий ИИ часто связано с конкуренцией, что усложняет кооперацию.

— **Как обеспечивается информационная безопасность при использовании ИИ?**

— На текущем этапе развития ИИ не способен выходить за рамки запрограммированной в нём аксиоматики, определяющей в числе прочего и стратегию его самообучения. Поэтому в настоящее время автоматизированные системы, использующие технологию ИИ, укладываются в классическое определение: система,



состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций. Соответственно, для обеспечения информационной безопасности при использовании ИИ необходимо проводить стандартные мероприятия. В том числе идентифицировать уязвимости, противодействовать угрозам, минимизировать возможные последствия реализации угроз, руководствоваться известными принципами защиты. Среди них: комплексность, системность, адекватность, проактивность, минимизация полномочий, наличие нескольких эшелонов защиты и т.д.

— Существуют ли особые, специфические проблемы информационной безопасности при использовании ИИ?

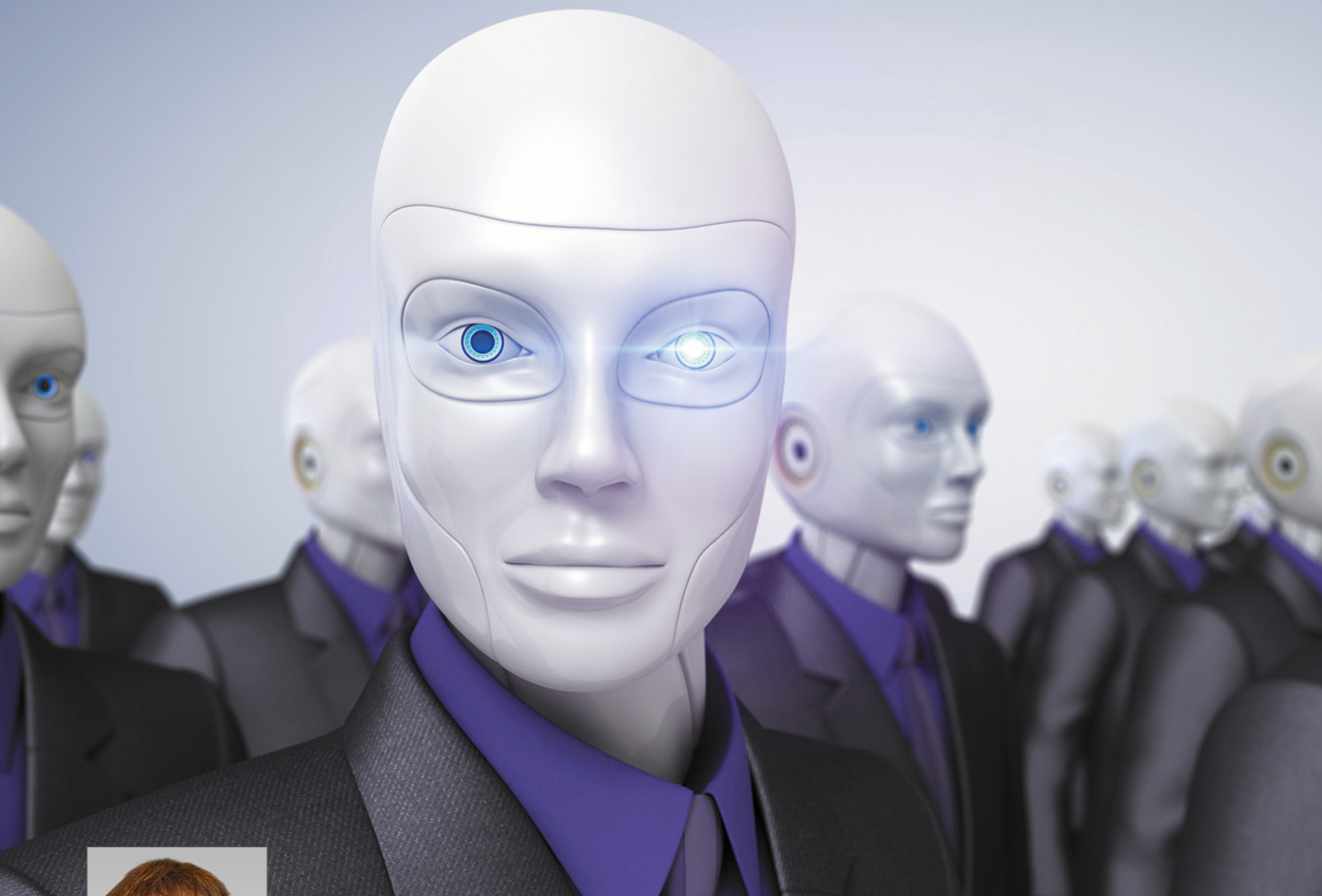
— Да, определённая специфика всё же есть. Например, Data Science — аналитикам для выполнения работ требуется доступ к максимально большому и заранее не определённому объёму данных, а разработка и тестирование моделей машинного обучения проводится, как правило, на реальных данных. При этом необходима установка и использование широкого спектра

современных средств разработки. В таких условиях для снижения рисков информационной безопасности требуется создание отдельных специализированных промышленных сред с особым режимом информационной безопасности.

— Как используется ИИ в работе службы информационной безопасности ВТБ?

— Безопасность данных и средств клиентов — приоритет для ВТБ, банк постоянно совершенствует методы защиты. Например, недавно ВТБ внедрил новую модель на основе искусственного интеллекта для предотвращения мошеннических операций по картам: обученный на более чем 10 тысячах параметров алгоритм машинного обучения выявляет в 1,5 раза больше попыток злоумышленников совершить мошеннические операции по сравнению с ранее действовавшими системами.

Разработанная специалистами ВТБ модель за несколько миллисекунд на основании всех доступных массивов Big Data анализирует операцию и при обнаружении потенциальной опасности направляет клиенту дополнительное уведомление о необходимости дополнительного подтверждения.



Елена
ПОКАТАЕВА
обозреватель
BIS Journal

КУДА СТРЕМИТСЯ «УМНОЕ» СТАДО?

КОЛИЧЕСТВО ПЕРЕХОДИТ В КАЧЕСТВО.
ОБЗОР СФЕР ПРИМЕНЕНИЯ ИИ В БАНКАХ

На первый взгляд, искусственный интеллект (ИИ) заполнил все этажи и закоулки цифрового пространства современного банка. Но это только часть истины — неутомимые механизмы ИИ, и правда, занимаются самыми разными задачами. Другая часть правды в том, что — по аналогии с «зоопарком» программно-аппаратных комплексов — сегодня можно говорить о «зоопарке» умных программ... со всеми вытекающими.

Например, в этом «зверинце» обитает немало «хищников», пожирающих гигабайты оперативной памяти, MIPSы вычислительной мощности и ресурсы дорогостоящих команд ИТ-специалистов. Так что нынешний хайп на тему ИИ в итоге уходит в плоскость оптимизации инвестиций и грамотного управления ИИ-зоопарком. Как выглядит с этой точки зрения эволюция интеллектуальных систем, работающих в российских банках?



МАШИННЫЙ ИНТЕЛЛЕКТ: БЫСТРЕЕ И ЛУЧШЕ ЧЕЛОВЕКА

Банки осуществляют свой бизнес в условиях жесткой конкуренции с финтехом. «Банкам необходимо очень постараться, чтобы достичь скорости, маневренности и гибкости, присущих их конкурентам — финтех-компаниям», — говорит Тимур Аитов, зампреда комитета ТПП по финансовому рынку и кредитным организациям. В этих условиях банки стараются с помощью ИИ поставить на службу бизнесу всю мощь данных, имеющихся во внутренних и внешних источниках. В первую очередь, ИИ внедряется на тех участках, где он справляется с теми или иными задачами очевидно быстрее или лучше человека. Так, системы на базе ИИ помогают управлять персоналом, лояльностью клиентов, маркетинговыми программами, бороться с внутренними и внешними угрозами.

Умный HR. Чаще всего ИИ используют для ускорения и оптимизации поиска персонала

за счет автоматического анализа и первичного отбора резюме. «Также технологии машинного обучения внедряются в WFM (Work Force Management) — системы управления персоналом, которые позволяют прогнозировать как общее число сотрудников, так и их наличие в конкретный момент в офисе или контакт-центре», — говорит Василий Кузь, директор по решениям для банков компании КРОК. Перспективное направление — Human Capital Management (HCM), системы управления человеческим капиталом, позволяющие выявлять особенности и аномалии рабочих процессов, влияющих на текучку кадров, эффективность работы сотрудников, а также формировать кадровый резерв.

«Удаленка» вызвала устойчивый интерес компаний к ИТ-системам, способным наблюдать за работой персонала «издалека». От таких систем ожидается двойной эффект — эффект «надсмотрщика», способного учитывать полезную активность сотрудников, и эффект защиты от «надомника-злоумышленника». Например, системный администратор через специальные приложения получает контроль над корпоративной сетью: видит все запускаемые программы, открытые окна и при необходимости блокирует опасные ресурсы.

В контактных центрах. Для передовых контактных центров, в которых реализовано омниканальное обслуживание клиентов, технологии распознавания естественного языка распространяются на все каналы коммуникаций операторов и клиентов: переписку по электронной почте и в мессенджерах, сообщения на корпоративных сайтах, форумах, в соцсетях. К классическому функционалу выявления позитива/негатива в высказываниях клиентов добавилось распознавание их тематики, выявление ключевых особенностей обращений и выбор сотрудника, который должен вступить в коммуникацию с клиентом.

Рядом с живыми операторами трудятся голосовые помощники. Эти «сотрудники» берут на себя рутинные функции дозвона и информирования клиентов. Поддержать разговор в «человеческом» стиле они пока не способны. Виртуального помощника, как и человека-оператора, нужно постоянно обучать, контролировать его работу и при необходимости вносить коррективы, а для этого необходимы существенные ресурсы.

Видеоаналитика. Технологии распознавания лиц помогают банкам контролировать доступ сотрудников и клиентов в помещения банков, управлять очередями в офисах. Они умеют выявлять VIP-персон, обеспечивая им спецобслуживание, а также мошенников, чьи фото есть в базе данных. Технологии позволяют идентифицировать пол человека, возраст и даже настроение. При

этом наличие маски на лице не снижает точности распознавания, равно как и попытки человека изменить внешность, надев парик, шапку, очки или накладную бороду. Умная видеоаналитика умеет выявлять нетипичное поведение: попытку взлома банкомата, оружие в руках посетителя и т.д.

Яркая примета дня — биометрия. На старте активного роста — биоэквайринг — оплата покупок не картой, а лицом, обращенным к видеокамере. Однако достоинствам сопутствуют и риски: биометрические атаки — уже реальность, и Liveness-верификация — подтверждение, что виртуальный собеседник — живой человек, а не его фотография, становится частью банковских услуг.

Внутреннее мошенничество. Инструментов контроля неправомерных действий сотрудников сегодня масса: от обычных видеокамер до решений, определяющих, с какого рабочего места «убежал» конфиденциальный документ. Такой контроль включает мониторинг потенциально опасных действий: подключение USB-устройств, факты печати на принтере, перехваты буфера обмена, мониторинг конфигурируемых лог-файлов и т.п. Подобные задачи лежат в области моделирования работы пользователей на основании их типичного поведения. Существенные изменения таких моделей — повод для сигнала службе безопасности.

Много полезного для борьбы с инсайдом находится в том, что называется цифровыми следами. Если наложить на них процессную аналитику (Process mining), можно выявить аномальные действия сотрудников, клиентов и даже их сговор. Для фрод-менеджмента используются и данные из внешних открытых источников, например, с помощью OSINT (Open Source Intelligence).

Интеллект клиентского опыта. Умные программные решения ведут банковские услуги к тотальной персонификации: предложения для клиента уже формируются с учетом местоположения и прочих значимых характеристик текущей ситуации. «Скоро банки смогут сегментировать аудиторию до одного физического лица», — считают эксперты.

Также, стимулируя лояльность корпоративного клиента, банки с помощью ИИ активно вторгаются на его территорию, например, анализируют его бизнес-связи и рекомендуют новых контрагентов. Для клиентов из малого бизнеса моделируют финансовые риски (дефолт, кассовый разрыв) в режиме реального времени и рекомендуют целевые стратегии и банковские продукты.

ИИ для маркетинга. Заменить человека на творческом этапе «придумывания» новых

маркетинговых программ ИИ не способен. Однако он может взять на себя часть рутины. Например, подготовить базу данных потенциальных клиентов или создать по заданному шаблону текст рекламного сообщения и иллюстрацию к нему — эти задачи сегодня уже поддаются автоматизации.

Передовые ИТ-решения поддерживают прогностическую аналитику — с их помощью можно просчитать варианты исхода задуманной маркетинговой программы. «На основании выявленных закономерностей по статистическим данным, не заметным человеку, ИИ показывает, насколько то или иное решение банка оптимально для разных категорий клиентов. Человеческий потенциал в этом вопросе уже достиг максимума, а цифровые решения способны обрабатывать и анализировать гораздо больше информации и делать это на порядок быстрее и качественнее.

Информационная безопасность. Настоящее и будущее ИБ банков однозначно связано с интеллектуальными решениями. Факт применения злоумышленниками ИИ для формирования новых атак требует адекватного ответа. Сегодня классические решения ИБ модернизируются и дополняются ИИ для более эффективной защиты. Это уже произошло с сетевой защитой, решениями для защиты конечных устройств и защитой баз данных. В средствах защиты ИИ, в первую очередь, позволяет минимизировать ложные срабатывания, делая акцент только на реальных инцидентах. Кроме того, сегодня взаимодействие пользователей с банковскими сервисами порождает огромный поток метаданных, и лишь ИИ способен анализировать и выявлять в нем аномалии.

По мнению Сергея Войнова, генерального директора компании EveryTag, ключевое направление развития ИБ-решений — продукты верхнего уровня, которые охватывают разные системы мониторинга, агрегируют сигналы от разных систем, выявляют закономерности и формируют прогнозы в стиле: что происходит? Он уверен, что корпоративный мир уходит от нынешней «лоскутной ИБ-информатизации» в сторону комплексных сервисов, которые будут обеспечивать и надежное хранение документов (и др. информации), и безопасность цифровых активов.

КРЕДИТНЫЙ СКОРИНГ: ИИ НА СЛУЖБЕ

Согласно отчету Банка России за 2020 г., кредитный риск оставался для банков преобладающим. В связи с пандемией снизились доходы



населения и многих компаний. Увеличение кредитных рисков для банков отразилось в росте расходов на резервы по кредитам и прочим активам на 52%: до 1,2 трлн руб. в 2020 г., по сравнению с 0,8 трлн руб. в 2019 г. Эти тренды повысили внимание банков к вопросам оценки заемщиков.

Стремление к автоматизации проверок заемщика. Скоринговая система с высоким уровнем автоматизации позволяет перевести клиента из «серой» зоны ручных проверок в «белую», пояснил Дмитрий Фомичев, замначальника Департамента рисков розничного бизнеса «Газпромбанка». Он рассказал, что в ходе трансформации розничного бизнеса, которая началась в банке в 2018 г., доля автоматических проверок (с временем принятия решения до 5 мин.) увеличилась в 9 раз. Однако повышение уровня автоматизации проверок сопровождается усложнением скоринговой модели, а значит, нарастанием модельных рисков и «черной» зоны скоринга.

Поиск идеальной модели скоринга в нейросетях. Скоринговые модели на базе ML видятся перспективными: в них можно включать множество признаков и при этом не требуется детально прописывать взаимосвязи между ними в процессе принятия решений. Счет параметров в ML-модели уже идет на тысячи. Например, компания Mobile Scoring рассчитывает баллы с помощью 3,5 тыс. параметров заемщика.

При создании больших нейросетевых моделей в ход идет разнообразная информация, получаемая из коммерческих баз данных, публикаций в СМИ, слухов в соцсетях. Источниками

служат данные с бирж, занимающихся продажей cookie, ведь в них собраны все интересы клиента банка, его поисковые запросы и многое другое. С помощью этих данных ИИ может, например, выяснить, что заемщик — постоянный клиент онлайн-казино. Отличный источник — сведения из банковской экосистемы: доставка продуктов, заказы такси, интернет-покупки, увлечения, состав семьи... Такие сведения можно приобрести на рынке либо использовать OSINT-систему. Причем, информация часто предоставляется уже в размеченном виде, пригодном для обработки.

Также повышается роль госисточников данных, отмечает Дмитрий Фомичев. Доступность данных о доходах клиентов из этих источников способна кардинально поменять скоринговую модель, полагает он: «Для банка уже не будет иметь значения, зарплатный это клиент или нет. И это новый вызов для банков».

Однако ML-модели пока еще не годятся на роль идеального скоринга. «Нейросетевые модели не обладают явными преимуществами перед статистическими моделями, но способны моделировать сложные нелинейные взаимосвязи факторов», — отмечает Никита Лукашевич, замдиректора Института промышленного менеджмента С.-Петербургского политехнического университета. При этом они сложны в настройке и не позволяют извлекать из данных знания. К тому же ModelOps — управление жизненным циклом ML-моделей, как оказалось, таит немало «подводных камней»: от деградации качества работы моделей до большого количества

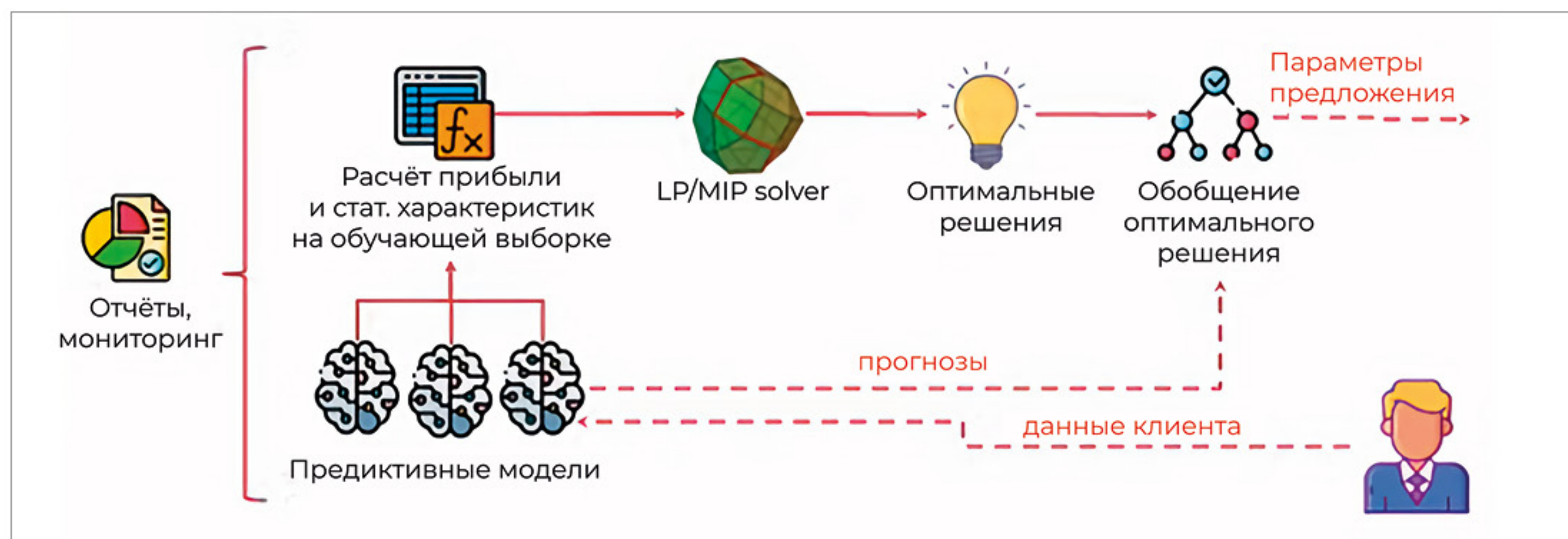


Рисунок 1.
Архитектура гибридного скорингового ИИ-решения «Хоум Кредит Банк».
Источник: Хоум Кредит Банк, сентябрь, 2021 г.

«разномастных» команд дата-сайентистов, действующих в разных бизнес-направлениях. «Это настоящее «лоскутное одеяло», состоящее из «кусочков» разных ML-инструментов: от Python до SAS», — говорит Павел Николаев, управляющий директор департамента интегрированных рисков банка «Открытие».

Такая ситуация обуславливает существенный модельный риск: в связи с одновременной работой большого количества моделей возможны сбои, которые невозможно выявить и отработать вручную. Есть и еще более серьезный недостаток — непрозрачность получения результата работы нейронной сети.

Поиск гибридных ИИ-моделей оптимизации скоринговых процедур. Просматривается два выхода из сложившейся ситуации. Первый — дальнейшие исследования для формирования правил влияния параметров настройки нейросети на точность классификации заемщиков. Второй — интеграция методов ML с другими технологиями ИИ для получения объяснимых результатов работы нейросетей. Такая интеграция, по мнению Юрия Визильтера, начальника подразделения интеллектуального анализа данных и технического зрения ГосНИИ Авиационных систем, может реализоваться двумя способами. Во-первых, получение с помощью ML различных эвристик, способных повышать эффективность систем логического вывода при решении конкретных классов задач. Во-вторых, глубокие нейросети, обрабатывающие символическую информацию, начинают работать под управлением предметных и общих онтологических описаний предметной области.

Михаил Дудалев, начальник отдела анализа данных в компании «Фаззи Лоджик Лабс», отмечает, что для задач построения сложных связей между многими сущностями, которые необходимы системам ИИ/ML, сегодня активно используется аппарат графовых нейронных сетей (Graph

Neural Network, GNN). По сути, графовые нейросети — это способ применения классических моделей нейронных сетей к данным в виде графов.

«Хоум Кредит Банк» реализовал свой вариант гибридного ИИ в сфере розничного кредитования и смог в результате добиться оптимизации кредитного решения. Как рассказал Сергей Герасимов, начальник отдела исследований и инноваций «Хоум Кредит Банка», система оценки заемщика включает предиктивное моделирование, каузальное моделирование (предполагает некоторое воздействие на клиента), обучение с подкреплением и алгоритмы линейного дискретного программирования. При этом в основе анализа лежит скоринговая карта, формирующая Probability of Default (PD), а также используются эвристики, связанные с ценообразованием и лимитной политикой (для них также используются специальные модели). В результате реализуется процесс оценки с максимизацией прибыльности заявок.

«Таким образом, создается результирующая модель, которая является результатом работы нескольких других моделей, и при этом она решает задачу оптимизации по различным параметрам», — поясняет Сергей Герасимов. Причем, реализован сложный вариант оптимизации на основе агрегированных (глобальных) показателей по всем клиентам (рис. 1).

Эксперт отметил интересный результат работы такой модели — снижение конверсии: «Брать кредиты стали действительно меньше, но предложения клиентам стали гораздо более выгодными для банка за счет персонализации».

ИИ ВМЕСТО ЧЕЛОВЕКА?

Современный банк — это цифровой сервис. Коммуникация с ним происходит не в формате человек — человек, а в формате человек — приложение. Чем выше уровень автоматизации



процессов и глубже межсервисные интеграции, тем эффективнее и рентабельнее банковское приложение. Это, в частности, объясняет, почему рынок программных роботов (RPA, Robotic Process Automation) «взлетел» несколько лет назад.

Цифровая рабочая сила. Оценки темпов роста рынка RPA в ближайшие годы разнятся, но не очень: Grand View Research прогнозирует рост в глобальном масштабе более чем на 40% до 2027 г., Impact — 31,1% до 2025 г.

Сегодня роботы несут службу в бухгалтерии, успешно справляются с обработкой кредитных заявок и открывают расчетные счета юрлиц, занимаются закупочной деятельностью, работают в HR-департаменте и клиентской службе. Они успели развить недюжинные способности: обрабатывают информацию из любых источников в едином потоке — фото с мобильного устройства, документ из сканера, скриншот с экрана планшета, тексты из социальных сетей и т.д. — и извлекают информацию, необходимую для принятия решений, с помощью технологий обработки текстов на естественном языке (рис. 2).

В целом, нынешние RPA хорошо справляются с задачами сбора данных, например, для KYC, и всяческими массовыми проверками документов различных типов. Но главный тренд развития RPA, по оценкам аналитиков «Делойт», заключается в их переходе на уровень интеллектуальной автоматизации процессов (Intelligence Process Automation, IPA), который отличается

возможностями сквозной автоматизации. «Автоматизация умных процессов позволяет составлять цепочки из программных модулей, которые запускаются в работу в конкретных точках бизнес-процессов», — поясняет Антон Ермаков, руководитель группы цифровых инициатив компании Comindware. Именно поэтому, добавляет он, сегодня так популярны технологии RPA, ведь они позволяют «склеивать» внутренние и внешние приложения, а также микросервисную архитектуру, которая позволяет уйти от монолитных приложений в ИТ-архитектуре.

Очевидно, что по мере продвижения от базовых RPA к IPA стираются грани между RPA, управлением бизнес-процессами (BPM) и гиперавтоматизацией (автоматизацией в формате комплексных сквозных процессов). На этом уровне появляются также решения интеллектуального анализа процессов Process Mining и аналитические возможности, позволяющие реализовывать нетривиальные RPA. Соответственно происходит трансформация набора автономных RPA в новую сущность — «цифровая рабочая сила».

Главный барьер, препятствующий успешному переходу RPA на этот уровень, как полагает Антон Ермаков, связан с порядком в бизнес-процессах организации: если его нет, то невозможно и четко сформулировать задачу для интеллектуальных систем RPA. Недооценка этого фактора приводит к тому, что даже сегодня 30–50% проектов RPA с элементами ИИ терпят неудачу (данные Ernst&Young).

Рисунок 2. Примеры банковских процессов, которые могут оптимизировать программные роботы. Источник: GmCS, март 2019 г.

ИИ в принятии бизнес-решений. В ближайшее время все отчетливее будет проявляться кризис традиционных бизнес-моделей: уходят в прошлое линейки банковских продуктов, а их место занимают компоненты в виде приложений, которые клиент подбирает самостоятельно в соответствии со своими потребностями. Но уже видны вешки дальнейшего — «встроенные» (embedded) финансы, способные встраивать платежи, дебетовые карты, кредиты, страховки и инвестиционные инструменты практически в любые нефинансовые продукты.

Этому состоянию финансовых информационных систем соответствует максимальная автоматизация бизнес-процессов, стремящаяся свести к нулю участие в них человека, в том числе, при принятии бизнес-решений. Так, в ВТБ, по словам вице-президента Вадима Кулика, на модели с применением технологий ИИ приходится до 70% задач аналитики и автоматического принятия решений. Артем Гришковский, коммерческий директор компании «Доверенная среда», полагает, что такие пропорции не случайны: именно решения ВІ станут в ближайшем будущем основой корпоративной автоматизации. И это случится, когда аналитический отдел перестанет работать как фабрика по производству отчетов, считает Юрий Сирота, старший вице-президент банка УРА ЛСИБ, и перейдет от сегодняшнего ретроспективного взгляда в прошлое к решениям, которые будут помогать создавать картину будущего.

Юрий Сирота отделяет предиктивную аналитику (прогноз будущего состояния) от предпринимательской аналитики, которая показывает наиболее выгодный путь к достижению будущего состояния. Это самый сложный в реализации вариант аналитической системы, но одновременно и самый мощный, ведь, по сути, ее результатом является цепочка управляющих воздействий. Теоретически уже просматриваются очертания того, каким образом результаты ВІ могут встраиваться в бизнес-процессы, обеспечивая сквозную автоматизацию с учетом текущих данных аналитики: необходимо внедрить инструменты рекомендательной аналитики и сформировать экспертную базу знаний процессов и принятия решений по различным событиям. «В этом случае можно будет сделать из ВІ программного робота, к чему, собственно, рано или поздно придет эволюция ВІ», — полагает Артем Гришковский.

ИИ не сделает офисы безлюдными. В представлениях аналитиков Gartner один из базовых элементов гиперавтоматизации — это люди, работающие на своих рабочих местах в рамках определенных рабочих процессов.

На первый взгляд, это звучит парадоксально: в эпоху усиливающейся тотальной автоматизации возрастает роль человеческого фактора? Парадокса нет, если вспомнить о растущей популярности Low-code подхода в реализации различных информационных систем корпоративного уровня: BPM, CRM, BI и т.д. «В том будущем, в которое мы все сейчас движемся, ИТ-комплексам смогут управлять сами бизнес-пользователи без привлечения профессионалов из ИТ-департамента», — говорит Антон Ермаков из Comindware. И, конечно, никакие умные ВІ-технологии не смогут полностью заменить профессионального аналитика. Более того, обеспечивая его умными вспомогательными инструментами, эти технологии устанавливают новую планку качества работы аналитика: не просто отвечать на поставленные вопросы, анализируя имеющиеся данные, а генерировать новые нетривиальные знания и предложения по их использованию на благо компании.

ВОПРОСЫ ВЕРЫ И СЕМАНТИКИ

Промежуточный технологический предел сложности задач, которые ИИ способен решать вместе с человеком, на сегодня достигнут. «Пока нет возможностей создать интерпретируемый и «доверенный» ИИ, то есть такую систему, которая даже для сложных моделей может гарантировать, что не будет странных проблем с необычными кейсами, и все результаты можно объяснить человеку», — говорит Михаил Дудалев. Тимур Аитов добавляет: «Хотя банки активно используют ИИ для решения многих аналитических задач, никто не сможет на 100% гарантировать истинность результатов анализа ИИ. Нельзя, например, утверждать наверняка, что ИИ не пропустил кредитную заявку мошенника, содержащую специально подобранный набор параметров. Искусственному интеллекту (и в искусственный интеллект!) в этом смысле банкам сегодня остается только верить».

Логично возникает необходимость четкого распределения ролей человека и программного помощника. Доверять ли на 100% рекомендациям ИИ или перепроверять их, фактически дублировать с помощью человеческого интеллекта? Первый вариант дешевле при масштабных внедрениях, а второй дает более точный результат. В этом, похоже, и будет состоять главная проблема «этики ИИ» в ближайшие годы: быстро, дешево или точно?

На практическом уровне мир ИИ-решений буквально на наших глазах шагнул далеко вперед, но у них осталось «родимое пятно» начального этапа — узконишевый характер. Нужно

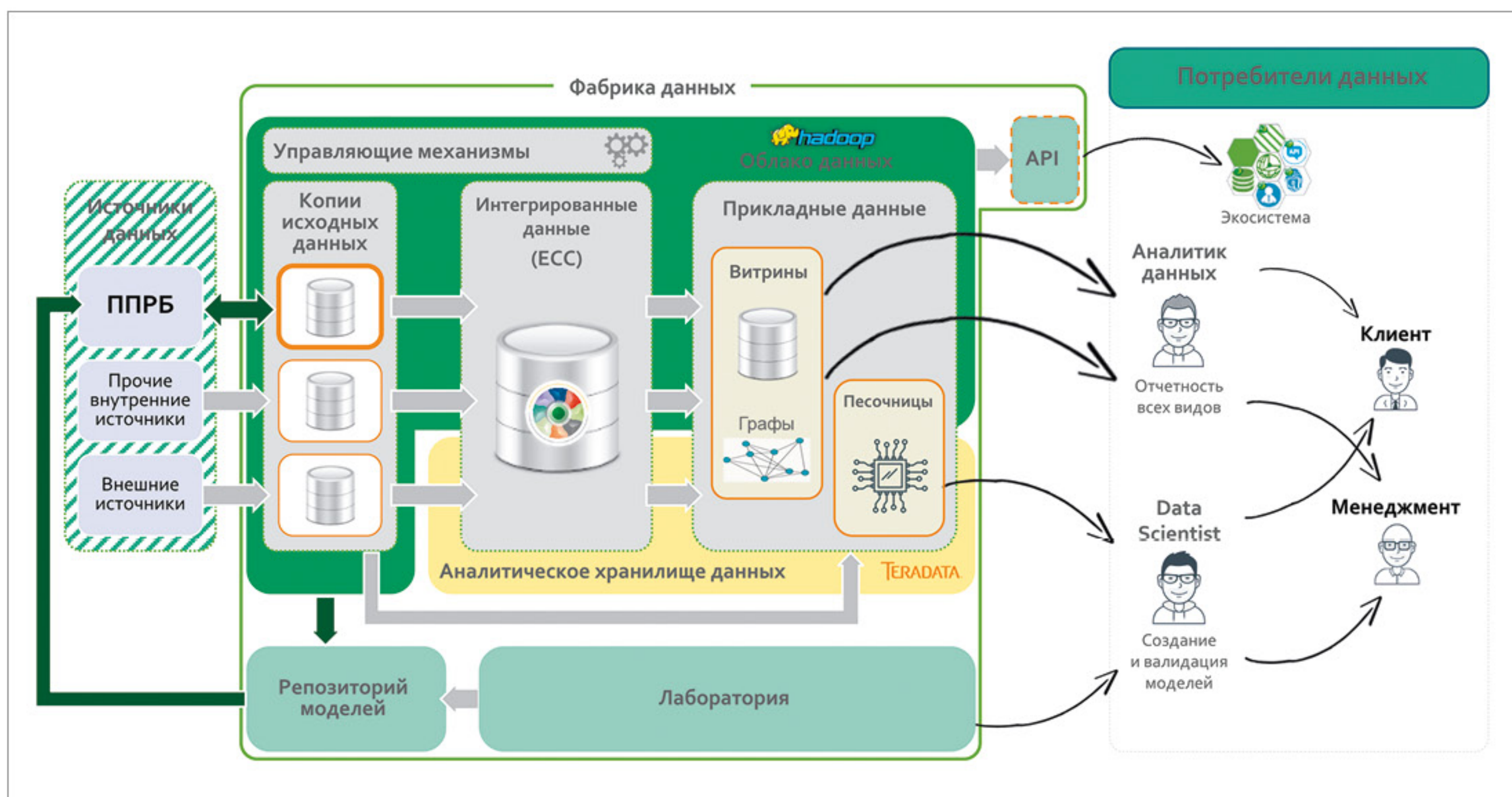


Рисунок 3. Архитектура Фабрики данных Сбербанка. Источник: Сбербанк, 2018 г.

констатировать: период экстенсивного развития узких ИИ-решений в банках завершился, настало время «собирать камни», то есть превращать множество разнородных BI-решений, моделей — ML/DL, логических (основанных на правилах), статистических и проч. — в единое пространство поддержки принятия решений специалистами банка.

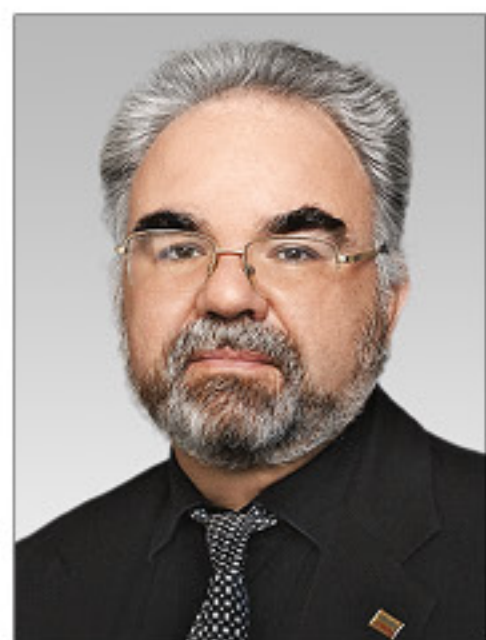
Фактически речь идет о задаче ситуационного управления, поддержки принятия решений в рамках единой платформы, что подразумевает модернизацию системной архитектуры и корпоративного хранилища данных. О трендах трансформации хранилищ можно судить, например, по опыту «Облака Данных» Сбербанка — Big Data кластера на базе Apache Hadoop, который поддерживает, в том числе, инкрементальную загрузку данных из высоконагруженных банковских систем на уровне нескольких десятков терабайт в сутки. Для эффективного управления этими процессами создается Единый семантический слой (ЕСС), базирующийся на «Корпоративной Модели Данных» — логической модели данных банка. Таким образом, основная задача ЕСС — отделить потребителя от «сырых» данных и предоставить единый способ

доступа к интегрированным, непротиворечивым и качественным данным из ЕСС, понятным бизнес-пользователям.

Семантическое содержание данных ЕСС упрощает интегрированную обработку данных, обеспечивает прозрачность и объяснимость всех операций с данными, переводя их в плоскость манипуляций с именованными сущностями (рис. 3).

Переход к семантическим описаниям структуры корпоративных данных логичен, ведь ключевым элементом ИТ-архитектуры становятся не сами данные, а их семантическая (содержательная) модель.

Таким образом, интеллектуальные методы и подходы к обработке корпоративных данных перемещаются с уровня прикладных решений вглубь цифровой инфраструктуры компании — там будет создаваться интеллектуальный фундамент корпоративных информационных систем. Это новый этап цифровой трансформации, к которому финансовая отрасль, как, впрочем, и все остальные, еще только подходит.



**Алексей
ЛУКАЦКИЙ**
бизнес-консультант
по безопасности
Cisco Systems,
эксперт BIS Journal

ЧТО НАДО ЗНАТЬ

ЕСЛИ ВЫ РЕШИЛИ ПРИМЕНИТЬ МАШИННОЕ ОБУЧЕНИЕ ПРИ МОНИТОРИНГЕ УГРОЗ

Существует два основных подхода при обнаружении угроз — сигнатурный и «аномальный». В первом случае мы начинаем с моделирования плохого поведения, а затем сравниваем с ним, ища совпадения в сетевом трафике, в журналах событий, в поведении процессов и т.п. При данном подходе очень важно заранее знать, что такое плохо! Во втором случае мы начинаем с моделирования хорошего поведения и затем смотрим на отклонения от него; так же в сетевом трафике, в логах, в поведении и т.п.

В этой ситуации очень важно знать, что такое хорошо! При этом в обоих вариантах важно учитывать:

- ♦ сложно моделировать то, чего вы не знаете (как с хорошей стороны, так и с плохой);
- ♦ если моделирование происходит при изначально плохом поведении (идут атаки, происходят мошеннические операции, пользователи нарушают политику информационной безопасности), то система будет рассматривать это поведение как норму и не будет выявлять в будущем схожие ситуации;
- ♦ окружение может заставить пользователей или иных субъектов вести себя аномально под влиянием внутренних или внешних факторов (авральная сдача проекта к сроку, отсутствие обучения и т.п.).

Если текущие варианты не способны эффективно бороться с новыми и неизвестными ранее угрозами, то что нам позволит это сделать? Ответ есть — машинное обучение! Но чтобы разобраться с тем, насколько оно эффективно и как его применять на практике, надо немного погрузиться в теорию.

НЕМНОГО ТЕОРИИ

Начнём с развенчания мифа, что систему на базе машинного обучения, в отличие от антивируса, не надо обновлять. Это не так — в любой системе машинного обучения есть два больших блока — собственно само обучение и исполнение, которые часто и объединяют под общим термином «машинное обучение». Заметьте, в процессе исполнения система, или, иными словами, модель, уже не учится. И если она делает ошибку на одних входных данных, то она будет делать ошибку и на других входных данных, пока не будут внесены изменения в саму модель. В отличие от человека, который учится в процессе работы, машинное обучение является итеративным. Обучили модель — запустили в работу — нашли ошибки и неточности — снова стали обучать — снова запустили в работу. Когда говорят, что машинное обучение не требует обновления, как сигнатурные механизмы, это некоторое лукавство. Модель надо регулярно дообучать на новых данных.

Жизненный цикл системы защиты на базе машинного обучения выглядит следующим образом:

1. Загрузка обучающих данных, так называемого датасета.
2. Предварительная обработка датасета.
3. Извлечение так называемых признаков. Это один из самых важных этапов большинства алгоритмов машинного обучения, который позволяет превратить сырые данные в информацию, которую может обрабатывать модель, на основе которой он и будет принимать решения на новых, неизвестных данных.
4. Выбор алгоритма или модели машинного обучения.
5. Тренировка модели, используя датасет и извлечённые из него признаки.
6. Повтор для поиска лучшей модели. Перед тем как мы выберем наиболее эффективную модель, нам придётся перепробовать многие из них, так как большинство из них может решить поставленную задачу, но с разным результатом — какая-то модель делать это быстрее, но менее точно; какая-то будет обнаруживать угрозы точнее, но медленнее. Мы можем упростить модель, снижая число

Заметьте, в процессе исполнения система, или, иными словами, модель, уже не учится. И если она делает ошибку на одних входных данных, то она будет делать ошибку и на других входных данных, пока не будут внесены изменения в саму модель

признаков, или усложнить её, добавив новые признаки, новые источники данных или скомбинировав модели.

7. Интеграция лучшей модели в «боевую» систему.

8. Запуск системы в промышленную эксплуатацию и подача ей на вход реальных данных.

9. По мере появления новых угроз возврат к первому этапу.

Машинное обучение позволяет сделать правильный вывод, опираясь на качественный датасет, который является одним из залогов успеха в обнаружении новых угроз. Чем больше и разнообразнее набор обучающих данных, тем точнее будет результат обнаружения. Чтобы научиться определять спам, нам нужны десятки и сотни тысяч электронных сообщений для анализа. Чтобы научиться предсказывать поведение пользователя, нужно отслеживать все его действия в течение нескольких недель (и ещё делать контрольное обучение в атипичное время — предотпускное, послеотпускное, перед корпоративом и т.п.).

Хорошие датасеты очень ценятся, и они являются лакомым куском для любой компании, которая занимается машинным обучением. Сегодня в Интернете можно найти немало таких датасетов в различных областях, но в области информационной безопасности их почти нет. Вы не можете его купить, вы не можете его получить у какой-либо ИБ компании, так как такая база является конкурентным преимуществом. Обычно датасеты хранятся в тайне, в отличие от тех же алгоритмов машинного обучения, которые часто раскрываются разработчиками. Однако бывают и исключения. Например, Splunk выложил в Интернет датасеты для изучения и тестирования своего продукта, но можно ли считать его подходящим для тестирования других средств защиты и построения собственной системы мониторинга на базе машинного обучения? На самом деле я бы не рассчитывал в обозримом будущем на чужие датасеты, а рекомендовал бы формировать собственную обучающую выборку, на которой и учить модели машинного обучения. У вас же есть сетевой трафик, вредоносные файлы, URL, электронная почта, действия пользователей? Собирайте их и обрабатывайте.

В качестве примера покажу, какой объём данных собирает Cisco в течение всего одних суток:

- ◆ 180 миллиардов DNS-запросов;
- ◆ 18 миллионов файлов, из них 1,5 млн вредоносных;
- ◆ 18 миллиардов URL;
- ◆ 600 миллиардов email;

Я бы не рассчитывал в обозримом будущем на чужие датасеты, а рекомендовал бы формировать собственную обучающую выборку, на которой и учить модели машинного обучения

- ◆ 250 тысяч облачных приложений.

Это большой объём данных, но, прежде чем их подавать в модель машинного обучения, необходимо их предварительно обработать, так как модель не понимает разницы между шумом и полезными данными. Кроме того, надо помнить, что в датасеты могут быть целенаправленно внесены некорректные или фальшивые данные, чтобы обмануть систему. Поэтому так важна предварительная обработка, в рамках которой мы выделяем так называемые признаки, например доменное имя, отправителя email или IP-адрес. На самом деле таких атрибутов может быть очень много, и зависят они от того, какую систему мониторинга мы будем строить/использовать. Например, для системы мониторинга сетевых аномалий (NTA или NDR) к таким признакам могут быть отнесены:

- ◆ порт источника;
- ◆ порт отправителя;
- ◆ протокол (udp, icmp, tcp, ipv6, другой);
- ◆ идентификатор приложения;
- ◆ входящие пакеты/фреймы (количество байт, количество пакетов, количество пакетов с битами rst, fin, syn, syn-ack);
- ◆ исходящие пакеты/фреймы;
- ◆ сервера и клиенты;
- ◆ длительность потока;
- ◆ число потоков (за определённый интервал времени);
- ◆ число соединений;
- ◆ число параллельных потоков;
- ◆ число новых потоков;
- ◆ время суток;
- ◆ процент прекращённых соединений;
- ◆ и др.

У решений класса EDR (Endpoint Detection & Response) признаков больше 400 — это метаданные, ассоциированные с анализируемым файлом, — наличие сетевых подключений, нестандартные протоколы, использование определённых вызовов, внесение изменений в файловую систему, разработка под определённую архитектуру, обращения к реестру, поддерживаемые языки, работа с оперативной памятью и жёстким диском, запуск других процессов и т.д.

А, например, при мониторинге DNS-запросов с точки зрения ИБ мы должны обращать внимание на следующие признаки:

- ◆ В какое количество IP-адресов резолвится домен?
- ◆ Число стран, в которых размещаются IP-адреса домена?
- ◆ Длина имени домена?
- ◆ Минимальный, средний и максимальный TTL домена?
- ◆ Как часто за сутки менялись IP-адрес домена?
- ◆ Каков возраст домена?
- ◆ Насколько равномерно распределены символы в домене?
- ◆ Насколько осмыслен домен?
- ◆ Кто владелец домена?
- ◆ В какой автономной системе располагается домен?
- ◆ Какие ещё домены «висят» на этом же IP-адресе?
- ◆ Кто регистратор домена?

После выбора признаков мы переходим к этапу, который чаще других ассоциируется с термином «машинное обучение», а именно к выбору соответствующей модели, который всегда будет являться балансом между скоростью работы, аккуратностью предсказания и сложностью модели. При этом помните, что ошибки будут присутствовать всегда. Не получилось с одной моделью, попробуйте другую. Не бывает единственно правильного или универсального алгоритма — исходную задачу можно решить разными способами, от выбора которых будет зависеть точность и скорость решения. Если вам нужно оперативное обнаружение в близком к реальному времени, вы выберете одну модель, для ретроспективного анализа постфактум — другую.

Стоит помнить, что вам нужно правильно выбрать все три элемента — датасет, признаки и алгоритмы. При этом датасет является самым важным. Если обучающая выборка мала, неполна или некачественна, то никакая модель не поможет.

МОДЕЛИ МАШИННОГО ОБУЧЕНИЯ

Наиболее популярным классом машинного обучения является обучение с учителем (supervised

machine learning). Эти алгоритмы используются в тех случаях, когда у вас достаточно простые данные и понятные признаки. Например, блокирование платёжной карты после снятия наличных за границей. Тут всё просто. Обычно все ваши транзакции проходят в домашнем регионе, а тут аномалия — внезапное (если вы не предупредили свой банк о поездке) снятие наличных за пределами страны. Наверное, до 75 % всех алгоритмов машинного обучения, используемые в том числе и в ИБ, — это нестареющая классика, то есть обучение с учителем, с помощью которого можно быстро решить нужную задачу.

Самыми популярными моделями являются классификация и регрессия. Первая позволяет предсказать категорию событий (например, конкретных угроз), а регрессия — предсказать значение. Например, если вам нужно предсказать, когда у вас будет рост атак, то вам нужна регрессия, а если вы хотите понять, каких атак у вас будет больше через полгода, то вам нужна классификация. С помощью машинного обучения с учителем можно выявлять заражение вредоносным кодом, взаимодействие с командным C2-сервером, загрузку вредоносного кода, фишинг и спам, DGA-домены и т.п. В этих моделях кто-то должен дать на вход модели уже размеченные данные (опять возвращаемся к важности датасета и разметки). Например, сказать: это спам, а это нет; это DDoS, а это просто новогодний всплеск заказов; это фрод, а это обычная транзакция.

Что делать, когда у нас нет размеченных данных? В этом случае нам поможет обучение без учителя (unsupervised machine learning), которое позволяет искать структуру и зависимости в неразмеченных данных и делать выводы на их основе. Если обучение с учителем позволяет выявлять новые, но всё-таки ранее известные типы угроз, то обучение без учителя фокусируется на угрозах неизвестных, например, расширение плацдарма злоумышленников в инфраструктуре (lateral movements), утечки данных, аномальный доступ к различным сервисам и серверам.

Представим себе, что мы фиксируем четыре неудачных попытки входа под одной учётной записью. Это явное нарушение, так как у нас в политике стоит ограничение в три попытки. Для обнаружения четырёх и более неудачных попыток не требуется машинное обучение. Активность одной учётной записи из разных географических точек в течение одних суток может означать вредоносную активность. А может и нет, если вы, например, полетели в

Не бывает единственно правильного или универсального алгоритма — исходную задачу можно решить разными способами, от выбора которых будет зависеть точность и скорость решения

командировку и заходили в какую-либо систему, например, из Москвы, Лондона, Нью-Йорка и Чикаго в течение суток (это, кстати, вполне возможно). По этой причине банки часто блокируют карточные транзакции, считая их фродом. Для обнаружения такой активности также не требуется машинное обучение. А вот доступ из непривычного места уже требует — тут как раз поможет кластеризация, для которой такая попытка будет рассматриваться как аномалия. Причём может оказаться, что это даже не кража учётной записи, а пользователь дал добро какому-то приложению через OAuth подключаться к облачному сервису и благополучно забыл об этом.

Вы не можете сказать, где провести грань между нормальным и аномальным числом удаляемых из облака или скачиваемых по локальной сети на один компьютер файлов. Вы можете только сравнивать между собой этот признак у разных пользователей и групп пользователей, выявляя тем самым нормальное и аномальное поведение, что и помогает делать машинное обучение без учителя.

Какие ещё сценарии можно назвать для систем машинного обучения без учителя? Вот только некоторые примеры:

- ◆ несовпадение профиля трафика или загрузки центрального процессора на идентичных серверах или сетевых сегментах, что может говорить о работе шифровальщика или утечке данных;
- ◆ неизвестная ранее сетевая или пользовательская активность;
- ◆ нестандартные коммуникации с коллегами (выявление центров силы, интрижка между сотрудниками, сговор);
- ◆ пользователь получает доступ к сетевому сегменту, системе или серверу первый раз;
- ◆ пользователь осуществляет действия с редко применяемыми привилегиями;
- ◆ первое использование определенных привилегий пользователем;
- ◆ пользователь, приложение, сервис или узел действуют в непривычное время;
- ◆ пользователь, приложение, сервис или узел активизировались после долгого периода неактивности;
- ◆ параллельный доступ учётной записи из нескольких мест параллельно;
- ◆ необычный объём действий пользователя, сервиса или узла.

МОЖНО ЛИ СВОИМИ СИЛАМИ?

И вот тут мы подошли к самому главному. Как получить максимальную пользу от машинного

обучения при мониторинге угроз? Я бы начал с ответа на три ключевых вопроса, с которых начнется длинный путь:

- ◆ Какие данные мне нужны?
- ◆ Что я хочу в них увидеть?
- ◆ Как и где это «что» будет применено?

После ответов на эти вопросы перед вами откроется две дороги — строить собственную систему машинного обучения или купить готовое решение. Первый путь откроет новый набор вопросов:

- ◆ У вас есть необходимые датасеты?
- ◆ У вас есть квалифицированные аналитики? В начале 2000-х годов на CISO Summit в Москве Антон Чувакин сказал: «У вас есть нужные данные, но нет правильных моделей. У вас есть правильные модели, но нет нужных данных». Сегодня ситуация изменилась: у вас есть нужные данные (и их слишком много) и правильные (наверное) модели... но нет аналитиков, которые могут свести всё это вместе.
- ◆ Какие алгоритмы вы будете использовать?
- ◆ Вы можете использовать доступные модели?
- ◆ Как вы будете проверять качество своих моделей?

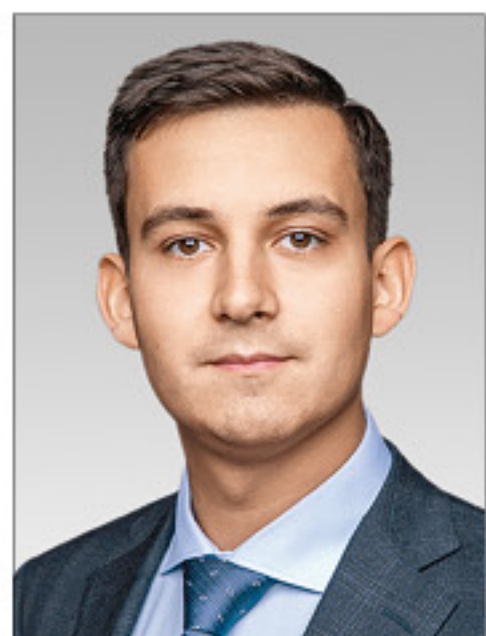
Непростые вопросы, не так ли? Второй путь может показаться более простым, но стоит помнить, что и он не устлан розами и лилиями и многие производители часто обманывают или не говорят всей правды своим клиентам, которые повелись на рекламу о применении машинного обучения для обнаружения угроз. В этом случае я бы задал вендору свою порцию вопросов:

- ◆ Какие алгоритмы/модели используются для обнаружения угроз?
- ◆ Какие наборы данных используются в алгоритме/модели?
- ◆ Где запускаются алгоритмы (на узле, в ЦОДе, в облаке)?
- ◆ Могут быть алгоритмы/модели обучены на моих данных?
- ◆ Как много обучающих данных требуется?

* * *

В заключение хочу отметить, что раньше люди покупали SIEM, чтобы снизить необходимость написания сигнатур для систем обнаружения атак, а также снизить число ложных срабатываний у них. Сейчас люди покупают или строят машинное обучение, чтобы не писать правила для SIEM или снизить число ложных срабатываний в них. Что дальше?

«ФИНАНСОВЫЕ УСЛУГИ НОВОГО ПОКОЛЕНИЯ ПОТРЕБУЮТ ЭТИЧЕСКОГО РЕГУЛИРОВАНИЯ»



Никита ЛОМОВ
руководитель
аналитического
отдела Ассоциации
ФинТех

Финансовые услуги и сервисы нового поколения будут базироваться на таких технологиях, как искусственный интеллект, машинное обучение, интернет вещей. Но их бесконтрольное использование может привести к дискриминации потребителей.

Ассоциация ФинТех провела исследование мнения российского финансового рынка по вопросам развития финансовых технологий. Наши респонденты, среди которых представители банков, страховых компаний, профучастников рынка ценных бумаг, сошлись во мнении, что уже сейчас необходимо разрабатывать регуляторные режимы для инновационных продуктов и решений, в том числе регулирование и стандарты для безопасного и этичного применения алгоритмов искусственного интеллекта (ИИ) в финансовой отрасли. В противном случае технологии будут нести риски для развития рынка.

Интересно, что именно искусственный интеллект стал одной из первых технологий, которые начали использовать представители финансового сектора. Так, в 1986 году APEx (Applied Expert Systems) представила PlanPower, решение на основе алгоритмов для создания финансовых планов для тех, у кого годовой доход составлял более \$75 000 в год.

Сейчас финансовые организации успешно используют решения с применением алгоритмов искусственного интеллекта в кредитовании, платежах, маркетинге и продажах. На основе ИИ создаются системы для обнаружения и предотвращения мошеннических действий. Страховые компании рассчитывают стоимость своих продуктов с помощью сложных моделей. Уже ставшие привычными чат-боты и виртуальные ассистенты также функционируют как самообучающиеся алгоритмы. Благодаря технологиям стало возможно создавать персонализированные решения с учётом потребностей и предпочтений каждого клиента. Ещё один пример — составление индивидуальных инвестиционных планов с учётом горизонта планирования, аппетита к риску и других параметров на платформах для инвестирования.

Эксперты прогнозируют, что в течение ближайших пяти лет финансовые организации будут внедрять решения на основе искусственного интеллекта в следующих областях:

- ◆ Управление бизнес-процессами и оптимизация с использованием инструментов интеллектуального анализа позволит компаниям сделать их более эффективными и повысить общую производительность.

- ◆ Обслуживание клиентов с помощью чат-ботов или виртуальных помощников. С учётом растущей конкуренции на рынке финансовых услуг реагировать на обращения клиентов необходимо мгновенно. Искусственный интеллект позволяет решать эту задачу.

- ◆ Кредитный скоринг. Большинство используемых в настоящее время систем кредитного скоринга устарели. Использование искусственного интеллекта и машинного обучения для принятия решений позволит улучшить их качество и предоставить доступ к кредитованию большему количеству клиентов.

- ◆ Киберзащита. Более широкое использование ИИ в области киберзащиты обеспечит проактивные механизмы для борьбы с атаками и защиты данных от хакеров.

По оценкам консалтинговой компании IDC, мировые расходы на системы ИИ к 2024 году достигнут \$110 млрд в 2024 году, удвоившись по сравнению с \$50,1 млрд в 2020 году. Недавний опрос EY показал, что 64% финансовых учреждений планируют широко использовать технологии ИИ в течение следующих двух лет.

ЧТО ЖЕ ВЫЗЫВАЕТ БЕСПОКОЙСТВО ПРЕДСТАВИТЕЛЕЙ ОТРАСЛИ?

Дело в том, что искусственный интеллект может невольно дискриминировать отдельные группы клиентов. Так, например, алгоритмы, которые применяются для автоматического скоринга, могут отклонять кредитные заявки клиентов на основе их религии, этнической принадлежности, образования или географического положения. Если в наборе данных отсутствует информация о поведении какой-либо группы, то модель будет построена некорректно, а значит и решения, которые принимаются автоматически, будут несправедливыми. Таким образом будут создаваться непреодолимые барьеры для получения финансовых услуг для множества людей.

С одной стороны, использование искусственного интеллекта должно исключить ошибки,

возникающие из-за человеческого фактора. Например, при рассмотрении заявки сотрудники банка могут неправильно оценить платёжеспособность заёмщика и отказать ему в предоставлении средств. ИИ при оценке кредитоспособности будет принимать решения, беспристрастно анализируя все возможные параметры. Но с другой, алгоритм может масштабировать одно неправильно принятое решение до невероятных размеров. Это всё та же человеческая ошибка, только возведённая в энную степень.

Ещё одна претензия к технологии заключается в том, что пользователи не знают, что именно происходит с данными, на основе чего принимаются решения, от которых зависит их благополучие.

КОДЕКС ЭТИКИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Именно поэтому во многих странах уже реализуются инициативы, направленные на создание безопасных инновационных продуктов и сервисов. И Россия не исключение, 26 октября ведущие российские компании и научно-исследовательские организации подписали кодекс этики искусственного интеллекта.

Документ устанавливает общие морально-этические принципы для всех, кто использует технологию ИИ. В кодексе говорится, что человеко-ориентированный и гуманистический подход является основным этическим принципом и центральным критерием оценки этического поведения в сфере ИИ. Компаниям рекомендуется использовать риск-ориентированный подход, ответственно относиться к влиянию ИИ на общество и граждан, обеспечивать комплексный надзор человека за любыми системами ИИ, иметь возможность отменить решения, принимаемые системой, на любом этапе. Также отмечается необходимость информировать пользователей о том, что они взаимодействуют с искусственным интеллектом и дать им возможность предотвратить это взаимодействие. В компаниях, которые присоединились к кодексу, должны быть назначены уполномоченные по этике ИИ.

В целях обеспечения справедливости и недопущения дискриминации компании должны принимать меры для того, чтобы удостовериться, что применяемые ими алгоритмы и наборы данных, методы обработки используемых для машинного обучения данных, при помощи которых осуществляется группирование и классификация данных, касающихся отдельных лиц или групп лиц, не влекут их умышленную дискриминацию.

Для того чтобы обмениваться опытом, компании, использующие ИИ, создадут свод лучших и худших практик решения этических вопросов, и предоставят к нему публичный доступ.

ЗАРУБЕЖНЫЙ ОПЫТ

Евросоюз же в апреле этого года представил проект законодательного регулирования искусственного интеллекта. От поставщиков и пользователей систем ИИ требуется соблюдение конкретных правил прозрачности данных, управления, ведения учёта и документации. Среди требований (наряду с установлением стандартов надёжности, точности и безопасности) обязательный человеческий надзор в тех областях, где есть риски, связанные с ограничением доступа потребителей к тем или иным услугам.

Нарушения приведут к штрафам, аналогичным штрафам за нарушение законодательства о персональных данных. В некоторых случаях эти правила также будут применяться к компаниям и за пределами ЕС. Европейские законодатели считают, что этическое регулирование в виде свода норм и правил должно так же неукоснительно соблюдаться, как и стандарты ведения бизнеса. Предложенное ЕС законодательство является наиболее всеобъемлющим по сравнению с нормами, принятыми в других странах.

С 2019 года правительство Великобритании запустило проект «Mandating Security Requirements For Consumer 'IoT' Products», целью которого является разработка регуляторных требований к производителям продуктов интернета вещей IoT.

Китай имеет «Пекинские принципы», которые являются этическими рамками, для регулирования того, как должен функционировать искусственный интеллект. В частности, Пекинские принципы гласят, что ИИ не должен использоваться против людей или наносить им вред.

В ряде стран, таких как Сингапур, Гонконг, Великобритания, с рекомендациями по использованию искусственного интеллекта выступают и Центральные банки, указывая как следует управлять связанными с технологией рисками в финансовом секторе.

* * *

Главное, к чему стремятся во всех странах, обеспечить прозрачность и объяснимость решений, которые принимаются с использованием искусственного интеллекта. Как лучше этого добиться, с помощью строгого законодательства, которое установит ответственность за любое отступление от правил или добровольного саморегулирования, пока открытый вопрос.



**Елена
ПОКАТАЕВА**
обозреватель
BIS Journal

ТОТ ЕЩЁ СУБЪЕКТ...

ПО МАТЕРИАЛАМ КРУГЛОГО СТОЛА «ЧЕЛОВЕК И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: ЕДИНСТВО И БОРЬБА ПРОТИВОПОЛОЖНОСТЕЙ» НА XVIII МЕЖДУНАРОДНОМ БАНКОВСКОМ ФОРУМЕ В СОЧИ

Субъектность искусственного интеллекта (ИИ) — это вопрос медийного хайпа, с одной стороны, и научных исследований в области правоведения — с другой. Но практические аспекты «дееспособности» ИИ, по сравнению с человеком, лежат в иной плоскости.

ПОКА ВСЁ ПРОСТО

Главный вопрос искусственного интеллекта (ИИ) — вопрос об ответственности за принимаемое решение. На базовом уровне он имеет простой ответ: человек описывает все этапы и сценарии «мыслительной деятельности» искусственного разума. Сегодня на этом уровне работает большинство систем ИИ: системы, основанные на правилах (rule based), медицинские экспертные системы, программы, рассчитывающие скоринговый балл заёмщика в банках, и прочие системы, помогающие человеку принимать правильные решения.

Выступая в сентябре на круглом столе «Человек и искусственный интеллект: единство и борьба противоположностей», Валерий Лях, директор департамента противодействия недобросовестным практикам Банка России, дал следующее определение этой ситуации: «ИИ и ML (машинное обучение) составляют сегодня «экзоскелет» для человека, помогая ему в принятии решений». Он подчеркнул, что модели ИИ используются для реализации простых в интеллектуальном смысле ИТ-систем, но в нетривиальных ситуациях по-прежнему нужен человеческий, а не машинный ум.

Действительно, ИИ самостоятельно никогда не может уволить. В недавнем нашумевшем скандале с увольнением 147 сотрудников компании Xsolla само решение принимал руководитель организации, ИИ лишь предоставил ему отчёт с данными измерений рабочей активности сотрудников по ряду метрик. ИИ также не может самостоятельно писать стихи, прозу и новостные сообщения. Он лишь реализует те программные описания и словари, которые заранее задал ему человек.

Модератор круглого стола вице-президент Ассоциации банков России Анатолий Козлачков предложил яркую аналогию, отталкиваясь от основ римского права: «В Древнем Риме раб назывался «говорящий инструмент». В наше время таким «рабом» в услужении человека является искусственный интеллект».

ПРОСМАТРИВАЕТСЯ СЛЕДУЮЩИЙ УРОВЕНЬ

Но уже просматривается следующий уровень реализации интеллектуальных ИТ-систем, когда результаты работы ИИ будут встраиваться в бизнес-цепочки конкретных действий, осуществляемых автоматически. Вся история эволюции корпоративной информатизации в сторону сквозной (end-to-end) автоматизации (с участием интеллектуальных механизмов на различных участках маршрута) приводит именно к этому состоянию: решение, которое автоматически примет специализированный ИИ на одном этапе, повлияет на выполнение задач на всех последующих участках.

Никакого самостоятельного принятия решений в смысле субъекта права на этом уровне по-прежнему не предвидится, но появляется фактор ответственности за решение, принятое ИИ.

На самом деле в таких ситуациях ИИ принимает решение чисто математически — делает вывод на основании имеющихся данных. И такое положение вещей обуславливает ряд важных аспектов интеллектуальных систем.

Уже просматривается следующий уровень реализации интеллектуальных ИТ-систем, когда результаты работы ИИ будут встраиваться в бизнес-цепочки конкретных действий, осуществляемых автоматически

Беспристрастность. В правила принятия решений для ИИ человек может внести предвзятые суждения. Уже набили оскомину примеры из американской действительности, когда заранее заданные правила поиска кандидатов на вакантные рабочие места смещены в сторону людей с определённым цветом кожи. Однако возможны и менее одиозные ситуации. Например, правила, которые описывают корреляцию между активностью сотрудника в компании (участие в совещаниях, выступления и комментарии на внутреннем портале) и его личной эффективностью, могут быть смещены так, что в кадровый резерв руководства попадут более говорливые сотрудники, а не те, кто действительно работает эффективно.

Прозрачность хода получения результата. Прозрачность всех шагов по пути достижения финального суждения обеспечивает объяснимость полученного результата. «Должна быть обеспечена объяснимость результатов. Не интерпретируемость, а именно объяснимость полученного решения», — подчеркивает Валерий Лях.

На настоящий момент прозрачность — одна из главных «болевых точек» систем ИИ. Системы машинного обучения по своей сути неспособны объяснить полученный результат, поскольку он является следствием множества операций оптимизации на совокупности данных. Объяснительный функционал, в принципе, может быть реализован в системах логического интеллекта, но с целью упрощения систем этого не делается.

ЗАВТРА НАЧИНАЕТСЯ СЕГОДНЯ

Например, сегодня биржевые роботы работают именно в качестве «экзоскелета» человека в терминологии Валерия Ляха. Но развитие финансовой сферы, в которой действуют всё более умные программные роботы, приводит регуляторов к необходимости получать доступ к исходному коду биржевых роботов, чтобы контролировать происходящие процессы.

Нужен контроль регулятора за тем, чтобы ИИ-система работала добросовестно, отмечает Валерий Лях: «Необходимо гарантировать, что действия таких программ не вызовут перекосов на рынке, создавая, например, преимущества для отдельных участников». Более того, множество таких программ, работающих одновременно, могут создавать волатильность на рынке. Это проблема не сегодняшнего, а завтрашнего дня, но уже сегодня их необходимо учитывать, занимаясь разработкой новых правил регулирования.

НЕ ЭТИКА, А УГОЛОВНОЕ ПРАВО

Созданием таких правил сегодня заняты все развитые страны. С чьей-то лёгкой руки они

получили название этических принципов взаимодействия ИИ и человека, хотя этический принцип там, по сути, один — верховенство человека над умной машиной. На самом деле вопросы причинения ущерба, связанного с применением ИИ, должны рассматриваться никак не в этическом русле, а в русле уголовного права.

ПРИНЦИПЫ ПРОТИВ ИНТЕРЕСОВ

Все обсуждаемые тезисы и подходы скорее относятся к вопросам регулирования. И все эти вопросы сегодня находятся в стадии активной разработки. Но уже намечен ряд основополагающих принципов, по которым сложился международный консенсус.

- ♦ Лица, ответственные в компаниях за ИИ-решения, должны иметь знания в области ИИ.

- ♦ Модели ИИ не должны быть чёрными ящиками с результатом, который не может быть объяснён.

- ♦ Используемые данные должны быть понятными, прозрачными и интерпретируемыми всеми сторонами, использующими ИИ-решения. В силу этого требования, в частности, не рекомендуется использовать сведения из соцсетей.

- ♦ «Этическое» поведение ИИ-систем, понимаемое как использование только достоверных данных и точных методов их обработки.

Возникает вопрос: насколько реализуемы принципы создания ИИ-систем, сформированные в русле международного консенсуса, для практических внедрений в разных странах? Ильдар Бегишев, заслуженный юрист, преподаватель Казанского инновационного университета имени В. Г. Тимирязова, предупреждает, что необходимо создавать собственную российскую систему правового регулирования взаимоотношений общества и ИИ и там отразить все вопросы правовой субъектности ИИ. «Глобальные ИТ-гиганты, предлагая свои концепции регулирования, ставят во главу угла свои интересы и лишь потом — интересы людей и государства».

Правда, как считает Игорь Ашманов, президент компании «Крибрум», член Совета при Президенте РФ по развитию гражданского общества и правам человека, от этого недостатка не свободен сегодня и проект кодекса этики искусственного интеллекта, который разрабатывается в нашей стране. По мнению эксперта, нынешний вариант кодекса «заточен» под интересы Сбера, «Яндекса» и других крупных компаний, которые занимаются его разработкой.

Так что признание факта, что ИИ — никакой не субъект права, проще нашу жизнь не делает. Пусть он и не субъект, но регулировать его активность точно необходимо.



Василий ПИСКАРЕВ
председатель Комиссии
Государственной Думы
по расследованию фактов
вмешательства иностранных государств
во внутренние дела России

ВАСИЛИЙ ПИСКАРЕВ: «ПРИЧАСТНЫЕ К КИБЕРАТАКАМ НА СИСТЕМУ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ ДОЛЖНЫ ПОНЕСТИ ЗАСЛУЖЕННОЕ НАКАЗАНИЕ»

По итогам Единого дня голосования, который в этом году пришёлся на 19 сентября, сегодня можно признать, что наша избирательная система выдержала и успешно прошла непростое испытание в условиях мощного прессинга извне.

Агрессивная кампания, развёрнутая в западных СМИ для дискредитации выборов в Государственную Думу, попытки внешних сил ещё задолго до самих выборов объявить их нелегитимными, несвободными, навязать россиянам при поддержке крупных американских цифровых платформ своих кандидатов и настойчиво предложить за них голосовать своей цели не достигли.

КАМПАНИЯ ПО ДИСКРЕДИТАЦИИ ВЫБОРОВ ПРОВАЛИЛАСЬ

Почему я так считаю? Во-первых, люди пришли на выборы. Ведь какая была мощная кампания не просто в западных СМИ, а особенно в их сегменте на русском языке! Вот в тех самых, финансируемых конгрессом США, СМИ-иноагентах, включая «Голос Америки» и «Радио Свобода»,

в финансируемой правительством ФРГ «Дойче велле», во множестве подпитываемых западными фондами сетевых изданий, да и в соцсетях. На наших сограждан обрушили всю мощь их пропаганды, чтобы убедить, что выборы «нелегитимны», «заранее сфальсифицированы», к ним не допустят 9 миллионов (!) россиян и т.д.

Цель всего этого нам понятна. Ведь если бы люди во всё это поверили, то они бы на выборы просто не пошли. Аномально низкая явка могла бы действительно повлиять на легитимность парламента и ударить по престижу нашей страны. Но этого не случилось. Наоборот, как вы знаете, явка даже превысила результат прошлых выборов в Государственную Думу.

Мне представляется, что люди просто оскорбились вот таким наглым давлением из-за границы, пришли на избирательные участки и сделали свой осознанный выбор.

ЭЛЕКТРОННОЕ ГОЛОСОВАНИЕ ПРОШЛО ПРОВЕРКУ НА ПРОЧНОСТЬ

Во-вторых, прошла проверка на прочность и доказала свою жизнеспособность система Дистанционного электронного голосования (ДЭГ). Это новая, перспективная форма волеизъявления, которая прошла в ходе нынешних выборов успешную обкатку в ряде регионов — а в Москве уже не в первый раз, — и очевидно, что она получит развитие в будущем. Голосовать дистанционно — это быстро, удобно и привлекает к участию в выборах и так называемых продвинутых пользователей, привыкших пользоваться самыми современными гаджетами и электронными услугами, и

Хочу отдать должное нашей системе защиты, которая выдержала мощнейшие кибератаки. Они продолжались все три дня, пока шло голосование, и были зафиксированы с IP-адресов, зарегистрированных в США, Германии, Украине, Китае и ряде других стран



На фото: Председатель Комиссии Госдумы Василий Пискарев и наблюдатель от Общественной палаты Наталия Горелик на избирательном участке в московской школе № 1400

тех, кто по каким-то причинам не находил времени прийти на избирательный участок. По всей видимости, именно этот факт вызвал откровенную панику и истерику у некоторых персонажей.

Мы зафиксировали прозвучавшие из-за рубежа на русском языке публичные призывы к организации кибератак на нашу электронную систему голосования. Эти подстрекатели установлены, их действиям должна быть дана правовая оценка, и они должны понести заслуженное наказание. Соответствующее обращение Комиссия направила в Генеральную прокуратуру Российской Федерации.

Хочу отдать должное нашей системе защиты, которая выдержала мощнейшие кибератаки. Они продолжались все три дня, пока шло голосование, и были зафиксированы с IP-адресов, зарегистрированных в США, Германии, Украине, Китае и ряде других стран. И практически половина кибератак шла из Соединённых Штатов. Всё же хотелось бы услышать объяснения от американских официальных лиц — что это, как не вмешательство в выборы?

Кстати, география сообщений о ложном минировании, которыми нас периодически забрасывают, и кибератак на выборы в России очень похожа. Иначе, чем актом гибридной войны против нас, я это назвать не могу. И обратите внимание, власти США вот уже сколько лет вешают на Россию

всех собак, обвиняя не только во вмешательстве в их выборы, но и едва ли не во всех смертных грехах. Но где доказательства? У нас, в отличие от них, что называется, «все ходы записаны».

«ШПАРГАЛКИ» В СМАРТФОНАХ НЕ ПОМОГЛИ

Вот, к примеру, разворачивавшаяся накануне выборов история, связанная с так называемым «умным голосованием». Очевидно, что организаторы этого проекта рассчитывали, что потом избранным с их помощью депутатам можно будет предъявить «счёт за услугу» и использовать их как агентов влияния. Но услуга оказалась поистине «медвежья».

Вся эта история с шумным и навязчивым продвижением приложения для смартфонов, от компании, связанной с Пентагоном (читай — властями США), имела скорее обратную реакцию. Кандидаты из «шпаргалки» для голосования не получили желаемую поддержку избирателей. Это просто оттолкнуло их сторонников. То есть случилось совсем не то, на что рассчитывали зарубежные «доброжелатели» России. А помимо того, создало трудности для IT-гигантов, которые использовались для продвижения программы. Ведь, по сути, речь шла о ведении агитации на выборах иностранными компаниями, что прямо запрещено российским законодательством.

Накануне голосования коллеги из Совета Федерации потребовали объяснений от руководства Google и Apple, мы тоже неоднократно контактировали с представителями обеих компаний. Как видим, они восприняли полученные предупреждения, удалили из своих магазинов приложение, продвигавшее в России деятельность экстремистской организации.

Кстати, по этому поводу в западной прессе было много шума о давлении на компании, которые «вне политики». Но всё-таки если внимательно посмотреть на ситуацию и отбросить излишние эмоции, то мы увидим, что имело место прямое нарушение российских законов, попытка иностранного вмешательства во внутренние дела нашей страны и, скажем прямо, поддержка экстремизма. При этом после удаления приложения много говорили о репутационных рисках компаний. Скажите, а открытая пропаганда деятельности экстремистской организации не влечёт никаких репутационных рисков? Нет?

APPLE И GOOGLE ПРОЯВИЛИ ПРАГМАТИЗМ

Удалив приложения из App Store и Google Play, обе компании фактически подтвердили, что попытка вмешательства в российские выборы была. Но нарушение законодательства любой страны влечёт последствия. В тех же Соединённых Штатах с этим очень строго, и бизнес знает, что никто с ними долго спорить не будет, и лишь многомиллионными штрафами не отделаешься. Но вот в данном конкретном случае цена возможным последствиям могла быть очень высока — замаячила угроза потери многомиллиардного российского рынка, крупнейшего в Европе. И Google, и Apple было принято прагматичное решение — не нарушать законодательство. Недавно принятый закон о «приземлении», который скоро вступает в силу, должен поспособствовать их работе именно в правовом поле.

Отмечу, что не было в дни выборов и такого массового вброса незаконной рекламы через сервисы медиаплатформ, который мы наблюдали, например, два года назад. Но тому же Google и его дочернему YouTube предстоит ещё многое сделать, чтобы выполнить все предписания Роскомнадзора по удалению незаконных публикаций, в том числе и не связанных с выборами.

В ходе телемоста, который Комиссия проводила весной с руководством Google, мы говорили о необходимости открыть в России полноценное представительство компании. Последние события подтвердили правильность сделанных тогда выводов и рекомендаций. Мы ожидаем не только от Google, но и от всех остальных IT-гигантов открытия представительств в России.

КОМПЬЮТЕРНЫЕ ИГРЫ ПРОТИВ ВЫБОРОВ

Особенностью этой избирательной кампании стало активное применение современных технологий. Помимо хакерских атак и использования «приложения-шпаргалки» для смартфонов, Комиссия зафиксировала и ещё одну интересную технологию — разработку специальных

компьютерных игр для вмешательства в выборы и воздействия на молодёжь.

Одно известное СМИ, — думаю, что не стоит его называть, чтобы не делать лишней рекламы, — продвигает компьютерную игру, пропагандирующую массовые беспорядки в связи с выборами.

Метод геймификации, вовлечения через игру, сегодня всё активнее задействуют против нашей молодёжи. В игровой форме ведь значительно проще вложить в умы людей свои идеи, навязать нужные стереотипы поведения. Психологи подтверждают: цель этих далеко не безобидных игрушек — вызывать возмущение, страх и, как итог, агрессию.

Понятно, к чему готовили авторы игры наших подростков. Мы видели это в реальности в начале года, когда даже детей младших классов пытались привлечь к незаконным акциям на улицах российских городов. Мы понимаем, насколько это опасно для жизни и здоровья детей, и не допустим повторения.

Использовались, конечно, и хорошо знакомые нам, «традиционные» технологии. И здесь отличился ряд хорошо знакомых нам НКО и НПО. Зафиксирована подготовка организаторов и исполнителей провокаций на избирательных участках, которые должны были создать видимость нарушений, фальсификаций, вбросов, устроить скандалы и дискредитировать выборы.

Хочу сказать, что в Центризбирком на все такие эпизоды оперативно реагировали, проверяли сообщения, разбирались в ситуациях и обращались в правоохранительные органы. Правоохранители сейчас разбираются с такими случаями, и участники провокаций обязательно будут привлечены к ответственности.

Мы внимательно анализировали появлявшиеся в ходе этой кампании фейки о выборах, и там есть немало информации для правоохранительных органов.

ЗАКОНЫ О ЗАЩИТЕ СУВЕРЕНИТЕТА ПОКАЗАЛИ ЭФФЕКТИВНОСТЬ

Наши законы о защите суверенитета и противодействии иностранному вмешательству, те 14 законодательных инициатив, которые были реализованы по результатам работы Комиссии, — успешно прошли испытание в ходе выборов.

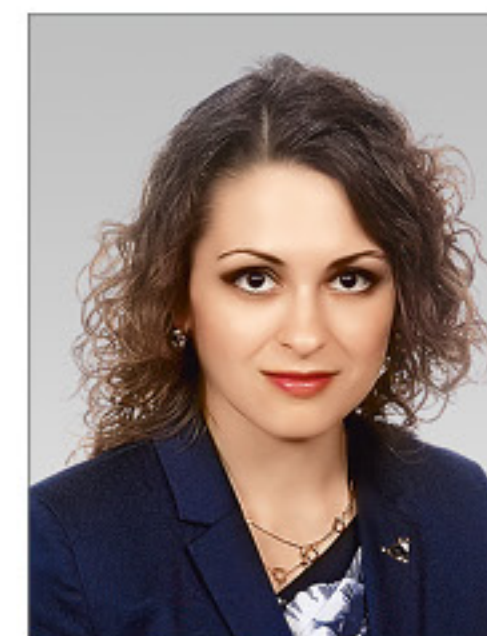
Мы видим, что принятые нормы повысили прозрачность политического процесса, и в том числе избирательной кампании. Людям стало понятнее, кто и на чьи деньги проводит политические акции, организует публикации в СМИ, призывает голосовать за тех или иных кандидатов. Кроме того, инициированные нами законы не допустили проникновения в законодательные органы идей экстремизма и терроризма и их носителей.

* * *

Мы полагаем, что законодательство в сфере защиты нашего суверенитета нужно и дальше совершенствовать. И такая работа обязательно будет продолжена.

ЦЕПЛЯЙТЕСЬ К СЛОВАМ И НАЗЫВАЙТЕ ВЕЩИ СВОИМИ ИМЕНАМИ

ПОЧЕМУ КОРРЕКТНАЯ ТЕРМИНОЛОГИЯ —
ЗАЛОГ ЭФФЕКТИВНОЙ РЕАЛИЗАЦИИ
ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ
ОПЕРАЦИОННОЙ НАДЁЖНОСТИ



**Екатерина
РАЧКОВА**
управляющий
директор
Управления
по обеспечению ИБ
Банка ВТБ (ПАО)

23 августа стартовали публичные обсуждения проекта положения Банка России «Об обязательных для кредитных организаций требованиях к операционной надёжности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг» (далее — Положение). Документ устанавливает обязательные для кредитных организаций требования к операционной надёжности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг. Планируется, что Положение вступит в силу в октябре 2022 года.

Под операционной надёжностью в проекте Положения понимается способность кредитной организации (далее — КО) обеспечить непрерывность функционирования критически важных процессов <...> в случае возникновения отказов и (или) нарушений функционирования применяемых КО информационных, технологических и других систем, оборудования и (или) несоответствия их функциональных возможностей и характеристик потребностям КО и (или) реализации киберриска в значении, установленном в пункте 7.2 Положения Банка России № 716-П от 08.04.2020 «о требованиях к системе управления операционным риском в кредитной организации и банковской группе» (далее — Положение Банка России № 716-П).

Похоже, что выставленный на обсуждение проект Положения мы видим далеко не в

окончательной редакции, некоторые формулировки однозначно требуют уточнения.

Например, ссылка из пункта 7 (буллит 4) Положения на пункт 7.5 Положения Банка России № 716-П дана, чтобы определить, что именно следует понимать под службой информационной безопасности (подразделение (работник), ответственные за организацию и контроль обеспечения защиты информации [так это проще прямо в тексте прописать, чем ссылку делать — прим. ред.]) или что должно включать в себя взаимодействие службы информационной безопасности, функционирующей в оперативном режиме работы, с Банком России (но об этом в п. 7.5 Положения Банка России № 716-П ничего нет).

Гораздо интереснее (и важнее) разобраться с терминологической развилкой «инцидент — событие риска».

Понятие «инцидент» до масштабного внедрения риск-ориентированного подхода в деятельность КО было хоть и заимствованным из международных стандартов, но интуитивно понятным, означавшим «беда». Оно явно призвало принять срочно хоть какие-то меры (что на начальном этапе зрелости процессов уже неплохо), но никак не помогало прояснить, кому надо принимать меры и на что они должны быть направлены. Мы все помним разъясняющую блок-схему «угрозы используют уязвимости...», в которую ещё как-то следовало вписать нарушителя (он помогал угрозе реализоваться),

Интересно, что параллельно Банком России в рамках деятельности ТК122 разрабатывается проект ГОСТ Р «Безопасность финансовых (банковских) операций. Обеспечение операционной надёжности. Базовый состав организационных и технических мер», в котором до последнего времени операционная надёжность была определена как «должная реализация процессов обеспечения операционной надёжности в условиях возможной реализации информационных угроз», а по плану выход данного документа планировался на IV квартал 2021 года.



неантропогенные движущие факторы (приводящие к реализации угроз различных стихийных бедствий и прочих катастроф), а также события (которые ещё не инциденты, но могут ими стать по результатам соответствующего анализа). Разобраться с источниками событий/инцидентов/угроз, а значит, и с зонами ответственности за их устранение было сложно, сделать чёткий классификатор событий и отделённых от них инцидентов — ещё сложнее. И многие в это просто не углублялись, действуя в каждом конкретном случае с организационной точки зрения во многом стихийно.

В современных реалиях подобная тактика решения проблем стала ненадёжна и расточительна в плане ресурсов. В соответствие пришли и регуляторные подходы, управление риском гораздо более структурировано, в нём разделение ответственности прозрачно.

Положение Банка России № 716-П (пункт 1.4) вводит и чётко разделяет понятия риска информационных систем (далее — ИС) и риска информационной безопасности (далее — ИБ). Один и тот же источник риска может дать начало событиям обоих типов. Но зоны ответственности подразделений КО при этом не смешиваются, поскольку привязываются к типу события, «завязанному» на категории актива, несущему потери, получающему ущерб, а у каждого актива есть владелец, ответственное за его использование и функционирование лицо/подразделение КО, провести «водораздел», даже с учётом

специфики оргштатной структуры каждой конкретной КО, гораздо легче.

В проекте Положения терминологию, в частности, по указанным выше причинам целесообразно гармонизировать с Положением Банка России № 716-П как с основополагающим документом. Это означает, что вместо понятия «инциденты операционной надёжности» (согласно п. 3 проекта Положения те инциденты, которые привели к неоказанию или ненадлежащему оказанию банковских услуг (в случае превышения допустимой доли деградации технологических процессов) надо будет использовать термин «события риска ИС». Не будет никакой путаницы с инцидентами ИБ (в Положении Банка России № 716-П — события риска ИБ, РС ИБ), не будет «перетягивания каната» по вопросу ответственности за реализацию требований проекта Положения между подразделениями ИТ и ИБ КО.

Но и с текущей редакцией проекта следует принимать во внимание тот факт, что обеспечение операционной надёжности существенным образом связано с обеспечением непрерывности деятельности КО и её восстановлением после возможных прерываний. При этом на обеспечение операционной надёжности значительное влияние оказывают проектирование, реализация и управление критичными активами в соответствии с установленными показателями операционной надёжности, в том числе разработка и (или) применение отказоустойчивых



решений, а это практически всегда зона ответственности подразделения информационных технологий КО.

Безусловно, участие подразделения ИБ КО в процессах обеспечения операционной надёжности есть, в том же объёме и того же характера, что и в процессах автоматизации, процессах обеспечения непрерывности и восстановления деятельности КО, в которых вроде бы зоны ответственности подразделений давно уже должны быть поделены.

Из описанного в текущей версии проекта Положения к деятельности подразделения ИБ в общем случае можно отнести задачи:

- ◆ доводить до сведения подразделения, ответственного за управление событиями операционного риска (к которому относится и риск ИБ) КО, информацию о специфике (при её наличии) методологии выявления и обработки РС ИБ, выявляемых подразделением ИБ КО (п. 5 буллит 4 проекта Положения);

- ◆ поддерживать в актуальном состоянии нормативно-методическое обеспечение процессов управления правами доступа к ИС КО, модель нарушителя ИБ КО, контролировать доступ работников контрагентов и иных сторонних организаций к информационно-телекоммуникационной среде КО, соблюдение требований ИБ к передаче конфиденциальной информации третьим лицам по телекоммуникационным каналам связи (п. 5 буллиты 5, 7, п. 5.6, п. 6 проекта Положения);

- ◆ поддерживать взаимодействие с ФинЦерт Банка России, представлять интересы КО в профильных объединениях по ИБ, поддерживать в актуальном состоянии политику ИБ КО и комплекс нормативных актов КО, описывающих её требования (п. 5 буллит 8 проекта Положения);

- ◆ проводить экспертизу поступающих на согласование в подразделение ИБ решений по информатизации на предмет их соответствия политике ИБ КО, требованиям законодательства и уполномоченных регуляторов в области ИБ, идентификации присущих указанным решениям рисков ИБ (п. 5 буллит 7, п. 5.1 буллиты 4, 8, п. 5.6, п. 5.7, п. 6, п. 7 буллит 1 проекта Положения);

- ◆ принимать участие в процессе согласования предоставления прав доступа к ИС КО (п. 5.1 буллит 6 проекта Положения), осуществлять аудит прав доступа к ИС КО (п. 5.6 проекта Положения);

- ◆ принимать участие в процессе управления уязвимостями ИС и информационной инфраструктуры КО в части выявления уязвимостей ИБ и согласования решений по их устранению в установленном в КО порядке (п. 5.2 буллиты 1, 4 проекта Положения);

- ◆ принимать участие в согласовании договоров КО с контрагентами, если участие подразделения ИБ в процессе согласования договора предусмотрено нормативными актами КО (п. 5.4 проекта Положения);

- ◆ принимать участие в сценарном анализе рисков ИБ в зоне компетенции подразделения ИБ по запросу подразделения, ответственного за управление событиями операционного риска (к которому относится и риск ИБ) КО, в установленном в КО порядке (п. 5.5, п. 7 буллит 2, 3 проекта Положения);

- ◆ осуществлять мониторинг, выявление и управление обработкой РС ИБ в зоне ответственности подразделения ИБ КО (п. 7 буллит 1 проекта Положения);

- ◆ принимать участие в проверках со стороны подразделения внутреннего контроля КО, выполнять поручения в адрес подразделения ИБ КО, выданные по результатам данных проверок (п. 7 буллит 3 проекта Положения).

И вряд ли в долгосрочной перспективе, не сиюминутно, кто-то выиграет от того, что ответственность за формальное соответствие документам, регулирующим фундаментальные требования по реализации критичных для КО процессов и задач, в силу большой нагрузки, нехватки ресурсов или любых других объективных причин будут пытаться перекладывать на непрофильные подразделения, вопреки функциям этих подразделений, духу регуляторных установок и здравому смыслу.

ВЕЗДЕ ЕСТЬ ПЛЮСЫ И МИНУСЫ, ГЛАВНОЕ, ЧТОБ НЕ ЗАМКНУЛО...

ЭССЕ О ПЛЮСАХ И МИНУСАХ НОВОГО ГОСТ Р 59407–2021 ОБ АРХИТЕКТУРЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ



Сергей ВИХОРЕВ
советник
генерального
директора
ООО «ИТ-Экспертиза»

Не так давно, в мае, копилка документов, определяющих требования по защите персональных данных, пополнилась ещё одним: ГОСТ Р 59407–2021 «Информационные технологии. Методы и средства обеспечения безопасности. Базовая архитектура защиты персональных данных», который предназначен для использования в качестве технического руководства для разработчиков ИСПДн. Как видим, несмотря на пандемию, «бешеный принтер» продолжает работу. Правда, вводится в действие этот стандарт с ноября 2021 года, так что время разобраться ещё есть. Давайте посмотрим, какова польза или вред от этого документа.

«НОЖИК ПЕРОЧИННЫЙ, ПЕРОЧИННЫЙ НОЖИК»

Видимо, согласно русской поговорке «Повторенье — мать ученья», в стандарте почти в каждом разделе указывается, что он предоставляет описания высокоуровневой базовой архитектуры и соответствующих мер защиты персональных данных в информационных системах персональных данных. Да и вообще, в стандарте очень много повторов, одна и та же мысль в разных разделах многократно повторяется с небольшими интерпретациями. Конечно, в этом нет ничего плохого, но читать тяжело. Думаю, это наследие международного стандарта, хотя можно было написать и простым доступным языком. Не будем забывать, что стандарт рассчитан на разработчиков ИСПДн и является техническим руководством, поэтому должен быть понятен с первого прочтения. Но если бы это была единственная претензия к стандарту, то жить было бы можно.

В стандарте очень много тривиальных деклараций типа «персональные данные надо всегда защищать» или «защита персональных данных является целью обеспечения безопасности информации». Эти повторы не приносят ничего нового. И конечно же, стандарт ну никак не вписывается в существующую систему нормативно-правовых актов по вопросам защиты персональных данных. Документ претендует на техническое руководство по построению архитектуры защиты, но сами технические

требования, изложенные в приказах и постановлениях регуляторов, никоим образом не увязаны с положениями стандарта. По сути, этот стандарт ничего не стандартизирует. Это, наверное, ближе к тому, что называют «лучшие практики», хотя и это не совсем формат этого стандарта.

Кстати, а почему в стандарте среди технических мер делается упор только на три — идентификацию, аутентификацию и авторизацию? Ведь в требованиях регулятора определяется пятнадцать классов мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных. Так что, остальные меры применять не надо? Неувязочка вышла. Мне кажется, что здесь должна быть прямая ссылка на приказ ФСТЭК России, устанавливающий технические требования.

ЧТО НОВОГО?

А нового, как ни странно, много. Не будем останавливаться на мелочах типа введения впервые в российской практике понятия «обработчик», однако лучше бы дать этому понятию более чёткое определение и описать его в разделе «термины и определения», это было бы логично.

Наверное, главное — это применение процессного подхода к построению архитектуры защищённых ИСПДн. Стандарт довольно чётко описывает этапы жизненного цикла обработки персональных данных и процессы, которые происходят, что позволяет правильно построить схемы потоков персональных данных и, как следствие, правильно выбрать элементы архитектуры защиты персональных данных. И это — хорошо!

А вот с другой новинкой не всё так однозначно. В благом порыве всё разложить по полочкам и систематизировать стандарт предлагает рассматривать весь процесс обработки персональных данных как взаимодействие трёх ИСПДн: субъекта ПДн, оператора ПДн и обработчика ПДн. Таким образом, появляется новая сущность: ИСПДн субъекта ПДн. С философской точки зрения — это важно. Появление новой сущности (ИСПДн субъекта ПДн) в какой-то степени противоречит фабуле закона о

персональных данных. Действительно, закон определил такие сущности, как субъект ПДн и оператор ПДн (ну, ещё есть и обработчик). Каждая из этих сущностей имеет свои полномочия и обладает определёнными правами и обязанностями. Субъект ПДн — это лицо, которое является обладателем¹ ПДн, так как выступает в роли генератора этих данных и свободно в своей воле предоставляет их оператору ПДн. А оператор ПДн отличается от остальных сущностей тем, что самостоятельно или совместно с другими осуществляет обработку персональных данных и при этом определяет цели их обработки, состав и действия (операции), совершаемые с ними². И исходя из этих полномочий оператор ПДн наделяется обязанностями принимать необходимые правовые, организационные и технические меры для защиты персональных данных³ и несёт за это ответственность. Именно оператор ПДн, а не субъект ПДн, не обработчик ПДн.

А теперь посмотрим на новую сущность ИСПДн субъекта ПДн. По идее, если есть некая ИС, то у неё должен быть хозяин — оператор. Но тогда он должен и отвечать за защиту персональных данных в своей зоне ответственности (что и предполагает стандарт). Получается, что ответственность за защиту персональных данных размывается между тремя сущностями. А это не способствует целостной системе защиты. Логика же закона немного иная. Давайте посмотрим, может ли субъект ПДн выступать в роли оператора? Наверное, нет. Прежде всего, он не определяет цель обработки ПДн, состав и действие с ними и, исходя из определения, уже не может быть оператором ПДн. Закон очень чётко и однозначно определяет, что за весь процесс защиты персональных данных отвечает именно оператор ПДн. Субъект передаёт свои персональные данные оператору для обработки и контролирует саму обработку⁴. Оператор получает персональные данные от субъекта, оценивает угрозы, формирует требования по защите, доводит их до обработчика и контролирует их выполнение⁵. Но при этом именно оператор ПДн, а не обработчик получает согласие на обработку персональных данных и несёт ответственность перед субъектом о соблюдении

правил их обработки и защиты⁶. Так что введение новой сущности в стандарт может привести к очередному когнитивному диссонансу в головах тех, кто организует защиту персональных данных.

ОПЯТЬ «ОБЯЗАЛОВКА»?

А теперь вот о чём. Вообще-то, закон говорит о том, что стандарты у нас применяются добровольно. Однако в отношении стандартов, определяющих требования в целях защиты сведений, относимых к охраняемой в соответствии с законодательством информации (каковыми и являются персональные данные), закон устанавливает обязательность их применения⁷. То есть, другими словами, каждая дефиниция стандарта является обязательной для исполнения. Обратимся к первоисточнику, точнее к п. 6.2 стандарта: «Подтверждение реализации мер защиты следует обеспечивать путём надлежащего документального оформления существующих мер защиты и предоставления заключения стороны, подтверждающей наличие таких мер, их правильную реализацию и надлежащее функционирование». Ключевым здесь будет «предоставления заключения стороны, подтверждающей наличие таких мер». Переведём с казённого на русский. Получается, что все меры должны быть подтверждены каким-то документом от компетентной организации, то есть аттестатом от лицензиата ФСТЭК России. Но в требованиях ФСТЭК России нет таких жёстких мер⁸, там есть альтернатива, которую этот стандарт рубит на корню. И мы опять вернулись к «обязаловке», что, наверное, не совсем правильно.

* * *

Вот весьма беглый взгляд на новый стандарт. Не сомневаюсь, что другие эксперты, внимательно изучая текст стандарта, найдут ещё много разных разностей. Наверное, и с моим мнением не все согласятся. Но оттачивать документ надо было не после его утверждения, а на этапе его подготовки. Много уже говорили, что для разработки таких концептуальных документов надо привлекать «коллективный разум». Жалко, что и в этот раз не получилось...

¹ Обладатель информации — лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам (Федеральный закон № 149-ФЗ, ст. 2).

² Федеральный закон № 152-ФЗ, ст. 3.

³ Федеральный закон № 152-ФЗ, ст. 19.

⁴ Федеральный закон № 152-ФЗ, ст. 14, ст. 16, ст. 17.

⁵ Федеральный закон № 152-ФЗ, ст. 6.

⁶ Федеральный закон № 152, ст. 18, ст. 18.1.

⁷ Федеральный закон № 162-ФЗ ст. 4.

⁸ Приказ ФСТЭК России № 21, п. 6. «Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится оператором самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию».

НЕ ТАК СТРАШЕН ЧЁРТ, КАК ЕГО МАЛЮЮТ

ОТВЕТ НА КРИТИКУ В ЭССЕ С. В. ВИХОРЕВА
«ВЕЗДЕ ЕСТЬ МИНУСЫ, ГЛАВНОЕ, ЧТОБЫ НЕ ЗАМКНУЛО»



Александр БОЙКО
руководитель
аналитического
отдела
АО «Аладдин Р.Д.»



Алексей САБАНОВ
заместитель
генерального
директора
АО «Аладдин Р.Д.»,
д.т.н.

Критиковать любой документ, конечно же, проще, чем его создавать. Тем не менее хочется поблагодарить автора, внимательно изучившего новый ГОСТ Р 59407–2021 и открыто высказавшего своё достаточно компетентное мнение. Удивляет только то, что текст статьи С. В. Вихорева вполне мог бы быть выслан ранее в виде замечаний, десятки которых авторы обработали перед разработкой окончательной редакции по окончании публичного обсуждения проекта стандарта.

При написании международных стандартов используются отличные от отечественных ГОСТ 1.7 и ГОСТ 1.8 правила. Поскольку в ТЗ на разработку данного стандарта стоял статус IDT (идентичный), перевод не должен отличаться от оригинала. Решение о переводе стандарта из IDT в NEQ было принято уже в процессе его сдачи. Отсюда множество «тривиальных деклараций» и «обилие повторов», которые при окончательном редактировании (уже для NEQ) в максимально сжатые сроки не удалось убрать полностью.

После такого своеобразного введения дадим пояснения о месте нового стандарта в системе национальных стандартов ГОСТ Р.

ЗАЧЕМ НУЖНЫ ТАКИЕ СТАНДАРТЫ?

Этот вопрос мы слышим часто и сами достаточно часто задаём при экспертизе многих проектов стандартов. Место «переводных» стандартов многократно обсуждалось представителями разных стран в ИСО, а также в отечественных технических комитетах, где состоим мы. Обобщая результаты дискуссий, можно сделать вывод, что они должны носить не обязательный и даже не рекомендательный, а скорее информационный характер. Простыми словами, читатель такого стандарта может познакомиться с тем, как решаются поставленные типовые задачи на международном уровне.

Теперь о месте и роли рассматриваемого стандарта. Из действующей нормативной базы ФСТЭК России и ФСБ России по

защите ПДн подавляющее большинство документов составляют требования, относящиеся к мерам защиты, реализуемым техническими средствами. Имеются ли документы, являющиеся рекомендациями по построению систем защиты ИСПДн? — не припоминается. Рассматриваемый стандарт является первой (может, и не во всём удачной) попыткой разработки рекомендаций по базовой архитектуре защиты ПДн. Встаёт вопрос, что лучше: полное отсутствие идеологических и методологических рекомендаций или наличие выработанной мировым сообществом экспертов основы, на которой можно построить систему защиты? Наверное, ответ очевиден.

ОТВЕТЫ НА ПРЕТЕНЗИИ

Теперь перейдём к высказанным С. В. Вихоревым претензиям. По сути, их всего две. Основной претензией является несоответствие стандарта нашей нормативно-правовой базе. Ответ простой: кто сказал, что каждый «переводной» стандарт должен ей соответствовать? Зарубежные авторы основного текста не знают, да и не обязаны знать нормативные акты различных стран. При срочной перелицовке текста в неэквивалентный нашей главной задачей было добиться, чтобы он не противоречил нашим законам и основным подзаконным актам. На мой взгляд, в целом с этой задачей мы справились.

Вторая претензия касается наличия трёх разных ИСПДн, между которыми, по утверждению С. В. Вихорева, «размывается ответственность». Вторым утверждением является то, что наличие ИСПДн субъекта «противоречит факту закона о персональных данных», это высказывание я бы отнёс к личной трактовке автора этой цитаты положений 152-ФЗ. Начнём со второго тезиса. Замечу, что у многих в домашнем компьютере хранятся сканы основных документов. Является ли этот компьютер ИСПДн? Скорее всего, формально является. Чаще всего данные не обрабатываются, а всего лишь хранятся. Противоречит ли это положениям 152-ФЗ? Укажите, где и в какой степени. По моим

понятиям, в 152-ФЗ нет запрета на то, что владелец (субъект) делает со своими персональными данными (ПДн). Аналогом является наличие автомобиля. Хочешь — едь на нём аккуратно, хочешь — врежься в первый попавшийся столб, ты владелец.

А теперь рассмотрим всю претензию. Если ты сам собираешь и хранишь в электронном виде свои ПДн, то согласно статье 23 Конституции РФ волен с ними делать что хочешь, в том числе защищать их так, как считаешь нужным. Никакой закон это не запрещает и не регламентирует. Но если ты добровольно передаёшь свои данные оператору, ты должен быть уверен в том, что оператор сделает всё возможное для их защиты. Как у нас, так и на Западе за это отвечает тот, кто собирает ПДн. А вот дальше в нашем отечестве имеются коренные различия в подходах с международными рекомендациями.

ДВА ПОДХОДА К ЗАЩИТЕ ПДН

К сожалению, в нашей стране для ПДн чаще применяется так называемая бумажная защита, а сами данные распространяются со скоростью развития интернета и множества недобросовестных фирм, использующих ПДн платёжеспособного населения для рекламы, директ-мейлов и различных способов выманивания денег. Существующие мизерные штрафы для чиновников за утечки ПДн можно повысить ещё в два раза (как это уже дважды было), а потом и ещё в два раза — это не решит проблему.

Для сравнения, в большинстве стран ЕС нормативная база приведена в соответствие с GDPR (General Data Protection Regulation — общий регламент защиты [персональных] данных), и все сборщики персональных данных (по-нашему операторы) отвечают за утечку ПДн в размере до 4% годового оборота компании, при этом годовой оборот тщательно оценивается с учётом бизнеса в других странах. При этом в ЕС нет такой развитой нормативной базы, как у нас, но оператор регулярно и аккуратно оценивает риски и сам принимает решение, какие меры и средства защиты он будет использовать.

В последние годы всё чаще для защиты баз данных начинает применяться шифрование. И это является мировой тенденцией, на которую мы также пока не реагируем. Так же как на то, что, например, такое модное в России явление, как идентификация личности по её биологическим характеристикам, напрямую запрещено пунктом 1 статьи 9 GDPR. Давайте приведём её полностью: «Запрещена обработка таких персональных

К сожалению, в нашей стране для ПДн чаще применяется так называемая бумажная защита, а сами данные распространяются со скоростью развития интернета

данных, которые раскрывают расовую или этническую принадлежность, политические взгляды, религиозные убеждения или философские воззрения, членство в профсоюзе, также запрещена обработка генетических данных, биометрических данных для проведения уникальной идентификации физического лица, данных о здоровье, половой жизни или сексуальной ориентации физического лица. Государства — члены ЕС могут сохранять или вводить дополнительные условия, в том числе ограничения, в отношении обработки генетических данных, биометрических данных или данных о здоровье».

Здесь есть о чём поразмышлять. Может, нам пора подумать о назревших изменениях в 152-ФЗ и ряд смежных законов? Я говорю не о гармонизации с европейским регламентом, а об изменении подхода к защите наших персональных данных, ведь сейчас собираются данные о практически всём трудоспособном населении...

* * *

Отсутствие судебной практики и наличие в интернете уже сегодня почти исчерпывающей информации о подавляющем большинстве работающих граждан, к сожалению, объективно говорят о том, что 152-ФЗ не работает и подход надо менять. Нужен ли подвергшийся неконструктивной критике стандарт? Да, нужен. Хорошо «вылизанный» или не совсем доработанный, но, как и многие другие созданные мировым сообществом документы, он может помочь сформировать новый подход к защите персональных данных, как наших, так и наших детей.

Из двадцати (!) стандартов ИСО по защите персональных данных у нас сейчас переведён и действует только один (ГОСТ Р ИСО / МЭК 29100–2011), и вот появился второй (ГОСТ Р 59407–2021), об остальных восемнадцати вообще мало кто знает, а ведь при разработке нового подхода к защите персональных данных нам придётся на что-то опираться, при этом обычно мировой опыт учитывается в первую очередь.



**Василий
ОКУЛЕССКИЙ**
заместитель
начальника
службы ИБ банка
«Возрождение», к. т. н.

«ТАКИЕ СТАНДАРТЫ У НАС НЕ ЧАСТО ВСТРЕЧАЮТСЯ...»

Перед нами новый стандарт ГОСТ Р 59407–2021 «Базовая архитектура защиты персональных данных» из серии «Информационные технологии. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ». Во введении утверждается, что «Настоящий стандарт предоставляет описания высокоуровневой базовой архитектуры и соответствующих мер защиты персональных данных в информационных системах персональных данных» и далее: «Настоящий стандарт не устанавливает требования для политик защиты ПДн; предполагается, что политики приняты и что в рамках ИСПДн определены требования защиты ПДн, а также реализованы соответствующие меры защиты ПДн».

На этом месте можно было бы поставить точку и дальше документ не читать. Но любопытство скорее нас одолеет, чем лень. Поэтому всё-таки посмотрим, а что же там.

Сознаюсь сразу, я только после третьего прочтения понял (мне хочется в это верить), зачем нужен такой стандарт. Стандарт переводной, носит «информационный» характер (по словам одного из авторов стандарта). Предназначен в основном для разработчиков ИСПДн. Именно для них будет наиболее полезен этот новый взгляд на то, не КАК, а ЧТО нужно делать на каждом уровне инфраструктуры и в каждом типе информационной системы.

Такие стандарты у нас сейчас не часто встречаются.

У нас пока большая редкость система, изначально предназначенная для обработки ПДн, мы в основном имеем дело с системами, занимающимися обработкой ПДн для чего-то своего, и специальные требования там учитываются, как правило, только для основной функциональности.

Приведу пример. Система обрабатывает ПДн субъекта не сама по себе, есть пользователь системы, который что-то делает с данными. При этом:

- ◆ не проверяется наличие согласия именно этого субъекта на обработку именно этих данных;
- ◆ не проверяется соответствие заявленных в согласии целей обработки и фактической обработки;

◆ не всегда проверяется легитимность прав пользователя системы (подтверждение его личности, подтверждение его прав на возможность такого вида обработки);

◆ не ведётся протоколирование действий системы и пользователя;

◆ и т.д. и т.п.

Те, кто в силу служебных обязанностей занимается процессами обработки и защиты ПДн в организации, знают, как непросто бывает приводить работающие системы в соответствие с требованиями. Стандарт при внимательном прочтении и применении способен сильно облегчить проработку архитектуры и составляющих компонентов будущих ИСПДн и снять эту серьёзную проблему.

Предлагаю читателям провести домашнюю работу: выписать 3 самых болезненных проблемы в приведении в соответствие с нормативными документами одной ИСПДн, а затем посмотреть, как бы выглядели эти болезни, если бы разработчики использовали этот стандарт. Очень интересный эффект. Если вы напишете в журнал о ваших результатах, это будет жизненное предметное продолжение обсуждения стандарта и возможностей его применения.

Хочу отметить ещё один нюанс, который вызвал неоднозначную реакцию читателей. Появилась, по сути, новая сущность в предметной области — ИСПДн субъекта ПДн. Это требует осмысления. При этом при первом подходе к этой сущности понимаешь, что системы, в том числе компьютеры, планшеты, смартфоны и прочие гаджеты, с которыми непосредственно имеет дело пользователь, требуют специального рассмотрения.

Если значимость идентификации и аутентификации всех участников информационного взаимодействия не вызывает сомнения, то отдельная глава, посвящённая шифрованию, как универсальному средству защиты данных сильно преувеличивает его место и значение.

* * *

И в заключение хочу выразить благодарность авторам стандарта и статьи, и отдельную благодарность С. В. Вихореву за его вклад в совершенствование нормативной базы по защите информации.

КриптоПро NGate — это универсальный высокопроизводительный TLS-VPN сервер, позволяющий быстро и безопасно реализовать защищённый доступ к веб-сайтам и корпоративным ресурсам через незащищённые каналы связи, в том числе сети общего пользования.

NGate может быть особенно полезен субъектам КИИ, государственным органам, операторам персональных данных, финансовым и иным организациям, которым необходимо обеспечить защиту передаваемой информации и удаленного доступа

Поддержка ГОСТ и зарубежных алгоритмов

NGate обеспечивает поддержку TLS с ГОСТ наравне с зарубежными криптографическими алгоритмами. Это позволяет реализовать плавный перевод защиты доступа к веб-сайтам на ГОСТ.

Выполнение требований регуляторов

Серверные и клиентские компоненты NGate сертифицированы по требованиям к СКЗИ и имеют соответствующие сертификаты ФСБ России по классам КС1, КС2 и КС3. Это позволяет использовать NGate для защиты персональных данных (152-ФЗ) и иной конфиденциальной информации при передаче по незащищенным каналам связи, в том числе из-за пределов РФ (имеется нотификация ФСБ России). Кроме этого, NGate позволяет реализовать защищенные TLS-соединения при передаче биометрических ПДн в рамках соответствующих взаимодействий в ЕБС. В настоящее время NGate входит в состав нескольких типовых и частных решений по подключению к ЕБС.

Простая реализация контроля доступа к ресурсам

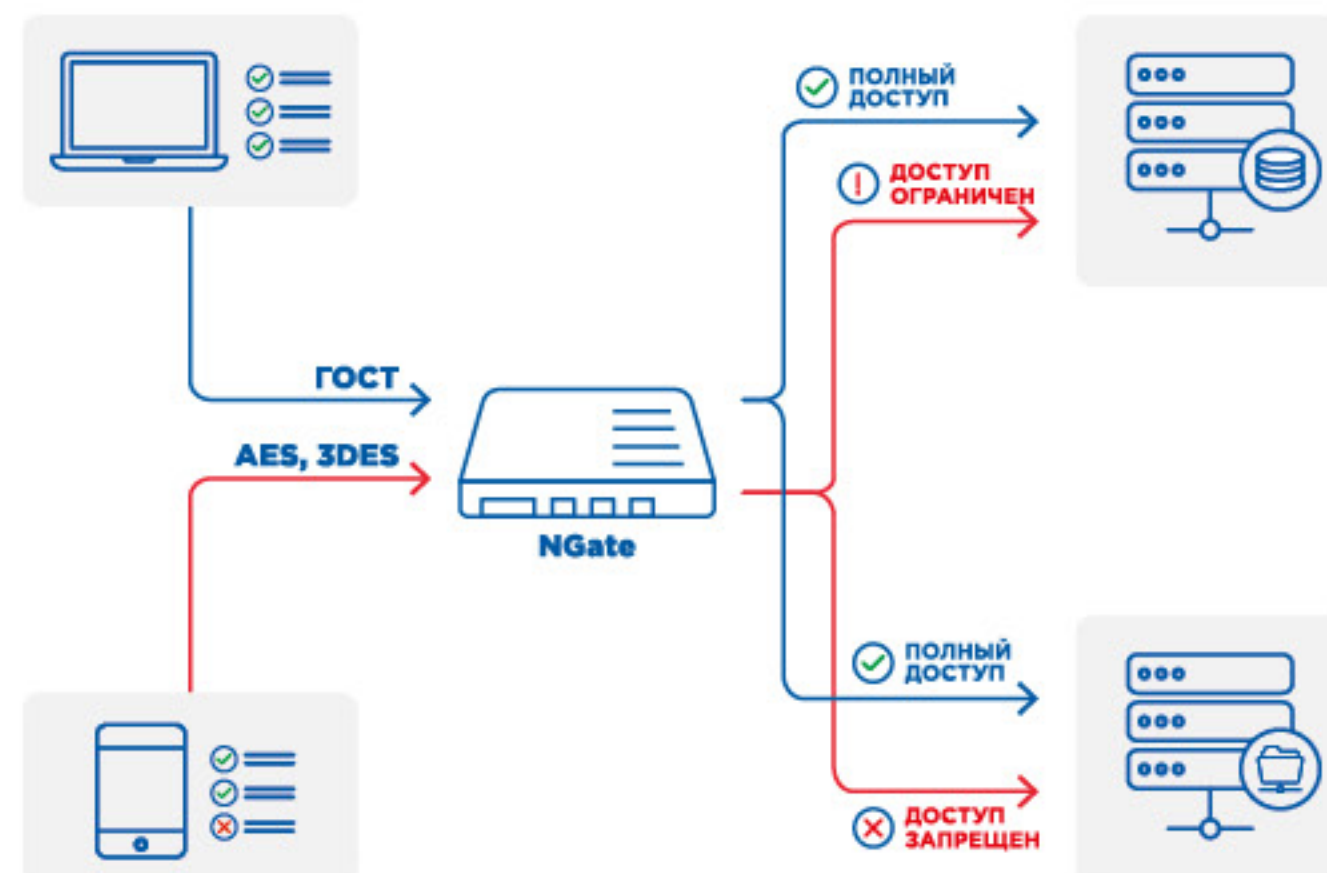
NGate обладает широкими возможностями по управлению доступом удалённых пользователей со строгой многофакторной аутентификацией по сертификату, LDAP/AD, Radius, а также гибким разграничением прав доступа к ресурсам.

Аутентификация с использованием токенов

NGate поддерживает различные аппаратные ключевые носители, такие как устройства Рутокен, eToken, JaCarta, ESMART и многие другие — в том числе с поддержкой российских криптографических алгоритмов.

Два режима работы

Режим TLS-сервера используется для безопасного подключения к веб-сайтам и другим веб-ресурсам и снятия нагрузки по обработке TLS-соединений с веб-серверов. В данном режиме NGate может использоваться для обеспечения безопасного доступа к государственным порталам, сайтам организаций, электронных торговых площадок и ДБО, а также в системах ВКС, телемедицины и др., предоставляющих доступ пользователей через веб-браузер. При этом доступ к веб-ресурсам возможен как напрямую без аутентификации, так и с аутентификацией через централизованной веб-портал, входящий в состав продукта.



Режим VPN-сервера используется для безопасного подключения с помощью VPN-клиента, поддерживающего все популярные платформы (Windows, macOS, Linux, iOS, Android, Sailfish) к произвольным корпоративным ресурсам, в том числе к информационным системам, файловым ресурсам, удаленному рабочему столу и т.д. При этом разграничение доступа возможно на уровне подсетей, в том числе виртуальных (VLAN).



Архитектура

Решение состоит из серверной (шлюз) и клиентской частей (VPN-клиент или браузер). Кроме этого, в состав решения входит центр управления сетью (ЦУС). Для небольших организаций шлюз и ЦУС могут быть установлены как единое решение на одну аппаратную или виртуальную платформу.

Масштабируемость

Один узел шлюза NGate держит до 45000 соединений с обработкой информационных потоков до 20 Гбит/с в режиме TLS-сервера. Данные характеристики легко увеличить добавлением новых узлов (до 32 штук) в кластер.

**Кирилл КУЗЬМИН**

руководитель
направления
«Развитие открытых
API» Ассоциации
ФинТех

ОТКРЫТЫЕ API: СОЕДИНЕНИЕ УСТАНОВЛЕНО

РОССИЙСКИЙ ФИНАНСОВЫЙ РЫНОК
СОВЕРШИЛ «БРОСОК» В СТОРОНУ
ОТКРЫТОГО БАНКИНГА

Сама технология API (application programming interface, программный интерфейс приложения) существует уже давно и хорошо знакома пользователям таких сервисов, как Amazon, Google, Facebook, «Яндекс». Например, API предоставляет возможность сторонним разработчикам подключиться к серверу компании и получить доступ ко всем необходимым данным для интеграции в свои приложения (прогноз погоды, стоимость акций, фотографии из соцсетей и т.д.). Это удобный и надёжный способ обмена информацией, который широко используется разработчиками и компаниями во всём мире.

Если говорить о финансовом рынке, то благодаря открытым API банки получают доступ к новейшим технологическим сервисам, не тратя время и внутренние ресурсы на их разработку. Финтех-компаниям (а также бигтехам и другим игрокам) Открытые API позволяют многократно сократить время и стоимость вывода на рынок своих разработок.

Так, с помощью открытых API банки, финтехи и другие игроки смогут, например, создать универсальное мобильное приложение для клиентов по управлению финансами в нескольких организациях или настроить онлайн-оплату товаров и услуг через партнёрские приложения.

Клиенты финансовых организаций благодаря открытым API получают новые сервисы и приложения, а качество и скорость существующих услуг возрастут.

Важно, что в среде открытого банкинга пользователи сами управляют своими данными: решают, какой информацией и с какой компанией поделиться, на какой срок разрешить доступ, и могут отозвать согласие в любой момент.

Открытый банкинг оказывает значительное влияние на финансовые рынки ведущих стран мира. Великобритания, США, Сингапур, Гонконг, Австралия — это неполный список государств, в которых регуляторы развивают режим открытого банкинга, а также постепенно расширяют его на других участников финансового рынка (страховые компании, пенсионные фонды, МФО и др.).

ФОРМИРОВАНИЕ СРЕДЫ

В России в настоящее время идёт активное формирование среды открытых API на финансовом рынке — частично уже пройден такой важный этап, как стандартизация. К настоящему моменту Банк России выпустил следующие стандарты открытых API¹:

- ◆ Открытые банковские интерфейсы. Общие положения;
- ◆ Открытые банковские интерфейсы. Получение информации о счёте клиента третьей стороной;
- ◆ Открытые банковские интерфейсы. Инициирование перевода денежных средств клиента третьей стороной в валюте Российской Федерации;
- ◆ Безопасность финансовых (банковских) операций. Прикладные программные интерфейсы обеспечения безопасности финансовых сервисов на основе протокола OpenID;

¹ <https://cbr.ru/fintech/acts/>

*Открытый банкинг оказывает
значительное влияние на финансовые
рынки ведущих стран мира.
Великобритания, США, Сингапур,
Гонконг, Австралия — это неполный
список государств, в которых регуляторы
развивают режим открытого банкинга*

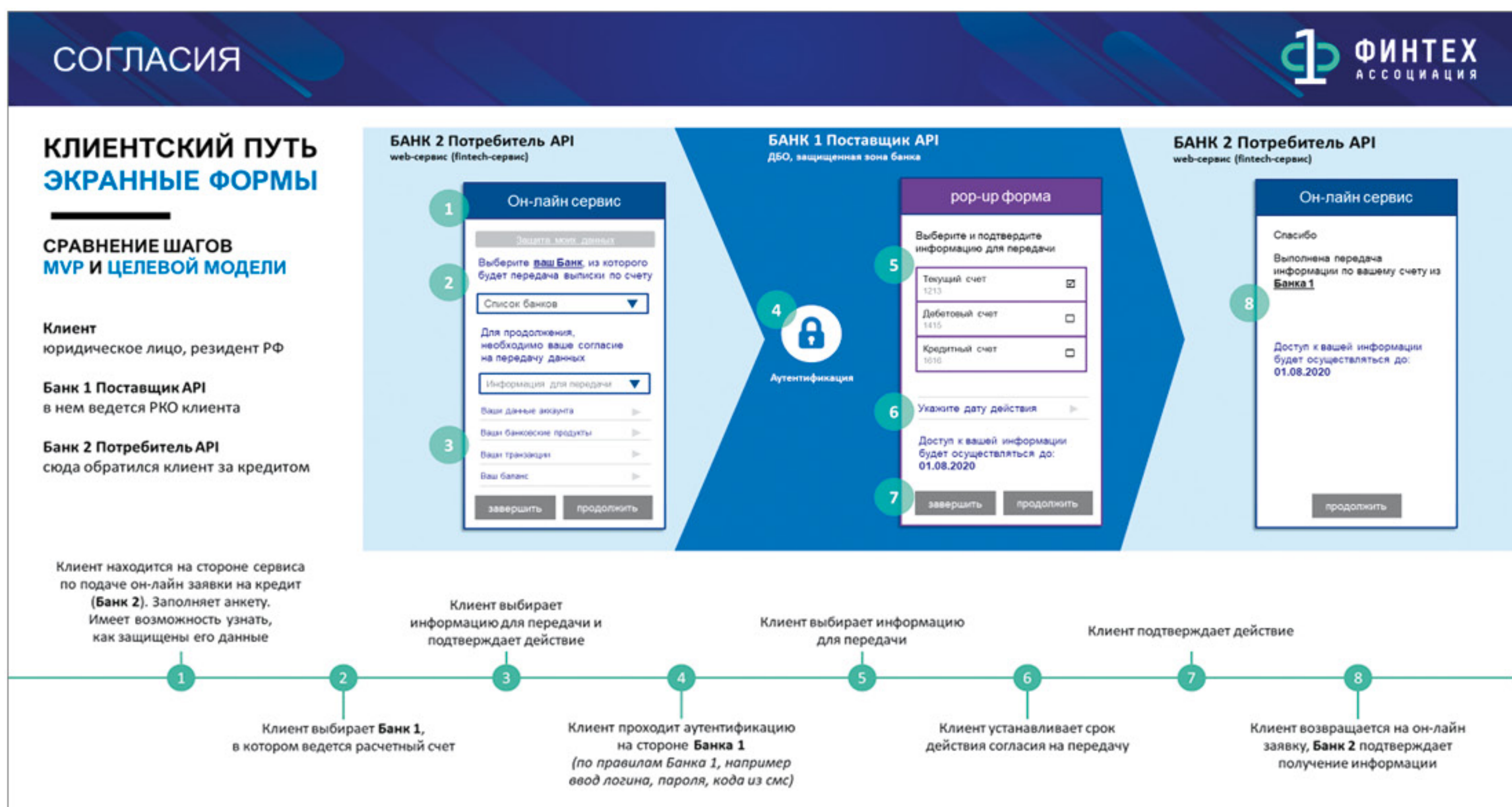


Схема механизма клиентского согласия. Все операции по обмену данными производятся исключительно с согласия клиента. На схеме изображено, как может выглядеть механизм получения согласия на передачу сведений

♦ Безопасность финансовых (банковских) операций. Прикладные программные интерфейсы. Обеспечение безопасности финансовых сервисов при инициации OpenID Connect клиентом потока аутентификации по отдельному каналу. Требования;

♦ Открытые банковские интерфейсы. Получение публичной информации о кредитной организации и её продуктах.

Стандарты открытых API в финансовой сфере являются рекомендательными как для банков, так и для финтех-компаний и других организаций, которые хотят взаимодействовать между собой для предоставления клиентам услуг и сервисов.

На площадке Ассоциации ФинТех создана инфраструктурная основа доверенной среды открытого банкинга. Действует сертификационный стенд, где участники проходят проверку на соответствие стандартам открытых API, а также информационный портал, объединяющий актуальную информацию и международный опыт в сфере открытого банкинга.

Среда открытого банкинга строится с учётом требований стандарта СТО БР ФАПИ.СЕК-1.6–2020, соответствующих требованиям ГОСТ, и OpenID Foundation (OIDF) — одной из лидирующих мировых организаций в области децентрализованных систем аутентификации. Это позволяет обеспечить максимальную защиту передаваемых данных и совершаемых операций.

Стандарты открытых API в финансовой сфере являются рекомендательными как для банков, так и для финтех-компаний и других организаций

В среде проходят технические проверки не только участники, выставяющие API, но и сервисы, использующие эти API (финтех-компании). Компания, не прошедшая технические проверки, не сможет подключиться к сервисам среды открытых API.

Первыми участниками, прошедшими проверки на сертификационном стенде, стали «Точка» и Промсвязьбанк. Также к среде подключился СКБ-банк. Запущены пилотные проекты по обмену выписками со счетов юрлиц и физлиц. На стадии подготовки находится ещё ряд пилотов.

* * *

Ассоциация ФинТех приглашает участников рынка к обсуждению стандартов открытых API и участию в пилотных проектах. Использование открытых программных интерфейсов в России станет связующим элементом современной цифровой финансовой системы и позволит обеспечить недискриминационный доступ провайдеров услуг к финансовой инфраструктуре.



**Александр
ВИНОГРАДОВ**
специалист Службы
ИБ КБ «Максима»



**Оксана
ДОКУЧАЕВА**
главный специалист
отдела мониторинга
и оценки рисков
сетевой безопасности
Дирекции
информационно-
технологических
систем и систем связи
ГУП «Московский
метрополитен»



**Анастасия
НИКОЛАЕВА**
начальник
Службы ИБ
КБ «АРЕСБАНК»

НЕ ПОДСТЕЛИЛИ СОЛОМКИ...

ПОЧЕМУ БАНКИ ОКАЗАЛИСЬ НЕ ГОТОВЫ К РЕЖИМУ САМОИЗОЛЯЦИИ?

В марте 2020 года мы узнали, что мир не будет прежним. Пандемия коронавируса внесла коррективы во все сферы жизни. Коснулись они и банковских организаций.

УКАЗОВ БЫЛО МНОГО

Согласно указу Президента России с 30 марта 2020 г. была объявлена неделя нерабочих дней для всей страны. Вскоре этот указ был дополнен другим — № 239 «О мерах по обеспечению санитарно-эпидемиологического благополучия населения на территории Российской Федерации в связи с распространением новой коронавирусной инфекции (COVID-19)», установившим нерабочие дни с 4 по 30 апреля включительно.

Указ № 239 не распространялся на ряд организаций, в т.ч. организации, предоставляющие финансовые услуги в части неотложных функций (в первую очередь услуги по расчётам и платежам), при этом вводил ограничения на передвижение и давал право органам власти проводить дополнительные комплексы ограничительных и иных мероприятий, направленных на обеспечение санитарно-эпидемиологического благополучия населения, в том числе в условиях введения режима повышенной готовности, чрезвычайной ситуации.

5 марта 2020 года мэр г. Москвы издал Указ № 12-УМ «О введении режима повышенной готовности», согласно которому работодатели должны были обеспечить измерение температуры тела работникам на рабочих местах с обязательным отстранением от нахождения на рабочем месте лиц с повышенной температурой, а также оказывать работникам содействие в обеспечении соблюдения режима самоизоляции на дому.

Данный Указ неоднократно дополнялся, что прибавляло работодателям новых обязанностей, например перевести граждан, обязанных соблюдать режим самоизоляции, на дистанционный режим работы или предоставить им ежегодный оплачиваемый отпуск,

В свою очередь, Роспотребнадзор издал Письмо от 10 марта 2020 г. «О мерах по профилактике новой коронавирусной инфекции

(COVID-19)», согласно которому работодателям рекомендовалось, в частности, обеспечить:

- ♦ возможность обработки рук кожными или дезинфицирующими салфетками с установлением контроля за соблюдением этой гигиенической процедуры;

- ♦ контроль температуры тела работников при входе в организацию (предприятие) и в течение рабочего дня (по показаниям) с обязательным отстранением от нахождения на рабочем месте лиц с повышенной температурой тела и с признаками инфекционного заболевания;

- ♦ качественную уборку помещений с применением дезинфицирующих средств вирулицидного действия, уделив особое внимание дезинфекции дверных ручек, выключателей, поручней, перил, контактных поверхностей, мест общего пользования;

- ♦ наличие в организации не менее чем пятнадцатидневного запаса дезинфицирующих средств для уборки помещений и обработки рук сотрудников, средств индивидуальной защиты органов дыхания на случай выявления лиц с признаками инфекционного заболевания (масок, респираторов).

НОВЫЕ ПРАВИЛА И ПРОЦЕССЫ

Безусловно, следующие один за другим указы и рекомендации легли на организации тяжёлым бременем, как финансовым, так и организационным.

В связи с новыми условиями необходимо было менять правила работы. Банк России издал опросник про выполнение требований Указа мэра Москвы о переводе сотрудников банков на дистанционную работу. Данное письмо потребовало от руководства банков созыва экстренных заседаний ввиду ограниченности сроков исполнения и неготовности банковско-технологических процессов к дистанционной или посменной работе.

Таким образом, банкам пришлось перестраивать свои бизнес-процессы под новые реалии и решать такие проблемы, как организация посменной работы либо «домашних офисов», обеспечение сотрудников на дистанционной работе необходимой техникой и каналами связи, незапланированные расходы на обеспечение

указанных процессов, недостаток сотрудников, присутствующих очно и т.п.

Кроме того, основные процессы ИТ и ИБ были приостановлены, поскольку было необходимо решать задачи, поставленные руководством, в связи с требованиями вышеуказанных нормативно-правовых актов.

ЧТО ДЕЛАТЬ?

Перед руководством банков встал ряд насущных вопросов. Сколько сотрудников можно отправить на дистанционную работу, не нарушая бизнес-процессы и существующие нормативно-правовые акты? Сколько сотрудников могут работать посменно? Как менять расписание работы в случае заболевания сотрудника, работавшего очно, с учётом требований самоизоляции лиц, контактировавших с заболевшим? Как организовать техническое и организационное обеспечение дистанционной работы с учётом принятых годовых бюджетов? К какой категории отнести и как выделить бюджет для расходов на маски, перчатки, антисептики, ПЦР-тесты и т.п.?

ДАЛЬШЕ — БОЛЬШЕ

В ходе применения дистанционного режима работы возникли проблемы. Пострадали процессы с применением электронной подписи, отправка и приём платежей, взаимодействия с клиентами, телефонией — потребовалась перенастройка телефонии (АТС) и др.

Требовалось определить, как правильно выстроить процессы с ПС БР, удалённый доступ к которой запрещён регулятором, в связи с чем руководитель был обязан обеспечить физическое присутствие в офисе как минимум четырёх работников, что стало болезненным моментом для небольших банков, особенно в случае заболевания даже одного сотрудника. Аналогичные проблемы коснулись, например, SWIFT.

Проявились трудности с контролем рабочего времени работников, в том числе из-за отсутствия регуляторных механизмов. Также из-за большого числа отвлекающих факторов при работе вне офиса возросло число ошибок и некачественно выполненных должностных обязанностей.

Ввиду использования для видеоконференций популярных платформ, чья надёжность сомнительна (Zoom, Teams, Skype и др.), повысился риск утечки информации. Также риск утечек возрос и в связи с вероятностью утраты рабочих устройств вне офиса.

Отдельно отметим неготовность внутренних документов, регламентирующих в банках режим работы такого рода.

ПУТИ РЕШЕНИЯ

В связи с тем, что бюджеты банков, как правило, формируются в начале года, статьи расходов на организацию дистанционной работы в 2020 году в них не были представлены. Решать вопросы приходилось имеющимися подручными средствами — бесплатное программное обеспечение, снижение уровня защиты в пользу удешевления, использование резервных средств и т.д. и т.п.

При дистанционной работе в основном применялись следующие решения.

1. VPN между АРМ сотрудника и домашним компьютером. При этом следует иметь в виду, что устанавливать банковское ПО на домашние компьютеры запрещено.

2. Виртуальная машина, к которой сотрудники подключались дистанционно, а она, в свою очередь, подключалась к рабочим АРМ для исключения заражения ВПО и возможных утечек информации. Виртуальная машина создавалась только на сеанс работы и при завершении сеанса осуществляла сброс к первоначальным настройкам. Для этого требовалось провести настройку личных компьютеров.

3. Другие решения. Назовём их «местные ноу-хау».

Вне зависимости от выбора решения, используемое устройство становилось непригодным для применения в личных целях, что приводило к конфликту между сотрудником и руководством банка.

ВЫВОДЫ

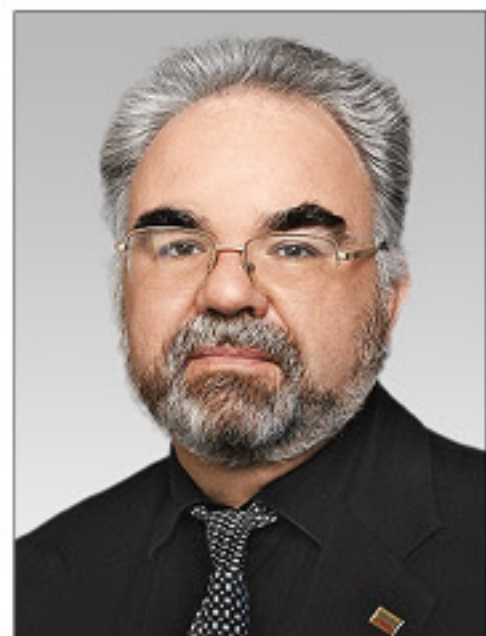
Возникшая форс-мажорная ситуация показала отсутствие гибкости в банковско-технологических процессах, что, с одной стороны, обусловлено необходимостью следовать высоким стандартам обеспечения безопасности, с другой — отсутствием соответствующих подобной ситуации регуляторных механизмов.

Для предотвращения либо минимизации последствий таких проблем в будущем желательно:

- ♦ регулятору в лице Банка России предоставить банкам рекомендации по правильной организации дистанционной работы и разработать соответствующие нормативные акты; предоставить банкам информацию о лучших практиках технической организации удалённого доступа;
- ♦ банкам провести самооценку на предмет соответствия требованиям, созданным в рамках вышеуказанного процесса; предоставить руководителю варианты решения возникших проблем, в т.ч. по изменениям нормативных документов банка, в т.ч. плана ОНВД; проработать бюджет на предмет возможных форс-мажорных ситуаций схожего рода.

РАЗБЕГАЮТСЯ ГЛАЗА

КАКУЮ МОДЕЛЬ ФУНКЦИОНИРОВАНИЯ SOC ВЫБРАТЬ?



**Алексей
ЛУКАЦКИЙ**
эксперт BIS Journal

На многих мероприятиях, связанных с центрами мониторинга и реагирования на инциденты, очень часто противопоставляются две модели организации SOC — целиком собственный и внешний, коммерческий, которому функция мониторинга передаётся на аутсорсинг. У каждой из этих полярных позиций есть свои сторонники и противники. Сторонники коммерческих SOC, которые, как правило, в этих центрах и работают, ратуют за то, что они оказывают профессиональные услуги в режиме 24×7 и имеют в штате высококлассных аналитиков и специалистов. Сторонники противоположной позиции считают, что, строя собственный SOC, не будут утеряны компетенции сотрудников, а также не будет потерян контроль над достаточно чувствительной информацией. Кто же прав? Какой из двух вариантов построения SOC является правильным?

Участвуя в полутора десятках проектов по построению или аудиту центров мониторинга, а также имея доступ к базе данных по сотне коммерческих и такому же количеству построенных SOC, могу сказать, что неправы обе стороны. Да, это звучит парадоксально, но это так. Дело в том, что существует гораздо больше моделей построения SOC, чем названные две, и выбирают они с опорой на множество факторов, которые надо принимать в расчёт. Давайте попробуем в них разобраться и в итоге ответить на вопрос, какой из множества моделей отдать предпочтение. Но для начала я попрошу вас ответить на 5 вопросов:

1. У вас есть адекватный бюджет для построения и управления SOC?
2. У вас достаточно квалифицированных специалистов для построения и управления SOC?
3. Как вы планируете сохранить ваших сотрудников SOC?
4. У вас есть место для SOC?
5. У вас есть программа обучения, позволяющая поддерживать уровень компетенций сотрудников SOC?

МОДЕЛЬ «МОГУ И ХОЧУ»

Это та модель, когда мы имеем и возможности, и ресурсы для построения собственного центра мониторинга. В этом случае мы покупаем нужные инструменты или создаём их своими руками, нанимаем высококлассных аналитиков и

разрабатываем для них как план обучения, так и карьерный путь развития (а иначе они уйдут от нас, когда поднаберутся опыта), мы покупаем подписку на сервисы Threat Intelligence. При этом мы готовы к достаточно небольшой скорости развёртывания собственного центра — обычно этот срок занимает от года и выше, и это ещё оптимистичная оценка. SOC постоянно развивается, и на достаточно зрелый уровень он выходит только через 2–3 года эксплуатации.

Считается, и это неслучайно, что основные затраты при построении собственного SOC приходятся на закупку решений, составляющих технологический стек будущего центра мониторинга — SIEM для сбора сигналов тревоги, SOAR/IRP для управления инцидентами и автоматизации реагирования, TIP для обработки данных об угрозах, платформу для взаимодействия аналитиков и членов команды реагирования, платформу для хранения и обмена знаниями. SOC нового поколения также включает, помимо SIEM, ещё и решение по анализу сетевого трафика (NTA или NDR), решение по мониторингу активности на конечных устройствах (EDR), а также при необходимости решение по мониторингу облачных сред (CASB). Если добавить сюда различные утилиты для проведения форензики (анализа памяти, реверс-инжиниринга), хранилище данных, сервера и персональные компьютеры, то сумма выходит достаточно кругленькая.

Отчасти поэтому, чтобы снизить риски санкций (как американских, мешающих использованию некоторых отечественных решений, так и российских, называющихся «импортозамещением»), а также для получения большей гибкости в решаемых задачах, многие компании строят свои SOC на компонентах open source (например, связка ELK + MISP + The Hive), а также используют иные способы экономии (рис. 1).

А ведь в собственном SOC нам надо ещё посчитать фонд оплаты труда для недешёвых аналитиков, работающих в 2–3 смены, их обучение, мебель, помещение и даже шредеры для уничтожения бумаг. В целом собственный SOC — это удовольствие недешёвое.

МОДЕЛЬ «ХОЧУ, НО НЕ МОГУ»

На противоположной стороне у нас находится аутсорсинговый SOC, услугами которого мы пользуемся, чтобы снять с себя все хлопоты по мониторингу и реагированию на инциденты.



Рисунок 1. Экономические аспекты оценки модели построения SOC

Параметр	Свой SOC	Чужой SOC
Контроль и подотчётность	Полные	Частичные
Гибкость в настройке под свои нужды	Высокая	Стандартные сервисы и стандартный SLA
Знание локального окружения	Высокое	Низкое или отсутствует
Скорость развёртывания	От полугода (обычно 2–3 года)	2 месяца
Режим работы	Обычно 5×8	Обычно 24×7
Возможности по реагированию	Максимальные	Средние
Масштабирование	Среднее	Высокое
Уровень компетенций	Средний	Высокий
Форма затрат	CapEx	OpEx
Предсказуемость затрат	Непредсказуемый	Предсказуемый
Гарантии (финансовые и т.п.)	Отсутствуют	Возможны
Зависимость от каналов связи	Средняя	Очень высокая
Хранение событий безопасности	Локально	За пределами организации
Права на технологии и процессы	Принадлежат заказчику	Принадлежат аутсорсеру
Выход за пределы своей организации	Невозможен	Возможно использовать данные по другим заказчикам
Видимость «брёвен в своём глазу»	Низкая	Высокая
Выделенный персонал	Да	Нет

Рисунок 2. Сравнение двух основных подходов к построению SOC

В этом случае все описанные ранее затраты у нас ложатся на выбранного партнёра, а мы уходим от модели капитальных затрат к операционным, которые выплачиваются небольшими частями ежегодно или ежеквартально; последний

вариант, однако, у нас в регионе не очень развит. Учитывая полную противоположность этой модели, можно даже привести таблицу их сравнения, которая покажет плюсы и минусы обоих вариантов (рис. 2).

Вроде бы кажется, что аутсорсинговый SOC обладает всеми преимуществами и не имеет недостатков, но это не так. Во-первых, в этом варианте построения центра мониторинга мы со временем теряем собственные компетенции и, если нам придётся по каким-то причинам расстаться с выбранным партнёром, мы останемся у разбитого корыта — никто нам уже не поможет оперативно разобраться с нашими инцидентами ИБ. Во-вторых, аутсорсинговый SOC всё равно требует контроля со стороны заказчика, что также требует и определённого инструментария, и персонала, который будет как минимум проводить анализ защищённости SOC (пентестеры или red team), а также оценивать результаты работы внешнего SOC и быть посредником между ним и внутренней ИТ-службой, которая должна будет реализовывать рекомендации по реагированию на инциденты и устранению причин, к ним приведших. В-третьих, любая внешняя организация гораздо хуже разбирается в вашей внутренней инфраструктуре, бизнес- и иных процессах, и поэтому реакция на некоторые инциденты может быть не всегда той, которую вы ждёте или которая лучше всего подходит к вашей ситуации. В-четвёртых, любая внешняя компания предлагает обычно типизированные сервисы, которые подходят большинству заказчиков. Если вы захотите чего-то особенного и выходящего за рамки привычных услуг SOC или их наполнения, то вам придётся раскошелиться — на коннекторы к вашим бизнес-системам, на особые условия реагирования (например, для изолированных систем), на написание собственных правил обнаружения и т.п. Ну и, наконец, не забывайте, что канал связи с вашим аутсорсинговым SOC может вдруг выйти из строя, снизится его пропускная способность или качество обслуживания, что тоже повлияет на оказываемые вам услуги SOC.

По опыту могу сказать, что аутсорсинг часто является промежуточным этапом при построении собственного SOC. Пользуясь услугами внешнего провайдера, мы изучаем процессы мониторинга и реагирования, обращаем внимания на сильные и слабые стороны этих процессов, перенимаем опыт и формируем собственный экспертный опыт, чтобы через несколько лет уже целиком строить свой центр мониторинга.

МОДЕЛЬ «ЕСТЬ ЧЕМ, НО НЕ С КЕМ»

Но существуют и иные модели организации центров мониторинга. Например, нередко ситуация, когда в организации есть весь необходимый инструментарий для сбора сигналов тревоги и расследования инцидентов, но нет людей для этого. Причём причиной может быть как

нехватка денег на квалифицированные кадры, так и внутренняя политика компании, которая имеет чётко определённую численность разных подразделений и не может увеличивать её по своему желанию. В этом случае у нас получается SOC по модели «Managed SIEM» (условное название), в котором мы берём от внешнего SOC только персонал (аутстаффинг), который либо располагается на нашей территории, либо подключается к нашим техническим решениям удалённо.

В этой модели промежуточного SOC основной головной болью будет контроль персонала, получившего доступ к нашей инфраструктуре гораздо более глубокий, чем в случае с аутсорсингом, при котором аналитики и специалисты по реагированию работают с инструментарием, расположенным на своей территории. Кроме того, придётся открывать большее число каналов для доступа к SIEM, IRP, TIP и т.п., что может быть небезопасно, особенно если злоумышленники сначала атакуют провайдера услуг SOC, а через него уже и самих его заказчиков. По данным SOC Секретной службы США, начиная с 2019 года число атак на провайдеров услуг многократно возросло (только в 2019-м их было более 60). Размещение внешнего персонала на своей территории в этом случае выглядит предпочтительнее, но тогда придётся задуматься о выделении отдельного помещения, а то и не одного, для этих людей.

МОДЕЛЬ «ЕСТЬ С КЕМ, НО НЕЧЕМ»

Четвёртая распространённая модель построения SOC заключается в том, что у компании могут быть квалифицированные специалисты, но нет ресурсов на закупку дорогостоящих коммерческих SIEM, SOAR, TIP и т.п. В этом случае нам остаётся либо осваивать open source (в таком случае эта модель превращается в первую), либо обращаться к услугам инструментов, развёрнутых в облаке (условно эту модель можно назвать SIEM-as-a-Service). Последний вариант, кстати, является достаточно неплохой альтернативой в случаях, когда вы редко сталкиваетесь с продвинутыми злоумышленниками, а про государственных хакеров слышали только по ТВ или читали в Интернете. В этом случае вам необязательно строить дорогостоящий SOC, но функции мониторинга и анализа событий безопасности вам всё равно нужны.

Эта модель позволяет быстро проверять новые возможности и гипотезы без установки нового ПО (достаточно просто «на время» арендовать услугу из облака). Отсутствие необходимости установки ПО (а по статистике 45 % компаний тратит только на внедрение SIEM



Рисунок 3. Четыре основных модели построения технологического стека SOC

	Свой SOC	Аутсорсинговый SOC	Облачная SIEM/SOC-платформа
Стоимость	\$\$\$	\$ \$	\$
Зависимость от административного персонала	+	+++	++
Зависимость от собственных аналитиков	+	+++	+
Гибкость	+++	+	++
Чувствительность к законодательству	+++	++	+
Требования к каналам связи	++	+	+
Контроль	+++	+	+++
Время внедрения	+	++	+++

+ - плохо ++ - хорошо +++ - отлично

Рисунок 4. Экспресс-сравнение основных моделей построения технологического стека SOC

более 3 месяцев) также снимает с нас головную боль по его масштабированию, обновлению, устранению уязвимостей и т.п. Также в зависимости от выбранной платформы в неё уже могут быть встроены различные плейбуки (дежурные процедуры реагирования), представлен каталог сценариев (use case), применяться инструментарию обогащения событий и т.п.

ЧЕТЫРЕ МОДЕЛИ

В итоге у нас получается четыре основных модели построения центра мониторинга и реагирования на инциденты ИБ, из которых Managed

SIEM является наиболее редкой. И у каждой из этих моделей есть свои преимущества и недостатки, которые не дают однозначного выбора в пользу одной из них (рис. 3, 4).

МОДЕЛЬ «ВСЕГО ПОНЕМНОГУ»

Но не стоит думать, что этими четырьмя моделями всё ограничивается. На самом деле существуют и различные промежуточные варианты, которые находятся где-то между всеми этими моделями. Например, мало кто содержит собственных специалистов по реверс-инжинирингу вредоносного ПО. Эта функция отдаётся обычно на

аутсорсинг, и то не на постоянной основе, а эпизодически, по мере появления ранее неизвестного ПО, которое вызывает подозрения, но на которое никак не реагирует имеющаяся песочница.

Другой пример. Согласно статистике некоторых российских коммерческих SOC число их заказчиков, выбравших не только мониторинг, но ещё и реагирование на выявленные инциденты, невелико — всего около 15 %. Иными словами, 85 % пользователей аутсорсинговых SOC отдают только мониторинг, но реагирование оставляют за собой, что требует не только соответствующих инструментов, но и специалистов.

Третий вариант гибридной модели заключается в том, что на стороне внешнего SOC реализуется только первая линия анализа событий безопасности, которые после обработки, классификации, приоритизации и объединения в инциденты, попадают на вторую и третью линию, расположенную уже на стороне заказчика. Кстати, возможен и противоположный вариант — первичный анализ осуществляется на стороне заказчика, а анализ со стороны более квалифицированных аналитиков требует привлечения внешнего SOC. А анализ в нерабочее время, выходные и праздничные дни? Кто его осуществлять будет, если у вас нет возможности обеспечить работу центра в режиме 7×24, а только в режиме 5×8?

А ведь мы рассмотрели только основные услуги, которые оказывает SOC, — мониторинг и реагирование на инциденты. А redteam'инг или фишинговые симуляции, которые тоже могут входить в сервисный каталог центра мониторинга?

ЧТО ВЫБРАТЬ?

Какую же тогда модель центра мониторинга и реагирования на инциденты выбрать? Какая из них будет более правильной? Может показаться, что ответа нет, но это не так. Он есть, и называется он «сервисная стратегия SOC». В ней определяются все исходные данные, которые влияют на выбор модели, — имеющиеся ресурсы, ожидания, желаемые результаты и сроки их достижения, распределённость компании и функционирование в разных часовых поясах и юрисдикциях, наличие инсорсинговой компании в холдинге, временные параметры, модель нарушителя, требования законодательства, квалификация персонала, возможности ИТ-службы, зависимость бизнеса от информационных технологий, культура компании. И это только часть вопросов, которые повлияют на решение о том, какой модели SOC надо придерживаться (рис. 5).

* * *

Главное, задать эти вопросы в самом начале пути под названием «центр мониторинга и реагирования на инциденты ИБ». Именно ответы на них позволят не только определить модель функционирования SOC, но и оказываемые им сервисы, ключевые процессы, необходимые для их реализации, оргштатную структуру и режим работы аналитиков SOC, программу их обучения и т.п. И только в самом конце мы подойдём к вопросу архитектуры SOC и технологического стека, лежащего в её основе. И только в таком порядке. Удачи вам на этом непростом пути!

Видение стратегии	Драйвера, ожидания заказчика, ключевые принципы и ожидаемый результат
Резюме по сервисам	Описание сервисов SOC – модель реализации, владелец, вход и выход для сервиса, компоненты
Ключевые процессы	Описание ключевых процессов, необходимых для реализации сервисов SOC
Организационная стратегия	Описание структуры команды SOC и всех ролей
Технологическая стратегия	Описание технологического стека SOC

Рисунок 5. Компоненты сервисной стратегии SOC

DEVSECOPS. ПОКА НЕ ПОПАЛ ВПРОСАК

УЗНАТЬ, ПРИНЯТЬ, НАЧАТЬ МОНИТОРИТЬ

Цифровая трансформация для служб ИБ вылилась в создание новой области защиты — непрерывной разработки и интеграции (или CI/CD). Безопасность CI/CD в народе стали называть DevSecOps, ну а мы посмотрим, с какого боку к DevSecOps подойти обычному корпоративному безопаснику, который традиционно занимается обеспечением безопасности на уровне ИТ-инфраструктуры и комплаенса. Также посмотрим на DevSecOps и с точки зрения обеспечения безопасности ИТ-инфраструктуры и прикладных сервисов для разработки. Вопросы Secure Software Development Lifecycle в фокус обзора не попадут.

Чтобы не изобретать велосипед, применим проверенный фреймворк NIST Cybersecurity Framework, то есть используем последовательность управления ИБ Identify-Prevent-Detect-Respond-Recover.

IDENTIFY

В CI/CD мы можем выделить целый ряд новых для служб ИБ объектов защиты. Выделим девять ключевых.

Системы управления задачами и процессами разработки (Trello, Jira и др.) — позволяют организовать совместную работу в одной команде и между командами. В них зачастую хранятся бизнес-требования, могут лежать секреты, а иногда их без согласования с ИБ используют в облачном варианте. После чего происходят истории вроде публичного доступа к тысячам досок в Trello¹.

Системы управления знаниями (Confluence, Notion и др.) — хранят различные материалы и позволяют совместную работу над документами и статьями. Основные проблемные ситуации аналогичны предыдущим, плюс отсутствие резервных копий.

Системы хранения кода и конфигурации (Gitlab, CircleCI и др.) — хранят программный код и конфигурации, обеспечивая

версионирование изменений, ревью коммитов (изменений) старшими разработчиками, возможность отката изменений и в целом обеспечивая подход инфраструктура-как-код (Infrastructure-as-a-Code). Основные проблемные ситуации — отсутствие резервных копий, отсутствие настроек ролевой модели, хранение секретов в открытом виде.

Системы сборки кода и организации развёртывания (Gitlab, Jenkins) — обеспечивают сборку кода в артефакты (полуфабрикаты программного обеспечения), которые в дальнейшем могут быть развёрнуты на основе, например, Docker образов. Основные проблемные ситуации — отсутствие интеграции security-проверок кода (SAST, DAST, SCA), проверка хранения секретов в открытом виде, проверка Docker-образов на уязвимости.

Системы хранения артефактов / Docker registry (собранный код, Docker образов — JFrog Artifactory / harbor, docker hub) — хранят в себе артефакты / Docker images, массово используются корпорациями всего несколько лет, из-за чего мало кто понимает, какие там роли в целом существуют и как их настраивать. Зачастую используются из облака (docker hub) или в гибридном режиме, добавляя риск автоматического подтягивания в наши образы произвольных библиотек без какой-либо проверки службой ИБ или любым другим сотрудником. Пример такой ситуации: симуляция тайпсквоттинг-атаки на PayPal, Microsoft и 33 другие компании, где атакующий залил вредоносный код в публичные репозитории с названием, похожим на легитимные зависимости². Кстати, 99,5 % организаций, по ощущениям автора, ещё даже не планируют забирать логи из артефактория, более того, даже не хотят понимать, куда уходят наши артефакты.

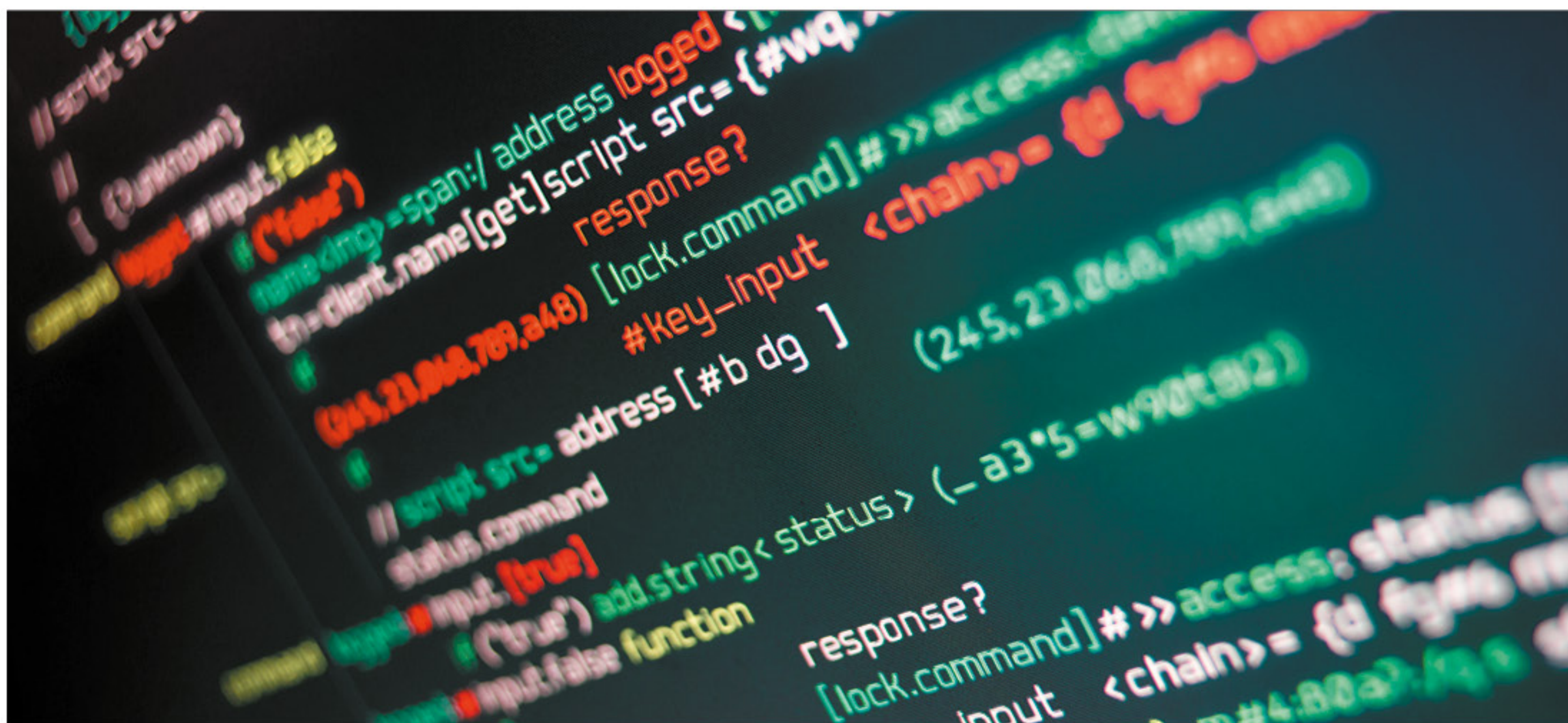
Системы оркестрации контейнеризации (Kubernetes, OpenShift) — предоставляют новую генерацию уровня абстракции для



**Александр
БОДРИК**
эксперт BIS Journal

¹ Апрель 2021, <https://www.kommersant.ru/doc/4781538>

² <https://www.bleepingcomputer.com/news/security/researcher-hacks-over-35-tech-firms-in-novel-supply-chain-attack/>



контейнеров, фактически новый *NIX, являясь интеллектуальным менеджером приложений, ресурсов и процессов в *NIX в реальном времени. Соответственно нечеловеческой сложности этой системы (на два порядка выше *NIX) количество проблемных ситуаций тяжело поддаётся счёту, фактически дублируя все ранее возможные ситуации (отсутствие толкового логирования, дефолтная анонимная аутентификация и др.) и возвращая нас во времена Windows 95.

Системы управления конфигурацией (puppet, helm) — обеспечивают динамическое развёртывание легаси и контейнеризированных инфраструктур и приложений. Основная проблемная ситуация — интеграции с разнообразными сервисными учётными записями, хранение секретов.

Серверная инфраструктура (билд-серверы и др.) — обеспечивают базу для работы других систем. Проблемные ситуации — большое количество уязвимостей, излишний доступ разработчиков к таким серверам.

Рабочие станции разработчиков / DevOps — место, где разработчики разрабатывают и иногда билдят. Проблемные ситуации — билдинг на рабочей станции, хранение кода на рабочей станции, неконтролируемый BYOD, незашифрованные жёсткие диски для мобильных устройств, секреты в открытом доступе, отсутствие ротации секретов.

К сожалению, традиционные практики оценки рисков плохо применимы для CI/CD-инфраструктуры. Это обусловлено большим количеством взаимозависимостей и сервисных учётных записей. Таким образом, качественно изолировать влияние от, например,

компрометации registry от влияния на весь CI/CD-пайплайн (автоматизированный процесс развёртывания ПО) невозможно.

PREVENT

Узнав, какие типы объектов защиты у нас есть, мы получаем возможность последовательного внедрения классических корпоративных доменов требований безопасности:

1. аутентификация;
2. авторизация;
3. управление уязвимостями и техническим комплаенсом;
4. криптография и управление секретами;
5. логирование и мониторинг;
6. DRP.

Стоит отметить: чем ближе приложение к модели SaaS, тем меньше в нём механизмов ИБ. Однако даже базовые механизмы нужно контролировать и проверять их работу.

Учитывая, сколько команд разработчиков и разрабатываемых приложений можно найти в корпорациях, работа по внедрению контролей безопасности займёт годы. Также стоит отметить, что работа по обеспечению безопасности CI\CD во многом подобна работе по обеспечению безопасности SAP. Например, процесс обновления Kubernetes кластера требует разработки и далеко не всегда возвращает предсказуемые результаты.

Для эффективной реализации программы по безопасности CI\CD предлагается применять следующие 5 принципов:

Security as a Code (безопасность как код) — по максимуму хранить проверки и конфигурацию инструментов безопасности в репозиториях

и автоматически их применять. Заодно это поможет держать в поле зрения работу молодых падаванов.

Постепенное внедрение — совместно с бизнесом и ИТ выберите один проект и внедрите стандарты безопасности для него. Потом можно будет тиражировать.

Трезвая оценка ситуации — комбинируйте Open Source и коммерческие инструменты. Первые будут тянуть ваше время, а вторые — деньги, очень удобно иметь возможность балансировать.

Человеческий язык — после понимания ландшафта CI/CD нужно коммуницировать с продуктовыми командами, часто они сами внедряют много улучшений безопасности.

Ответственный подход — в случае инцидентов ИБ служба ИБ так или иначе будет за них отвечать. Это значит, что нужно или внедрять контрольные ворота (приёмку), или регулярно делать аудиты DevSecOps и чётко представлять, что происходит в разработке. Это, в свою очередь, позволит профессионально управлять рисками: принимать (хоть и временно) или снижать их в зависимости от критичности приложения, чувствительности данных, в нём обрабатываемых, наличия людских, финансовых и других ресурсов для реализации контролей по снижению рисков.

Отдельно отмечу, что в данной статье не упомянуты все риски, связанные с Kubernetes, — это большая и сложная тема. Введением в неё будет классический CIS Benchmark, а также некоторое количество лабораторных работ, которое нужно будет сделать, чтобы почувствовать, что такое Kubernetes, на своей шкуре (hands-on), например, O'Reilly Katakoda.

DETECT

Однако в ситуациях, где невозможно реализовать ограничения на уровне предотвращения (Prevent), мы можем внедрить детектирующие контроли. Например, если программное обеспечение написано так, что конкретным Docker-контейнерам нужны значительные права, мы можем детектировать опасные системные обращения в Kubernetes-кластере, например:

- ◆ повышение привилегий;
- ◆ запуск docker-клиента внутри контейнера;
- ◆ чтение чувствительной информации (/etc/sudoers.d, /etc/pam.d и другие);
- ◆ изменение конфигурационного файла shell;
- ◆ подключение к C2-серверам.

Стоит понимать, настройка детектирующего контроля — это часть дела, нужны ещё люди, которые будут триажить (сортировать) и расследовать алерты. Учитывая кадровый голод в

службах ИБ и SOC, DevSecOps подразделения будут полагаться на себя и максимальную автоматизацию деятельности по мониторингу и DevSecOps в целом.

RESPOND

Автоматизация реагирования в CI/CD весьма новая область, и далеко не всё сейчас можно автоматизировать с приемлемым уровнем false positive / false negative. Первым делом на ум приходят решения SOAR, но им хватает работы и в традиционных ИТ-инфраструктурах.

На самом деле на уровне инфраструктуры разработки на помощь приходят admission controllers, например, Open Policy Agent, которые выполняют роль NAC для Kubernetes на стекоидах. На уровне кода — Application Security Orchestration and Correlation решения — SIEM для проблем в коде с учётом инфраструктур разработки различных команд. Например, Archery / Defect Dojo.

RECOVER

Резервное копирование нужно производить особенно тщательно там, где у нас нехватка предотвращающих и детектирующих контролей, таким образом, хотя бы снижая риск значительной приостановки цифровых бизнес-процессов.

Recovery Time Objective (RTO) CI/CD равняется наибольшему RTO из компонентов CI/CD ландшафта, за исключением вспомогательных систем по управлению задачами и знаниями.

Recovery Point Objective не так критичен, как в классических информационных системах, потому что данные обычно хранятся вне CI/CD. С точки зрения сохранения состояния среды оркестрации подход GitOps позволяет практически восстанавливать её, однако внедрение GitOps само по себе — отдельная масштабная задача, и не для всех она полезна.

Это также значит, что тестирование бекапов критично как никогда — снова можно провести параллель с SAP security.

* * *

Джинна цифровизации и инхаус разработки уже не загнать назад в бутылку, поэтому пора открыть глаза на реальность. Лучше начать создавать функцию DevSecOps до того, как разработчики и инженеры DevOps, непрерывно создавая и развивая новые защищённые приложения и инфраструктуры, доведут вашу службу ИБ до неприятной ситуации. Тем более что тема DevSecOps большая, чем привлекает много молодых и энергичных специалистов.



Алексей ЮДИН
директор центра
мониторинга
Infosecurity



Андрей КОНЯХИН
начальник отдела
информационной
безопасности
ПАО «Норвик Банк»

ОТ НЕПОНИМАНИЯ ДО ЗАКЛЮЧЕНИЯ КОНТРАКТА

ОПЫТ ПОДКЛЮЧЕНИЯ «НОРВИК БАНКА» К ОБЛАЧНОМУ ЦЕНТРУ МОНИТОРИНГА СОБЫТИЙ ИБ ISOC

В этом году «Норвик Банк» подключился к облачному центру мониторинга событий информационной безопасности ISOC компании Infosecurity (ГК Softline). Потребность во внедрении автоматизированного решения была связана с необходимостью реализации защиты данных в соответствии со стандартами ГОСТ Р 57580 и PCI DSS и рядом других причин. На вопросы BIS Journal отвечают Андрей Коняхин, начальник отдела информационной безопасности ПАО «Норвик Банк», и Алексей Юдин, директор центра мониторинга Infosecurity.

— С чем были связаны предпосылки внедрения SOC в инфраструктуру «Норвик Банка»?

Андрей Коняхин, «Норвик Банк»: Помимо повышения уровня кибербезопасности ИТ-инфраструктуры, нам необходимо было выполнить требования к обеспечению защиты информации при осуществлении банковской деятельности — ГОСТ Р 57580. Если коротко, то этот стандарт помогает делать денежные операции в банке или другой финансовой организации безопасными. Звучит просто, но на деле все гораздо сложнее: в стандарте содержится

более 400 требований, и всем им необходимо соответствовать.

— Изначально банк не планировал подключаться к облачному SOC из-за желания построить собственный и риска отдавать контроль над инцидентами сторонней компании. Что изменилось?

Андрей Коняхин, «Норвик Банк»: Изменилось наше отношение к облакам. Коллеги обосновали сильные стороны облачного решения в сравнении с построением собственного центра мониторинга. Изначально мы планировали построить собственный SOC с нуля, но быстро пришли к выводу, что с нашими ресурсами, в том числе кадровыми, это будет невозможно сделать в существующих жёстких временных рамках. Подключение к ISOC для нас стало оптимальным по срокам и финансово выгодным решением.

Алексей Юдин, Infosecurity: Мы действительно прошли большой путь от непонимания до заключения контракта. Нашими аргументами в вопросах безопасности стали опыт построения собственного центра мониторинга и наша команда специалистов с более чем десятилетним стажем управления

О ПРОЕКТЕ

Заказчик: ПАО «Норвик банк»

Продукт: Облачный ISOC

Исполнители: Infosecurity (ГК Softline)

Срок реализации: ноябрь 2020 — март 2021

Решённые задачи:

1. Выполнение требований ГОСТ Р 57580
2. Повышение кибербезопасности ИТ-инфраструктуры банка
3. Внедрение дополнительных контролей и организация реагирования при инцидентах нарушения правил безопасности критичных узлов ИТ-инфраструктуры банка

инцидентами, причём в различных отраслях. Немаловажной составляющей стала политика кадровой безопасности Infosecurity и активное взаимодействие с ФинЦЕРТ, Центром отслеживания и реагирования на кибератаки в кредитно-финансовой сфере. Это означает, что мы постоянно «держим руку на пульсе» и можем ещё оперативнее реагировать на компьютерные инциденты.

— Какие ещё особенности руководство банка учитывало при принятии решения в пользу облачного SOC от Infosecurity?

Андрей Коняхин, «Норвик Банк»: Мы приняли во внимание уникальный опыт построения собственного SOC компании Infosecurity. В недалёком прошлом, будучи частью корпорации, входящей в топ-50 российских банков, команде удалось организовать мониторинг и реагирование на инциденты информационной безопасности для инфраструктуры в 35 тысяч узлов, а это солидный показатель. Плюс ко всему коммерческое предложение партнёра оказалось оптимальным по стоимости. Благодаря нашему сотрудничеству мы сможем сохранять от 3 до 5 млн рублей в год, которые расходовались бы при гибридной схеме, когда оборудование разворачивается в инфраструктуре банка, а управление осуществляется сервис-провайдером. Плюс к этой сумме ещё добавились бы затраты на расширение собственной команды службы безопасности и покупку лицензий на SIEM.

Алексей Юдин, Infosecurity: В случае с «Норвик Банком» идея была проста: зачем платить больше, если есть проверенное и работающее решение? Благодаря сотрудничеству с банками мы понимаем все процессы банковской деятельности, знаем подводные камни и имеем большой опыт адаптации SOC под нужды кредитных организаций. Значит, мы сможем адаптировать наше предложение и к их запросам.

— Насколько быстро удалось выстроить систему работы с инцидентами и был ли пилот?

Андрей Коняхин, «Норвик Банк»: Время на реализацию проекта было ограничено. Команда банка была параллельно загружена реализацией сразу нескольких проектов, но мы смогли совместно выработать комфортный для обеих сторон график и темп работы, и всё получилось.

Алексей Юдин, Infosecurity: Сроки были максимально сжатыми. Проведение пилота могло добавить ко времени реализации проекта от нескольких месяцев до полугода, поэтому

Благодаря нашему сотрудничеству мы сможем сохранять от 3 до 5 млн рублей в год, которые расходовались бы при гибридной схеме, когда оборудование разворачивается в инфраструктуре банка, а управление осуществляется сервис-провайдером

от него решили отказаться. На результате это никак не отразилось — у нас были все инструменты и опытная команда по внедрению ISOC.

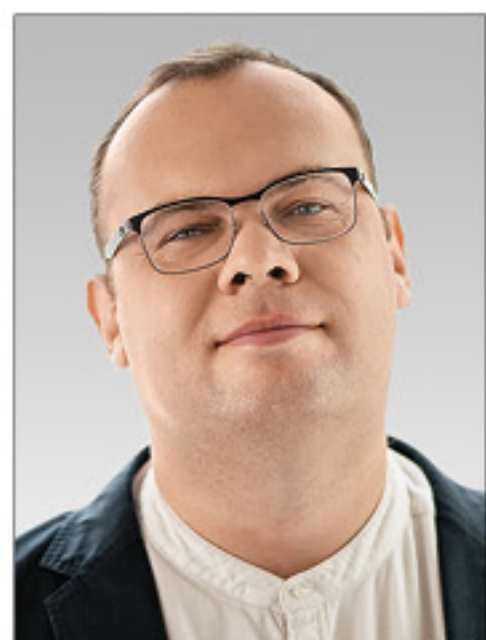
— С какими трудностями столкнулись при подключении банка к ISOC?

Андрей Коняхин, «Норвик Банк»: Так совпало, что как раз в этот период у нас полностью сменилась команда службы информационной безопасности. Мы опасались, что ситуация может негативно сказаться на процессе подключения к облачному сервису: пришлось бы тратить много времени на введение в курс дела новых специалистов, их адаптацию и обучение. К счастью, опасения оказались лишними. Аутсорсинг ISOC дал нам важное преимущество — вместе с сервисом мы получили опыт специалистов Infosecurity с уникальной экспертизой.

Алексей Юдин, Infosecurity: Всё верно, смена команды в середине проекта не повлияла на процесс внедрения ISOC. Это говорит о том, что система стабильно работает независимо от кадровых изменений в организации. Наши специалисты первой и второй линии, отвечающие за мониторинг инцидентов и оповещение, всегда «на подхвате» и выполняют свои обязанности в режиме 24/7/365.

— Что отличает кейс подключения «Норвик Банка» к ISOC от других уже осуществлённых проектов?

Алексей Юдин, Infosecurity: В качестве дополнительного бонуса мы предложили прописать «Норвик Банку» организационно-распорядительную документацию по разграничению и выстраиванию процесса взаимодействия команды SOC и банковской группы реагирования на инциденты ИБ. Это помогло руководству банка оптимизировать собственные временные и финансовые затраты на разработку соответствующих документов. Также мы кастомизировали и реализовали ряд нетиповых источников в рамках сервиса.



Иван МЕЛЕХИН
директор IZ:SOC
компании
«Информзащита»

ПРОЗРЕТЬ!

ТОЛЬКО ТАК СМОГУТ ВЫЖИТЬ СЛЕПЫЕ СРЕДИ КИБЕРРИСКОВ

Можно сказать, что SOC — Security Operations Center — это своеобразный орган зрения, позволяющий видеть в киберпространстве. И даже намного больше. В настоящее время на российском рынке под SOCами в 85% случаев подразумевается именно мониторинг. Согласно нашему опросу, услугами SOСов пользуется 27% аудитории, а около 70% — только задумываются об этом или не видят в них необходимости.

УДИВИТЕЛЬНАЯ КАРТИНА

Наша компания проводит тесты на проникновение. Главная цель заказчиков — проверить, как работают внедрённые средства и сервисы ИБ. Статистика за последние 5 лет следующая.

Пентесты востребованы во всех отраслях, особенно в финансовом секторе (рис. 1). Последнее связано с требованиями регуляторов, отраслевыми стандартами и повышенным интересом хакеров к деньгам.

Свыше 50% заказчиков имеют более одного офиса, а в большинстве компаний — до 1 тыс. сотрудников (рис. 2).

Обращаются за разными пентестами (рис. 3). Большинство заказывает внешние и внутренние. Это способ увидеть картину уязвимости в целом: как при попытках доступа извне, так и при доступе из внутренней сети.

79% компаний имеют уязвимости. Эксплуатация найденных уязвимостей в 86% случаев позволяет провести атаку и добраться до чувствительных данных. То есть около 70% (86% от 79%) компаний были успешно взломаны. Причём большинство — за несколько простых шагов.

По итогам двух разных опросов получается удивительная картина: 70% не осуществляют мониторинг и 70% могут быть успешно взломаны. Картина, где всемогущий хакер подобен зрячему, попавшему в мир слепых!

Действительно, кибератаки давно превратились в мощную масштабную индустрию, где на одном краю — спонсируемые государствами группировки, а на другом — профессиональные команды вымогателей. Под их удар может попасть любая организация: и стартап, и промышленный гигант, и госструктура.

ПРЕСТУПНИК ОСТАВЛЯЕТ СЛЕД

Цепочки атак, которые мы восстанавливали в процессе расследований нашего Центра мониторинга, отличаются сложностью и многоэтапностью. В большинстве случаев используются как автоматизированные средства, так и ручное управление, ведётся подготовка целевой вредоносной нагрузки, не выявляемой традиционными средствами защиты типа антивирусов или межсетевых экранов.

Но не нужно забывать, что любая активность в инфраструктуре, как бы хорошо ни был подготовлен нарушитель, оставляет следы. Нужно просто уметь их замечать и распознавать. В этом случае злонамеренные активности могут быть пресечены на самых ранних стадиях.

ЧТО НУЖНО, ЧТОБЫ ВИДЕТЬ?

Что нужно, чтобы начать видеть следы активностей?

Вопреки распространённому мнению, подогреваемому маркетингом вендоров, недоста-



Рисунок 1. Потребность рынка в тестах на проникновение. Отраслевой разрез

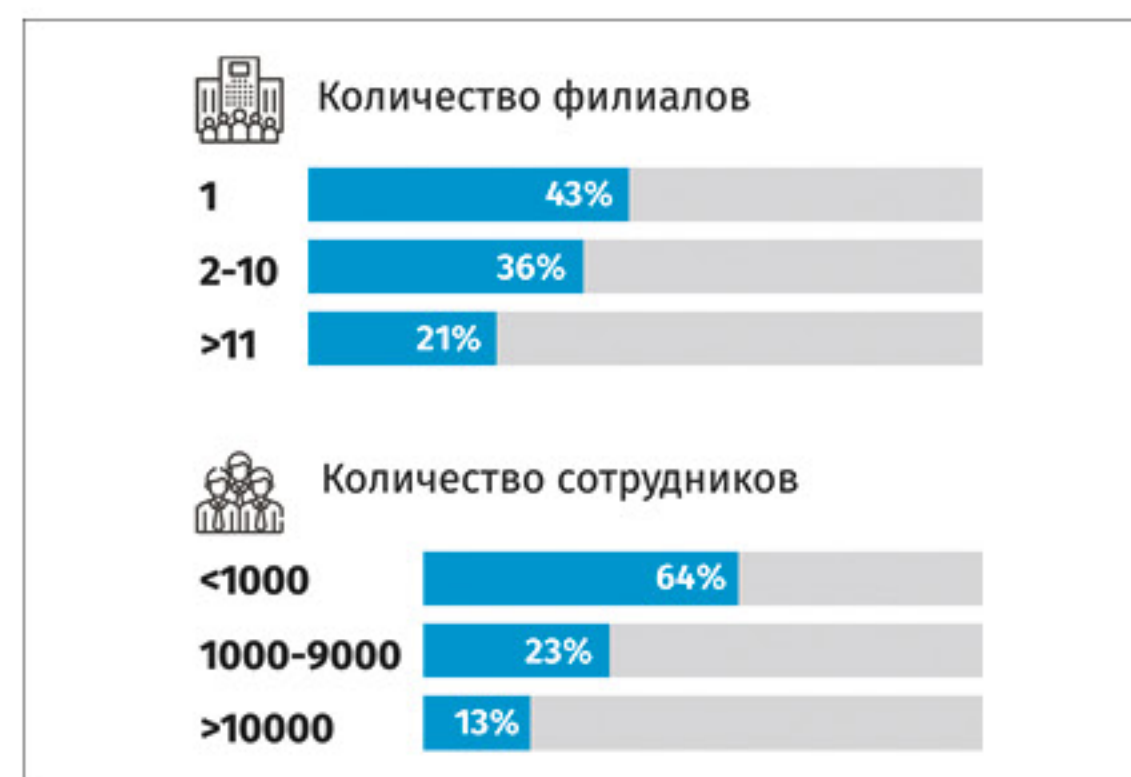


Рисунок 2. Распределение компаний-заказчиков по количеству филиалов и сотрудников

точно купить один продукт (SIEM, IRP, SOAR, XDR и т.п.). Мониторинг киберинцидентов базируется на четырёх «китах»: инфраструктура, контент, процессы и люди.

Инфраструктура. Мониторинг киберинцидентов — это в первую очередь история про данные. Объём событий, поступающих от источников в инфраструктуре, может достигать десятков и сотен тысяч событий в секунду. Этот поток нужно на лету обрабатывать, хранить, осуществлять поиск. Требования к доступности так же высоки, как и требования к масштабируемости. SIEM является одной из частей конвейера обработки данных, который в крупных SOCaх состоит из множества компонентов. Но конвейер обработки данных — далеко не всё. Нужны системы сервис-деск и мониторинга, средства взаимодействия с внешними системами и допсервисы. Нельзя забывать и об аппаратной части, системах хранения, средах виртуализации... В целом инфраструктура современного SOCa очень сильно отличается от одной большой SIEM.

Контент. Получив данные, необходимо понимать, что в них искать. В актуальной матрице MITRE ATT&CK для предприятий описано только 245 техник атак верхнего уровня. Для детектирования каждой техники нужны правила. База правил, позволяющая выявлять актуальные угрозы, составляет от 400 правил в SIEM, отлаженных и оптимизированных к ложным срабатываниям. И это, не говоря о процессе TI, поиске индикаторов компрометации и threat hunting. Безусловно, вендоры предлагают вместе со своими продуктами наборы правил, но, по общему мнению экспертов, эти правила невозможно использовать без адаптации и оптимизации к инфраструктуре. То же самое и с моделями машинного обучения, если таковые используются. Контент любого коммерческого SOCa составляет основу его успеха.

Процессы. При выявлении подозрительной активности встаёт вопрос: что делать? Как проводить анализ на ложное срабатывание? Как взаимодействовать с ИТ и бизнесом, предотвращать распространение, зачищать инфраструктуру, расследовать? Всё это нужно делать, и не только это. От распределения смен при круглосуточной работе до взаимодействия с внешними организациями при реагировании на инциденты — всё это процессы в рамках SOCa, и все они должны быть понятными и отрепетированными.

Люди. Дефицит кадров на рынке ИБ по разным данным варьируется от 300 тыс. до миллиона человек. За любым более-менее знающим специалистом охотятся сразу несколько компаний. Ситуация усугубляется серьёзным несоответствием знаний, полученных в вузе, требованиям рынка. Плюс новое поколение (Z) сотрудников имеет



Рисунок 3. Статистика пожеланий заказчиков

особенности, например, среднее время их работы на одном месте не превышает 2–2,5 лет вне зависимости от условий и компенсаций. Удержать такое молодое дарование крайне сложно. Кроме того, новые сотрудники, как правило, не готовы быстро освоить свои функции в Центрах мониторинга. Для решения этой проблемы, мы, например, активно распространяем наши внутренние требования к грейдам аналитиков, которые можно получить, обратившись к автору статьи.

ВАРИАЦИИ НА ТЕМУ

Безусловно, всё вышеперечисленное (квартет «инфраструктура-контент-процессы-люди») можно развивать самостоятельно или пользоваться как сервисом в разных сочетаниях. Но при выборе формы взаимодействия нужно помнить:

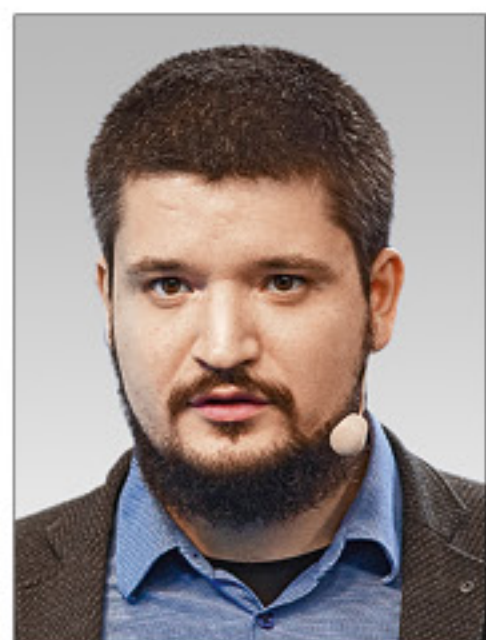
- ◆ Если весь квартет на стороне поставщика услуг, то скорость подключения сервиса будет максимальной, а цена — оптимальной. Квалификация людей также будет на высоком уровне.

- ◆ Можно оставить инфраструктуру у себя, но её сложно отделить от контента. Если провайдер придёт со своим контентом в ваш SIEM, он сохранит над ним контроль и после разрыва контракта. То есть, имея свою инфраструктуру, нужно быть готовым к заказной разработке контента или к его покупке у провайдера.

- ◆ Инфраструктуру можно поделить на уровни, например, предоставив провайдеру вычислительные мощности и системы хранения, а всё, что выше, — получить от него. В этом случае не будет сложности с контентом.

- ◆ Самый простой и дешёвый случай — это типовые процессы провайдера, отработанные на массе клиентов. Но если ваш случай специфичный, сервис будет существенно дороже.

- ◆ Если вы хотите, чтобы на вашей инфраструктуре работали сотрудники провайдера, то ищите не поставщика услуг SOCa, а поставщика персонала, т.к. провайдеру придётся заниматься не ИБ, а аутстафом.



**Тимур
ЗИННЯТУЛЛИН**
директор Центра
киберустойчивости
группы компаний
Angara

SOC ПРОТИВ PENTEST

ON-PREMISE ИЛИ OUTSOURCE?

В идеальной картине мира состав потенциальных возможностей сегодняшних Security Operations (SecOps) должен в достаточной мере обеспечивать как все потребности бизнеса в виде услуг и сервисов, которые оказываются соответствующим подразделением, например SOC, так и принципы эшелонированной обороны для постоянно изменяющихся контролируемых объектов и информационной инфраструктуры в целом. Для включения в арсенал SOC доступно множество детектирующих и превентивных мер и средств защиты, статических и динамических. Постоянно растёт и уже трудно поддаётся синтаксическому анализу количество фидов и их форматов. Происходит расширение границ и глубины мониторинга (X-C3I, Next Generation C3I и т.д.), и применяются методы машинного обучения (ML), правда, я не берусь утверждать, поскольку сам на практике не встречал его полноценную реализацию.

Все эти факторы должны положительно влиять на возможности предотвращения и устранения инцидентов ИБ. И всё-таки, к сожалению, мы продолжаем читать истории о том, как ещё одна компания оказалась не готова к противодействию злоумышленникам.

На этом фоне потребность в квалифицированном выстраивании и повышении надёжности защиты вверенной информационной инфраструктуры постоянно растёт. Вернее, становится всё более актуальной, поскольку изначальный уровень запущенности данных процессов и

отсутствия security by design, по сути, значительно не меняется уже десятилетиями.

На решение компании о необходимости создания SOC, помимо всего прочего, часто влияют объективные экономические факторы: как общая структура расходов с преобладающим CAPEX или OPEX, так и стоимость владения соответствующим ФОТ с учётом необходимости его обучения и развития, обеспечения обслуживанием, удержания и т.д. В зависимости от зрелости внутренних процессов ИБ и ИТ, в лучшем случае на основании спрогнозированной стоимости защищаемых активов и модели угроз, оценивается допустимая стоимость контрмер, как и их состав и целевое назначение. Затем принимается решение о том, какие функции реализуются самостоятельно, а какие будут отданы внешнему партнёру. В итоге, как правило, для удовлетворения потребностей бизнеса классическое разделение — собственный SOC или внешний — оказывается размытым. А с учётом растущей вариативности и сложности архитектур информационных систем и степени их проникновения в повседневную жизнь общества функции SecOps разделяются между партнёрами в уникальной для каждой компании пропорции, как разделяются и архитектурные, и операционные схемы их взаимодействия. Теперь для формирования, внедрения и развития SecOps компаниям нужен надёжный партнёр с накопленным опытом не только в части реализации SecOps в любом форм-факторе, но и в части обоснования своих предложений перед бизнесом.

Говоря об анализе защищаемых активов и формировании ALE (Annual Loss Expectancy) с последующей оценкой cost/benefit анализа контрмер, следует упомянуть процесс оценки рисков в целом и его текущую роль в моделировании угроз. Часто звучат тезисы о том, что данный процесс неосуществим в реалиях большинства российских компаний. На практике же подобные примеры есть, и их становится всё больше. Без циклического проведения оценки рисков с той или иной степенью детализации и результативности приступать к реализации

Для формирования, внедрения и развития SecOps компаниям нужен надёжный партнёр с накопленным опытом не только в части реализации SecOps в любом форм-факторе, но и в части обоснования своих предложений перед бизнесом

SOC нецелесообразно. Помимо того, что это требуют основные отраслевые регуляторы и стандарты, важно помнить, что, только основываясь на постоянном и цикличном процессе оценки и анализа рисков, можно получать и обновлять знания о контролируемой инфраструктуре, актуальных угрозах и, что немаловажно, о допустимой стоимости применяемых контрмер. Это информация, которую недооценить крайне сложно, особенно при выборе соответствующих сервисов и продуктов. Для дополнения классических методик оценки рисков инженеры и аналитики Центра киберустойчивости группы компаний Angara предлагают свои уникальные наработки по автоматизированной атрибуции потенциальных угроз и TTP (Tactics, Techniques and Procedures), основанной на публичных данных, полученных в ходе расследований реальных, подтверждённых инцидентов ИБ. В том числе возможность приведения итоговых результатов к соответствию новой методике оценки угроз БДУ ФСТЭК и маппинга к ресурсам MITRE ATT&CK® и MITRE SHIELD®.

Результаты, во-первых, будут гарантированно повторяемыми благодаря автоматизации, а значит, применимыми в рамках цикла PDCA, что позволит создавать и сравнивать карты покрытия техник в разных промежутках времени. Во-вторых, помогут в процессе оценки и выбора различных сервисов и продуктов.

Баланс между внутренними и внешними SecOps движется к размытому или разнородному равновесию: сторонняя экспертиза может быть привлечена к работе как с уже внедрёнными, собственными СЗИ, процессами и сервисами, включая SOC, так и со своим инструментарием SecOps ввиду отсутствия у компании необходимых ресурсов. Возможны варианты привлечения лишь технологий SecOps, например, в формате SaaS, с дополнительным консалтингом. Экспертиза будет востребована в различных гибридных форматах: для полного или частичного замещения и дополнения любых функциональных и технологических потребностей SecOps и бизнеса конкретной организации, меняющихся в зависимости от её ресурсов или пересмотра стратегии. Следуя требованиям времени, группа компаний Angara создала Центр киберустойчивости для консолидации опыта и экспертизы двух ранее обособленных направлений: подразделения, занимавшегося развитием и внедрением решений по направлению SecOps on-premise, и подразделения, предоставлявшего услуги коммерческого SOC в качестве сервиса. Объединение позволило приступить к формированию той самой гибридной модели оказания услуг исходя из текущих и будущих потребностей бизнеса.

На сегодняшний день Центр киберустойчивости включает широкий перечень направлений. У нас даже есть опыт выполнения функций по реагированию на подозрения на инциденты ИБ, которые направляет сторонний SOC.

При таком количестве решений и угроз различных классов и высоких требований к экспертизе, с целью постоянного закрепления имеющихся навыков и развития новых группа компаний Angara проводит регулярные спринты с участием SOC и подразделения анализа защищённости (pentest). При подготовке к ним руководители «красной» и «синей» команд совместно определяют перечень векторов атаки, которые либо давно не прорабатывались, либо ещё никогда не использовались (новые уязвимости, модели нарушителей и т.д.).

Каждый спринт улучшает общий уровень зрелости и защиты, и нападения, а накопленный практический опыт преобразуется в новые правила SOC и новые инструменты pentest. Все наработанные инструменты защиты и нападения впоследствии переходят в промышленную эксплуатацию при оказании услуг коммерческого SOC и анализа защищённости. Одновременно с этим, поскольку спринты проводятся на инфраструктуре группы компаний Angara, повышается уровень защищённости собственных объектов инфраструктуры, которому уделяется значительное внимание. В дополнение к спринтам регулярно проводятся учения с использованием методов социальной инженерии, сканирования периметра и других.

Для организации подобных спринтов или учений используются адаптированные под собственные процессы и ресурсы выдержки из общемировых методологий, например, таких как Singapore — AASE, EU — TIBER-EU, NATO — CRT и других.

* * *

С учётом скорости развития информационной безопасности в целом и необходимости постоянно быть готовыми ответить на любые современные вызовы группа компаний Angara моделирует и подготавливает решения и услуги с целью удовлетворения любых потребностей бизнеса. Известное выражение гласит: «Нужно бежать со всех ног, чтобы только оставаться на месте, а чтобы куда-то попасть, надо бежать как минимум вдвое быстрее!». И этого «вдвое» можно достичь путём объединения усилий организации и надёжного партнёра в области информационной безопасности, каким является группа компаний Angara для своих заказчиков.

РАЗВИВАЕТЕ SOC? МЫ ЗНАЕМ, КАК ВАМ ПОМОЧЬ

**Борис ОСЕПОВ**

технический эксперт
по построению
систем комплексной
защиты от кибератак,
«Лаборатория
Касперского»

Чтобы оценить, насколько всё изменилось в сфере SOC, достаточно ответить на встречный вопрос: а насколько поменялся мир в целом и образ жизни в последние годы? Ваш ответ можно смело умножить на десять, так как процессы, структура, технологии, метрики и многое другое в информационной сфере (особенно в безопасности) меняются настолько быстро, что вы, читая эту статью, уже немного не успеваете за трендами. Но это не есть плохо, главное — стремление понять, что у вас происходит в центре мониторинга ИБ, ведь нельзя улучшить то, что нельзя измерить.

SOC состоит из ряда столпов, таких как люди, бизнес, процессы, технологии и сервисы. Каждый из них напоминает цепочку действий с обратной связью, задача которой — постоянное улучшение того или иного направления. Вспомним модель Шухарта — Деминга (PDCA): Plan-Do-Check-Act. Работа в SOC — это постоянная работа над ошибками.

Для того чтобы люди успешно работали, им необходимы хорошие инструменты. Что нужно использовать из технологий в центре мониторинга ИБ? Прежде всего, существуют основополагающие классы решений, такие как SIEM-системы, IRP, IAM-системы и Threat Intelligence, и базовые технологии: средства антивирусной защиты, сканеры уязвимостей, межсетевые экраны, средства обнаружения вторжений, средства динамического анализа и т. д. Каждый вектор атаки должен покрываться несколькими слоями защиты для соответствия принципу эшелонированной ИБ. Не нужно обходить стороной и новые системы защиты, например EDR, XDR, SOAR.

Решений на рынке много, и полезно иметь в своём арсенале комплексные системы и платформы, которые смогут покрыть несколько классов систем. Примерами могут быть такие продукты, как Kaspersky Unified Monitoring and Analysis Platform (KUMA) или платформа Kaspersky Anti Targeted Attack (КАТА). Первое решение сочетает в себе функциональность SIEM-системы, которая может работать под высокой нагрузкой, тикет-систему, которая потоково обогащается данными Threat Intelligence через платформу CyberTrace, а также имеет возможность автоматически запускать задачи на Kaspersky Security для бизнеса при помощи интеграции с Kaspersky Security Center. К слову, данная SIEM-система хорошо зарекомендовала себя не только на проектах у клиентов,

но и при собственном использовании в SOC «Лаборатории Касперского».

Платформа Kaspersky Anti Targeted Attack сочетает в себе функциональность анализа сетевого трафика и продвинутого динамического анализа файлов и ссылок в веб-трафике, почте и др. Также платформа интегрирована с Kaspersky Endpoint Detection and Response — решением для выявления продвинутых угроз и реагирования на них на уровне конечных станций и серверов. Вместе с Kaspersky EDR платформа Kaspersky Anti Targeted Attack составляет современное решение класса XDR (Extended Detection and Response), которое предназначено для комплексной передовой защиты от сложных угроз и целевых атак, в том числе класса АPT.

Использование лучших практик, наличие развитой инфраструктуры систем ИТ и ИБ, а также обученные специалисты в штате Security Operations Center — далеко не верх зрелости центра компетенции, необходимо постоянно держать команду в тонусе — обучать новым навыкам и обмениваться опытом с другими продвинутыми центрами мониторинга ИБ. Делать всё вышеперечисленное своими силами не так просто, поэтому аутсорс услуг SOC набирает популярность. К примеру, «Лаборатория Касперского» предлагает сервис управляемой безопасности Kaspersky Managed Detection and Response, который включает основные преимущества собственного SOC без затрат на его создание — в частности, круглосуточный мониторинг происходящего в системе безопасности и реагирование в случае возникновения инцидента. Кроме того, у «Лаборатории Касперского» есть специализированные сервисы Kaspersky SOC Framework Development и Kaspersky SOC Maturity Assessment. Первый поможет на всех этапах построения центра мониторинга ИБ, а второй будет полезен для тех, у кого уже есть сложившиеся практики операционной безопасности, — он поможет оценить их зрелость и наметить дорожную карту дальнейшего развития.

Чтобы оценить собственный уровень зрелости SOC и понять свои сильные и слабые стороны, можно самостоятельно применять SOC-CMM (Capability Maturity Model). Используйте новые подходы для улучшения работы процессов и условий труда специалистов и не бойтесь совершать ошибки, ведь ошибок не делает тот, кто ничего не делает. А чтобы их было меньше, обращайтесь к нам — «Лаборатория Касперского» всегда к вашим услугам!



**Будьте в центре
событий ИБ**

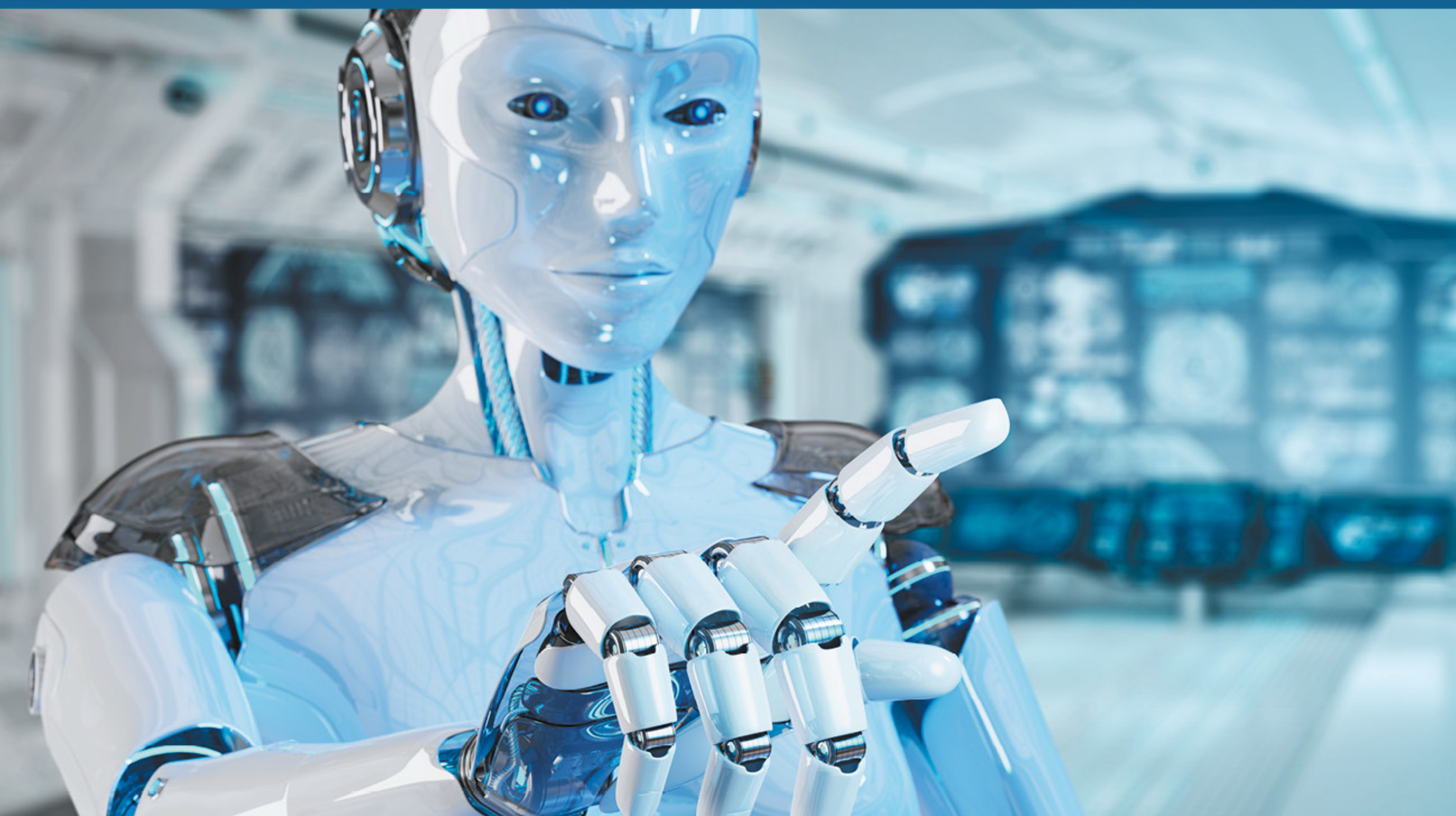


Kaspersky
Unified Monitoring
and Analysis Platform

kaspersky



18+



БЕРИТЕ КРЫЛЫШКО!

SOC ПОД ПРЕДВОДИТЕЛЬСТВОМ ИИ



Антон ФИШМАН
технический
директор компании
RuSIEM

Небольшой дисклеймер: это не научная статья, и тем, у кого уже есть SOC, многое из сказанного покажется очевидным. Для тех, кто только задумывается, а целиться ли в ту сторону вообще, сначала поговорим о том, зачем в принципе нужен SOC и уже потом — что из его функций есть смысл брать сразу с added value в лице технологий искусственного интеллекта.

Далеко не всем нужна ИБ как стратегическая функция, далеко не у всех есть риски, которые нужно парировать с помощью сложносочинённого набора дорогих и непростых в использовании инструментов. Кому-то достаточно антивируса и межсетевого экрана, кто-то только-только подошёл к установке SIEM. Это всё хорошо и правильно. Хотя — не хочется пугать, но тем, кто в ИБ давно, уже очевидно: ИБ-угрозы, актуальные раньше только для крупных организаций, всё чаще рикошетом бьют по братьям их меньшим. Атаки на цепочки поставщиков ПО (например, когда вредоносный код внедряется в программное обеспечение в

процессе его разработки или обновления), фишинг, шифровальщики — со всеми ними всё чаще сталкиваются компании среднего и даже малого бизнеса.

Шифровальщики — это вообще бич последних лет: волна возникла в США, затем перекинулась в Старый Свет и затем дошла до России. Информации об этих атаках сравнительно немного, но все мы понимаем почему: словить шифровальщик — это, простите, как подхватить неприличную болезнь. Занимаемся до упора втихаря самолечением, и только когда ситуация начинает печально напоминать народный фольклор, идём сдаваться врачам. И то страшно: а вдруг узнают.

Собственно, это и ответ на вопрос, зачем нужен SOC. Если для вас репутация — актив, если нарушение непрерывности процессов — это ЧП, которое не должно происходить ни при каких условиях, если вы развиваетесь и растёте и если вам нужен свой домашний доктор, который в случае чего справится самостоятельно, стадия «принятие» (рис. 1) наступит неизбежно.

И здесь большой вопрос — когда вы будете искать этого доктора? Как и с любым персоналом, здесь два варианта: когда уже рвануло (хватаем первого вроде подходящего втридорога) или заранее, воспитывая и выращивая его под себя за те же деньги, но растянуто по времени, планируемо и попутно нагружая его дополнительными функциями. Как мы уже сказали, SOC включает в себя процессы от мониторинга до парирования усложняющихся угроз, а также обучение, пентест, проверки соответствия и т.д. То есть ключевая характеристика инструментов, входящих в набор SOC, — способность к оперативной адаптации и обучению. Виды средств защиты информации (СЗИ), которыми он комплектуется, в каждом конкретном случае зависят от отраслевого профиля и размера организации, однако все они решают одни и те же задачи (рис. 2).

Как мы видим, набор вполне себе взрослый, и не сказать, что простая функциональность — особенно если нужно подступиться к его внедрению единомоментно, когда уже «рвануло».

Кстати, про «никогда не было, и вот опять». SOC отлично себя проявили в пандемию. Поскольку в предыдущие годы под чутким руководством регуляторов вырос уровень информационной безопасности организаций, представляющих наибольший интерес для киберпреступников (КИИ, финсектор), — в ответ повысился и уровень сложности атак. В дополнение к этому в результате перехода организаций на

Отрицание. Гнев. Торг. Депрессия. Внедрение. 5 стадий проекта

гибридный режим работы и как минимум удвоения подключённых к их ИТ-инфраструктуре пользовательских устройств, нагрузка на ИБ возросла, и лучше всех подготовленными к этому оказались наиболее технически оборудованные организации. Их SOC приобрели опыт, как практический, так и в части комплаенс, обеспечения соответствия стандартам и требованиям регуляторов. Приятный бонус.

И да — ИИ уже является неотъемлемой частью наиболее современных центров реагирования. Конечно, очень не хотелось всё так усложнять, но парировать современные киберугрозы просто невозможно без использования в их узловых системах (SIEM и SOAR) алгоритмов выявления генерации вредоносных доменов, анализа аномалий, поведенческой аналитики пользователей и защиты конечных точек от сложных угроз. Это не мы начали, честно.

ИНЬ И ЯН. РИСКИ

Принципиальный момент: ИИ можно разделить на две основные категории — «консультрующий», функция которого — агрегировать, анализировать информацию и резюмировать

Рисунок 1. Пять стадий проекта. Стадия «внедрение» наступит неизбежно

Функции SOC по версии MITRE				
Колл-центр	Мониторинг и приоритезация событий	Сбор и анализ бюллетеней безопасности	Публикация бюллетеней безопасности	Cyber Intel Creation
Подготовка бюллетеней безопасности	Trending	Анализ угроз	Анализ инцидентов	Tradecraft Analysis
Координация деятельности по реагированию	Реализация мер защиты	Реагирование на инциденты с выездом на объект	Удаленное реагирование на инциденты	Forensic Artifact Handling
Анализ вредоносного ПО и НДВ	Исследование свидетельств	Управление средствами защиты периметра	Управление инфраструктурой SOC	Sensor Tuning and Maintenance
Разработка сигнатур и правил корреляции	Разработка инструментария	Сбор и обработка данных аудита	Генерация данных аудита	Insider Threat Case Support
Расследование действий инсайдеров	Контроль топологии сетей	Выявление уязвимостей	Анализ уязвимостей	Тестирование на проникновение
Оценка технических решений	Консультирование по вопросам ИБ	Повышение осведомленности	Распространение знаний о способах проведения атак	Распространение знаний о способах противодействия атакам
Взаимодействие с СМИ				

Рисунок 2. Виды средств защиты информации (СЗИ) в каждом конкретном случае зависят от отраслевого профиля и размера организации, однако все они решают одни и те же задачи

Представьте себе полностью автоматизированный SOC с ИИ, который борется с атакующим ИИ от киберпреступников. Победит более технологичный (и не связанный законом и правилами регуляторов)

выводы, которые используются человеком для принятия решений, и принимающий их самостоятельно. Самостоятельные системы сами выявляют, анализируют и главное — реагируют на угрозы, консультирующие — поставляют аналитикам информацию для грамотного принятия решений по реагированию.

Системы, принимающие решения, в безопасности сейчас практически не используются. Во-первых, не разработан хороший механизм защиты целостности данных. Иными словами, если система самообучаемая, то есть риск того, что лица, заинтересованные в искажении объективных результатов их работы, будут намеренно их дезинформировать. Во-вторых, совершенно не урегулированы вопросы юридической и финансовой ответственности за принятые ИИ решения. В-третьих, злоумышленники используют те же технологии, что и безопасники. Они крайне редко ведут собственные фундаментальные разработки, предпочитая не изобретать нужную технологию, а украсть её или купить. Представьте себе полностью автоматизированный SOC с ИИ, который борется с атакующим ИИ от киберпреступников. Победит более технологичный (и не связанный законом и правилами регуляторов). Так что мы бы пока доверяли решениям, включающим человеческий фактор — в данном случае он будет позитивным элементом. При этом, конечно, необходимо помнить, что человеческий фактор подвержен своим ошибкам.

ЗАЧЕМ? А ЗАТЕМ!

Лучше всего ИИ справляется с анализом массивов данных и прогнозированием комплексных рисков. Отсюда делаем вывод, кому это нужно.

ИИ жизненно необходим SOCам холдинговых структур и компаний с распределённой филиальной сетью, а также экосистем. Если на головные структуры, как правило, в силу их значимости, распространяются законодательство о КИИ и требования ЦБ РФ, то в нижестоящих организациях уровень защиты информации на порядок ниже. Однако мы все помним,

что киберустойчивость этих самых нижестоящих напрямую влияет на устойчивость системы в целом: филиал или поставщик услуг может являться источником такого же риска, как крупные партнёры.

Соответственно, объём данных будет таким, что «вручную» или полуавтоматически их обрабатывать будет экономически невыгодно, и как раз здесь ИИ может найти своё применение: в системах предиктивной аналитики, поведенческой аналитики, для анализа отклонений транзакционного потока. Модели, основанные на ИИ, качественнее определяют подозрительное поведение, чем статические правила, при этом их использование повышает скорость реагирования на инциденты и снижает нагрузку на человеческих аналитиков.

Искусственный интеллект может применяться также для прогнозирования и реагирования на функциональные сбои, то есть для обеспечения бесперебойного функционирования и операционной надёжности информационных систем и производственных процессов. Исторический анализ функционирования событий и выявление закономерностей позволит с высокой вероятностью сказать, что в точке, характеризующейся соблюдением определённых условий, будет сбой. Соответственно, чем раньше система заметит отклонения, ведущие к схождению условий в одной точке, тем проще вовремя среагировать и предотвратить инцидент. Целевые интересанты этой функции — банки, медицинские организации, фармацевтические компании, атомная промышленность и любое другое производство, для которого остановка смерти подобна.

ИМПОРТОЗАМЕЩЕНИЕ

SOC — это не просто несколько систем и пара инструкций. SOC — это большая структура, обладающая широким набором настроенных решений, полноценно оркестрируемыми процессами и слаженной профессиональной командой. Это выстраивается годами. И если для выполнения требований 187-ФЗ ядро SOCа — SIEM/SOAR/TIP и другие системы придётся менять, эта замена должна будет пройти плавно, не повлияв негативно на уровень защищённости. Такой процесс будет сопряжён с выбором и внедрением новых систем, изменением процессов, переучиванием команды, что занимает далеко не 1–2 месяца. И стоит как самолёт. Поэтому — не корысти ради, но, на наш взгляд, очевидно, что если вы только подходите к созданию SOC, то лучше сразу выбирать российские решения с ИИ (если они не находятся под санкциями). Берите крылышко.

СЕРЬЁЗНЫЙ ИНСТРУМЕНТ



Дмитрий МИХЕЕВ
технический
директор
«АйТи БАСТИОН»

СКДПУ НТ — ОДНО РЕШЕНИЕ ДЛЯ НЕСКОЛЬКИХ ЗАДАЧ

Особенность работы кредитных организаций в том, что на их информационной инфраструктуре работает сразу несколько команд — как собственных, так и привлечённых. В условиях удалённого доступа безопасно подключить сотни сотрудников и понимать, что они делают на инфраструктуре, — сложная задача. И один из инструментов для решения подобного класса задач — это СКДПУ НТ.

Система контроля действия поставщиков ИТ-услуг СКДПУ НТ — это шлюз доступа по базовым протоколам удалённого доступа RDP и SSH, который дополнен несколькими модулями — модулем аналитики, модулем масштабирования и автоматизации, модулем отказоустойчивости. Поэтому продукт не только осуществляет доступ к целевым устройствам прозрачно для пользователя, но и обеспечивает для ИТ и ИБ-служб мониторинг и контроль подключений. Кроме того, СКДПУ НТ без ущерба для текущих процессов встраивается в инфраструктуру и бизнес-сценарии.

Мы постоянно развиваем продукт, дополняя его функциональностью, в которой нуждаются наши заказчики. И оказалось, что комплексное решение востребовано уже не только ИТ и ИБ-подразделениями, но и службами эксплуатации и автоматизации.

ШЛЮЗ ДОСТУПА

Периметр банков — чувствительная структура. Утечки данных клиентов происходят всё чаще и получают всё более широкую огласку. Публикации в СМИ по итогам расследований говорят: злоумышленники проникали в закрытые базы именно через

систему удалённого доступа, и чаще всего источником таких утечек становились сотрудники с «привилегиями» на чтение и обработку конфиденциальной информации.

Для предотвращения таких случаев нами реализованы механизмы уведомления о доступе и даже его организация с дополнительным подтверждением, исключающим вход в периметр без разрешения «сверху». А архитектура шлюза устроена таким образом, что подключение к целевому хосту всегда происходит с точки, являющейся безопасной, вне зависимости от того, какой компьютер используется для входа. Более того, политики системы задают права и полномочия для доступа к информации и возможностей по её копированию, в т.ч. через привычные средства «буфера обмена», будь то файл или скопированный текст.

Благодаря дополнительной функциональности, продукт не только информирует соответствующие службы кредитных организаций и накапливает доказательную базу, но и проводит анализ событий в оперативном режиме. Так мы решили две задачи сразу: снизили нагрузку на персонал, поскольку подсвечивались события, требующие особого внимания, и повысили общее понимание состояния инфраструктуры благодаря отчётам и статистикам по информационным объектам. Теперь у каждой потенциальной проблемы появляется «имя и домашний адрес».

МОНИТОРИНГ И КОНТРОЛЬ РАБОТ

Мало дать сотрудникам или аутсорсерам защищённый доступ. Важно понимать, что происходит на инфраструктуре. Это уже задача не безопасности,

а менеджмента. Банки платят подрядчикам огромные деньги, однако, когда речь заходит об ИТ-инфраструктуре, часто заказчик не может проверить, были ли сделаны работы, каково их качество и были ли потрачены на них именно те сотни человеко-часов, что указаны в акте сдачи-приёмки.

СКДПУ НТ позволяет профилировать пользователей: сотрудник ИТ-службы всегда может посмотреть, когда каждый из подрядчиков «заходил», что делал и как долго. А аномальные «всплески» активности зафиксирует и создаст на их основании инцидент для дальнейшего разбирательства.

Кроме описанных сценариев СКДПУ НТ также может «забрать на себя» большую и ресурсоёмкую задачу автоматизации согласования доступа к инфраструктуре. Рутинные процедуры выстраиваются через автоматическое взаимодействие процесса заведения новых доступов с учётными системами и системами оркестрации виртуальных окружений. Также совместно с компанией «Мультифактор» мы реализовали сценарий двухфакторной аутентификации пользователей. Это позволяет кредитным организациям выбирать конфигурацию и систему подтверждения личности администраторов сети, то есть — усилить защиту периметра.

Запросы заказчиков на дополнительный функционал продукта позволяют нам видеть тренды в развитии стратегий ИТ и ИБ в кредитных организациях. Это, в свою очередь, даёт возможность дорабатывать продукт, чтобы он был актуален и востребован. А в конечном итоге — помогал строить прозрачные и эффективные процессы в инфраструктуре заказчика.

**Василий ОКУЛЕССКИЙ**

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

ЭТИ РАЗНЫЕ ЛИЦА

Сейчас одной из самых избитых, но так и не раскрытых тем является импортозамещение. Почему-то мы как-то с недоверием говорим про **наши** продукты. Типа ну, разве наши могут делать что-то **настоящее**. Работа в информационной безопасности заставляет нас следить за продуктами разных компаний: и зарубежных, и отечественных. Оценивать эти продукты, сравнивать, размышлять над рейтингами...

Но ведь и там, и здесь продукты делают люди, такие же, как мы с вами. А что мы о них знаем, о тех, кто создаёт эти невероятные продукты — продукты информационной безопасности. Мы чаще знакомы с сейлами, продакт-менеджерами, коммерческими директорами, просто директорами. Но они нам продают продукты, а кто их создаёт?

Попытался поговорить об этом с сотрудниками самых разных компаний. Не всегда получалось — а тебе зачем? Но всё равно появились истории, которые в конечном счёте могут повлиять и на выбор решения или компании в пользу **наших**.

Например, в течение многих лет я имел опыт работы с самыми передовыми решениями в области борьбы с фродом. И не так давно очередной опыт обернулся открытием. Про компанию-открытие я попросил рассказать сотрудницу этой компании. Кто они — разработчики?

А вот друзья-основатели другой **нашей** компании постоянно заряжают меня энергией и новыми идеями. Они своим позитивом и профессионализмом вполне могут стать достойным примером начинающим разработчикам.

Итак, сегодня наши герои — компании-разработчики.

«ФАЗЗИ ЛОДЖИК ЛАБС»

«УДАЛОСЬ СПАСТИ БОЛЬШЕ 100 МЛРД РУБЛЕЙ»

ОТ ПОДРАЗДЕЛЕНИЯ ДО КОМПАНИИ

Создание антифрод-системы Smart Fraud Detection начиналось с разработки математических моделей в 2012 году, когда на базе российской компании коллектив разработки получил запрос из банка на фрод-мониторинг карточного канала обслуживания клиентов. В дальнейшем поток транзакций в этом банке сильно вырос и потребовалось уже новое технологическое решение — обработка удалённых каналов обслуживания клиентов: интернет и мобильный банкинг. После проектов

внедрения стало ясно, что для нового продукта нужна отдельная компания. Так появилась «Фаззи Лоджик Лабс».

Название выбрано неслучайно. В переводе с английского fuzzy logic — это раздел математики «Нечёткая логика». В методах обнаружения кибермошенничества компания делает акцент на алгоритмы машинного обучения и выявление сложных закономерностей.

ПЕРВЫЙ ЗАКАЗ

Первые крупные заказы приходили первоначально в отдел разработки. Один из вендоров ПО по информационной

безопасности запросил реализовать компонент функционального взаимодействия с его продуктом. Задача состояла в доработке математической модели для большого количества событий (до миллиарда) и подготовке первичных данных для максимально быстрой обработки без потери точности. Разработанная в «Фаззи Лоджик Лабс» математическая модель позволяла быстро обрабатывать и добавлять любое количество дополнительных параметров по профилированию пользователей с обновлением системы практически в режиме реального времени.

WEB CONTROL

«НАЙДИТЕ ДЕЛО ПО ДУШЕ,
И ВАМ НЕ ПРИДЁТСЯ
РАБОТАТЬ НИ ДНЯ!»



Андрей АКИНИН



Сергей ПЕТРОВ

Название любой компании вызывает у нас чёткую ассоциацию — бренд, решения, история успеха и медийное лицо. Мы к этому привыкаем и уже редко задумываемся: а кто за всем этим стоит? Кто эти конкретные люди, которые создают компанию, её историю и её успех, вкладывая свои силы и время?

В начале любого пути должны быть основатели, идейные вдохновители, заряженные идеей и мечтой и ведущие за собой других. Такими идеологами в компании Web Control являются **Андрей Акинин** и **Сергей Петров**. Два друга, оставшиеся верными студенческой дружбе и спустя 15 лет после окончания Бауманки почувствовавшие в себе силы начать собственное

дело, образовали уникальный сплав компетенций удачливого первооткрывателя-визионера и талантливого менеджера-предпринимателя. Основная идея предприятия — «не работаем с тем, что не работает». С самого начала друзья выбрали редкую тогда модель дистрибьютора с добавленной ценностью, хорошо подходившую для работы с высокотехнологичными передовыми решениями. Миссия компании — делать мир лучше, создавать новые ценности, работать с продуктами, которые интересны сегодня, будут нужны завтра и без которых не обойтись в будущем.

До этого момента Андрей успел поработать в создании и дистрибуции ПО, телекоме, компании-интеграторе, участвовал в реализации крупных

проектов и создании новых бизнесов. Накопив опыт и знания, он решил, образно говоря, сменить службу старпома на крейсере на фуражку капитана своей шхуны и отправиться в собственное плавание к новым открытиям и горизонтам. Постоянное стремление к новому и неизведанному движет им до сих пор, не давая останавливаться на достигнутом.

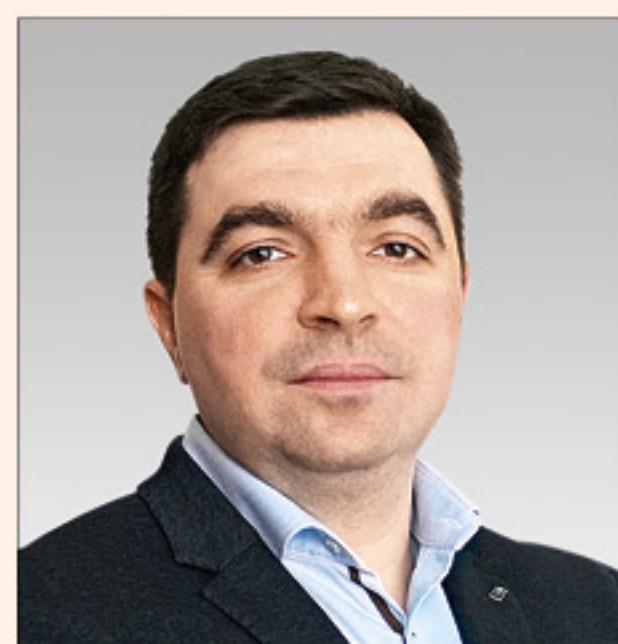
Верным соратником в этом деле стал ему Сергей Петров, который уже не один год бороздил рынок самостоятельно, был предпринимателем и знал все подводные камни в этих водах. Опыт ведения собственного бизнеса, понимание всех его тонкостей, а также внимание Сергея к деталям и сейчас обеспечивает плавучесть и стабильность судна под названием Web Control.

О РАБОТЕ И НЕ ТОЛЬКО

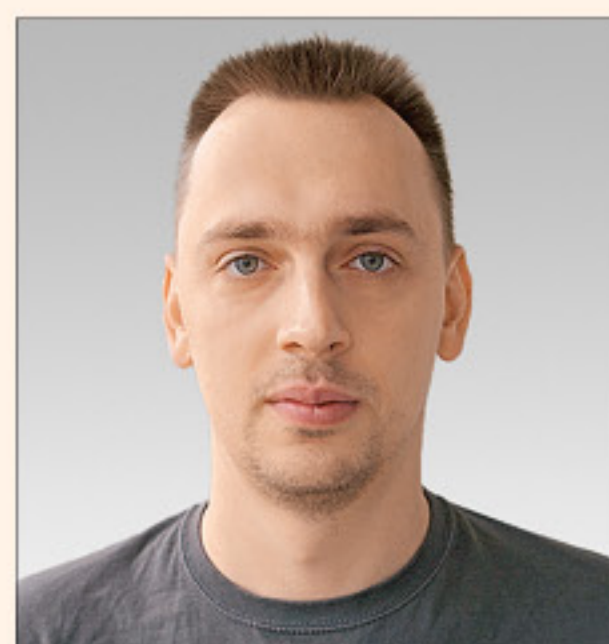
Сейчас коллектив Фаззи Лоджик Лабс составляет 50 сотрудников, часть из них работает с самого начала. Сейчас компания планирует активно увеличивать штат и повышать квалификацию уже работающих специалистов.

Сергей Парфёнов, технический директор: «Безусловно, большую часть занимает работа... Если выдаётся свободное время, предпочитаю проводить его с семьёй, с детьми: прогулки, велосипедные марши, поездки... Особое место в жизни — рыбалка. Выезжаю на несколько дней, что позволяет оторваться от городской суеты, погрузиться в другой — дикий — мир и полностью перезагрузиться».

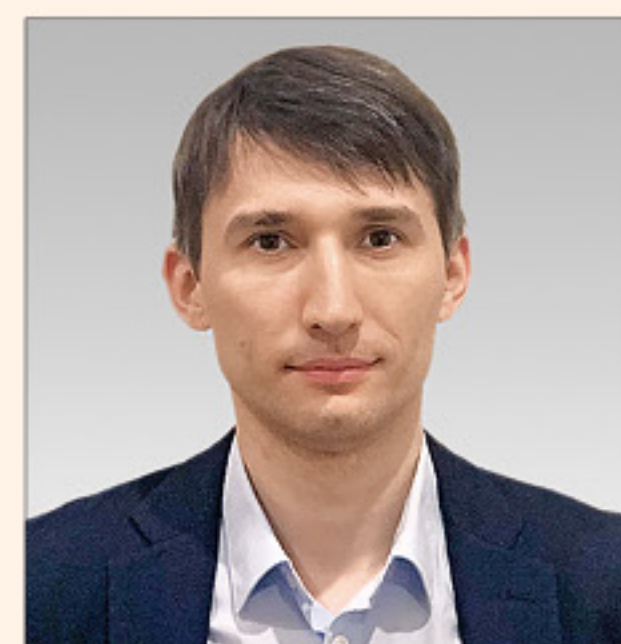
Михаил Дудалев, начальник отдела анализа данных: «Я семь лет прожил в



Сергей ПАРФЁНОВ



Михаил ДУДАЛЕВ



Тагир КУДАШЕВ

Австралии, где работал с машинным обучением в алготрейдинге и других направлениях для австралийских банков. Сейчас пытаюсь доучить китайский, а вот с путешествиями в прошлом году пришлось притормозить...»

Тагир Кудашев, начальник отдела внедрения и сопровождения ПО:

«Люблю катание на сноуборде, велосипеде, электросамокате, а также... локальные IT-эксперименты: на выходных люблю внедрять релизы (шутка). Последние два года много свободного времени тратится на воспитание трёх дочек, две из которых двойняшки».

Создавая бизнес, Андрей и Сергей руководствовались принципами артели, добровольного объединения людей для совместной деятельности, и искали в свою команду таких же единомышленников-новаторов, как и они сами

Создавая бизнес, Андрей и Сергей руководствовались принципами артели, добровольного объединения людей для совместной деятельности, и искали в свою команду таких же единомышленников-новаторов, как и они сами. Труд должен создавать новую ценность и приносить удовольствие — вот один из их принципов. Только кросс-функциональная самоорганизующаяся команда способна решать любые задачи в изменяющемся мире. Только мотивированные профессионалы способны к инновациям и развитию. И это базовые принципы артели, только сформулированные в терминах Business Agility. Хочешь пробовать новое — приходи к нам,

мы тебе обеспечим фронт работ, поможем и поддержим, справедливо разделим результат — таков девиз у руководства. Неудивительно, что костяк коллектива — это выходцы из Бауманки, неудивительно, что в компании люди «приживаются» и остаются надолго. И это действительно работает, в чём также кроется залог успеха компании.

Будучи открытыми к инновациям в бизнесе, Андрей и Сергей и в личной жизни — страстные увлечённые люди, которые любят путешествовать и ищут новые впечатления, хотя и делают это по-разному. Как большой интеллектуал и глубокий знаток истории, Сергей предпочитает посещение исторических

мест, морские круизы, знакомство с новыми странами, будь то Исландия, Гренландия или Испания...

Стиль Андрея — открытие нового и неизведанного, поэтому самый лучший отдых для него — рюкзак, палатка и высокие горы в компании близких друзей. Здесь он черпает энергию, заряжается новой силой. И обязательно созидание, именно своими руками и каждый раз в новой сфере, будь то печь, дом или автомобиль.

Неудивительно, что часть сотрудников разделяют их увлечения, отправляясь вместе с ними в то или иное путешествие.

В июне компании Web Control исполняется 13 лет. За это время она стала перспективной и узнаваемой командой, но капитанами бизнеса были и остаются Андрей Акинин и Сергей Петров. Они по-прежнему не довольствуются достигнутым, ставят новые амбициозные цели и ведут свой корабль к новым землям. И это не столько про бизнес, сколько про жизнь, потому что компания и есть часть их жизни.

ПОДДЕРЖКА 24/7

Функция антифрод-систем — выявлять и предотвращать мошенничество. Однако важно, чтобы система была разработана с учётом специфики банковского бизнеса, легко интегрировалась с IT-инфраструктурой банка, была кросс-канальной.

С развитием функциональности системы процессы техподдержки в «Фаззи Лоджик Лабс» менялись, оптимизировались. Новые тренды кибератак требуют новых инструментов борьбы с ними. Сейчас система Smart Fraud Detection — это зрелый продукт, апробированный на больших данных российских банков. После внедрённых проектов компания «Фаззи Лоджик Лабс» предоставляет техническую поддержку 24/7 с оперативным устранением ошибок и анализом логов приложений.

Тагир Кудашев: «Вопросы по техподдержке возникают и в час ночи, и в 4 утра... Это были запросы по

конкретным клиентам, по сработавшим или несработавшим правилам, по моделям оценки риска и многие другие. Мысль о том, что мы сами строим компанию и отвечаем за её результат, определяет отношение к работе. К тому же в компании всегда можно было работать удалённо ещё до пандемии, а кто хотел, по желанию, ездили в офис...»

Раз в полгода для компаний-заказчиков выходит бесплатный релиз с новыми разработками в функциональности системы и защитой от новых типов мошеннических атак.

Михаил Дудалев: «Одним из источников для обновлений системы служат инциденты из банков. Это похоже на игру в кошки-мышки: задача — обнаружить фрод и поймать злоумышленника, когда это даже на аномалию не похоже. Поэтому мы не только работаем по запросам, но и отслеживаем гипотетический фрод и открытые новые уязвимости по разным источникам».

ЗАЩИТА КЛИЕНТОВ

Диджитализация последних лет и пандемия коронавируса существенно изменили многое: то, как люди стали покупать и платить, то, как многие индустрии стали работать, 2020 год можно назвать годом электронной коммерции. Доля фрода и мошеннических операций в России — одна из самых низких в мире, высока доля платежей, которые проходят по самым современным стандартам шифрования и безопасности.

Сергей Парфёнов: «Для нас, в компании «Фаззи Лоджик Лабс», защита репутации и спасение денежных средств клиентов — это основные задачи, с которыми мы имеем дело. В общей сложности удалось спасти от внутреннего и внешнего фрода более 100 млрд рублей финансовых средств клиентов»¹.

¹ Данные по предотвращению хищения денежных средств, Сбер, период 31/12/2018–31/12/2020, из открытых источников.



Дмитрий СЛОБОДЕНЮК
коммерческий директор
компании ARinteg



Алексей КУРСКИХ
руководитель направления
pre-sale по ИБ компании
ARinteg

ИСКУССТВО ВЫБИРАТЬ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ С «ЛАБОРАТОРИЕЙ КАСПЕРСКОГО» И ARINTEG

Вероятность кибератаки на бизнес есть всегда, независимо от его размера, количества компьютеров или денежных средств на счёте. Поэтому защищать компьютерную сеть и данные компании нужно, однако траты должны быть пропорциональны стоимости защищаемых активов и размеров компании.

Как защитить компанию от репутационных и денежных потерь? И от каких показателей для подбора оптимального решения отталкивается ARinteg, один из ведущих системных интеграторов, с продуктами от «Лаборатории Касперского», одного из мировых лидеров кибербезопасности, — расскажем в статье.

ТИПОЛОГИЯ КИБЕРАТАК

Выбор средств для защиты киберпространства широкий, а их применимость определяется ответственными специалистами компании. В целом угрозы в интернете можно разделить на два типа: веерные атаки и точечные целевые атаки.

Киберпреступность часто прибегает к веерным рассылкам, когда вредоносный код или фишинговые ссылки отправляются всем подряд в надежде, что кто-нибудь, всё равно кто, попадёт на неё. Такие атаки чаще всего делаются с целью наживы или усиления вредоносной архитектуры (например, для увеличения ботнета).

Атаки такого типа отбиваются довольно хорошо автоматизированными

средствами защиты вроде классического антивируса в силу того, что зачастую кибермошенники используют один и тот же инструмент для атаки, один и тот же вредоносный код, который хорошо детектируется базовыми средствами защитного ПО. Естественно, под эти атаки попадают практически все компании и частные лица, так как атака не имеет конкретной цели.

Точечные целевые атаки — более изощрённый тип угроз, включающий этапы подготовки, изучение цели, возможно, подкуп пользователей или проникновение за периметр сети нестандартными средствами. Таким нападениям, как правило, подвержены обычно только крупные компании, так как цель всегда должна оправдывать средства, а денег у крупных компаний всегда больше, чем у малого бизнеса. Кроме того, за такими атаками могут стоять другие государства с целью шпионажа.

Целенаправленные атаки наносят колоссальный ущерб — технический, финансовый или репутационный. Они

почти всегда способны обойти все автоматизированные средства защиты жертвы и могут быть зачастую обнаружены только экспертами информационной безопасности и только сложными системами типа расследований инцидентов Threat Hunting.

Компании среднего размера подвержены обоим типам угроз: и веерным, и целенаправленным.

ЗАЩИТА С «ЛАБОРАТОРИЕЙ КАСПЕРСКОГО»

Выбор нужного продукта или сервиса для обеспечения необходимого уровня безопасности любой организации — лишь самый первый шаг. Для успеха бизнеса в долгосрочной перспективе очень важно разработать продуманную стратегию корпоративной киберзащиты. Основная идея состоит в том, что размер отделов и экспертиза информационной безопасности и отдела информационных технологий напрямую зависят от типов угроз, с которыми предполагается бороться. Ровно такая же аргументация должна

Выбор нужного продукта или сервиса для обеспечения необходимого уровня безопасности любой организации — лишь самый первый шаг. Для успеха бизнеса в долгосрочной перспективе очень важно разработать продуманную стратегию корпоративной киберзащиты

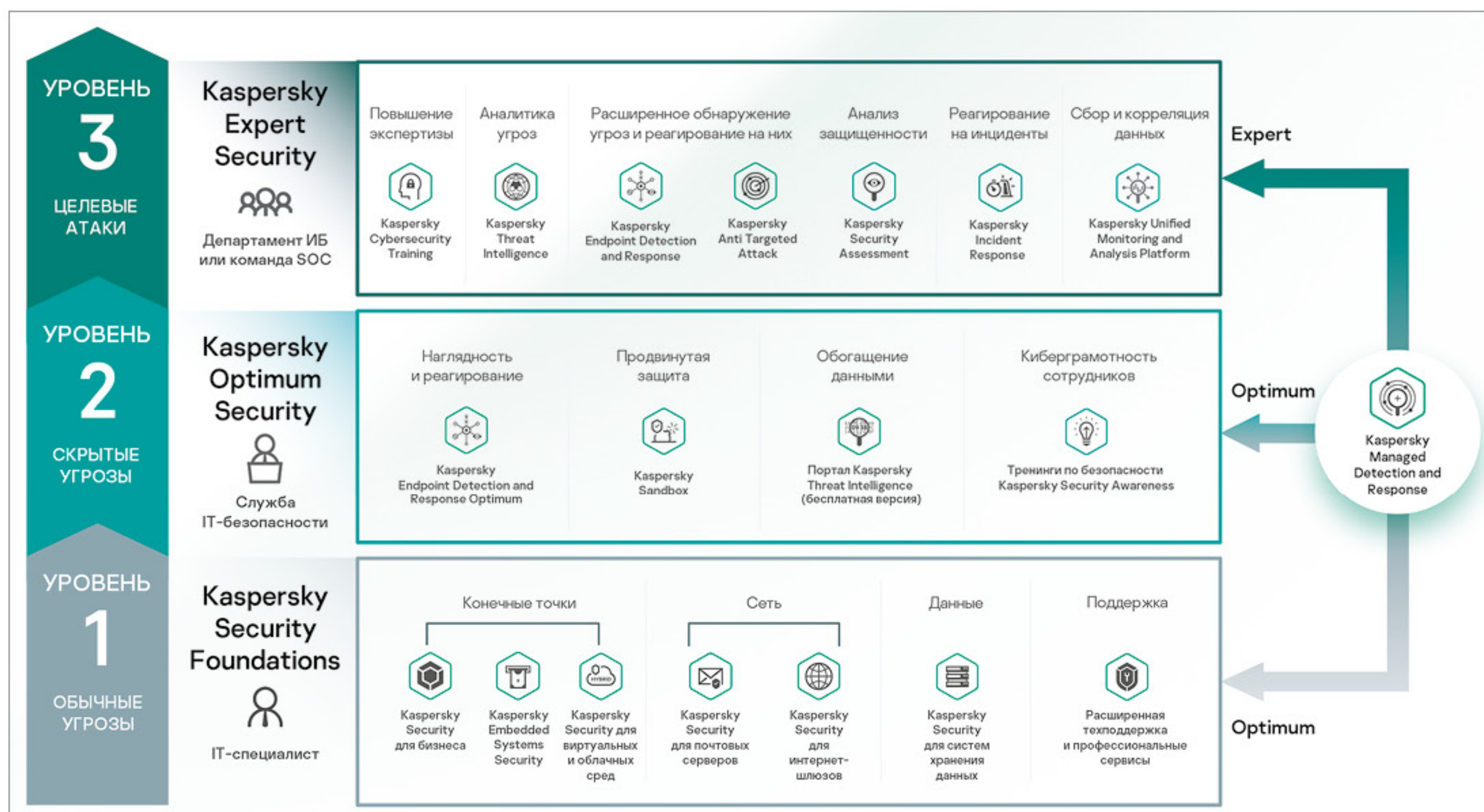


Рисунок 1. Портфолио решений для бизнеса

прослеживаться и при выборе инструментов информационной безопасности.

Решения «Лаборатории Касперского» удовлетворяют любые потребности современного бизнеса в кибербезопасности вне зависимости от уровня ИБ-зрелости организации. Благодаря разработанному производителем ступенчатому подходу, включающему различные уровни защиты от киберугроз всех типов, можно эффективно блокировать простые атаки, обнаруживать сложные, быстро реагировать на любые инциденты и предотвращать будущие угрозы в зависимости от потребностей организации.

КАК ПОДОБРАТЬ ОПТИМАЛЬНОЕ РЕШЕНИЕ?

С учётом актуальных угроз и различных уровней кибербезопасности клиентов можно разделить решения для ИБ на три уровня (рис. 1).

1. Kaspersky Security Foundations

Kaspersky Security Foundations — базовый этап организации безопасности для компаний любого масштаба с инфраструктурой любой сложности, заключающийся в создании интегрированной и автоматизированной системы защиты от сложных угроз. На этом уровне

обеспечивается многовекторное автоматическое предотвращение большого числа возможных инцидентов безопасности, вызванных обычными угрозами.

Обычно такого решения вполне достаточно для небольших компаний, в которых есть только IT-отдел. Безусловно, в средних и крупных компаниях этот слой киберзащиты также должен присутствовать как обязательный, однако заметим, что его одного может быть недостаточно для эффективной и стабильной работы бизнеса.

Основной продукт для первого, базового, уровня защиты — «Kaspersky Security для бизнеса».

2. Kaspersky Optimum Security

Уровень Kaspersky Security Оптимальный — это логическое продолжение Kaspersky Security Foundations. Он позволяет организациям с развивающейся IT-инфраструктурой защищаться от обычных атак и угроз, способных обходить существующие механизмы предотвращения. Решения на этом уровне подобраны с учётом ограниченности ресурсов и идеально подходят небольшим, но уже существующим ИБ-отделам, обладающим базовыми знаниями и опытом, но имеющим желание улучшать свой экспертный опыт

в этой области и бороться со всё более сложными угрозами.

На этом уровне клиенты могут улучшить систему обнаружения угроз и реагирования на них, а также воспользоваться преимуществами круглосуточной защиты, управляемой экспертами. В то же время тренинги Kaspersky Automated Security Awareness Platform по основам кибербезопасности помогут выработать у сотрудников навыки кибергигиены и мотивировать их следовать безопасному поведению.

С Kaspersky Security Оптимальный появляется возможность находить «скрытые угрозы» — вредоносное программное обеспечение, использующее различные маскирующие механизмы. Подобные средства нападения стоят особняком от других типов атак в силу того, что они представляют из себя уже внедрённое в сеть организации вредоносное программное обеспечение, которое выполняет свою работу, но не может быть обнаружено стандартными средствами защиты.

Большого смысла бороться со скрытыми угрозами в размерах малого предприятия нет, хотя и очень бы хотелось, но догадаться о наличии такого ПО можно зачастую только по косвенным



Решение Kaspersky Managed Detection and Response позволяет активировать передовые функции защиты без необходимости нанимать дополнительных сотрудников и обучать существующих

признакам или поведенческому анализу. И дело не только в том, что средства для обнаружения скрытых угроз стоят дорого, дело в наличии необходимой экспертизы и понимания механизма их работы техническими специалистами заказчика.

Именно потому «Лаборатория Касперского» приняла решение включить во второй уровень защиты комплект программного обеспечения Kaspersky EDR для бизнеса Оптимальный — инструмент анализа и блокировки скрытых угроз, который оптимизирован под работу в рамках небольших компаний.

На этом уровне заказчикам предлагается уже использовать такой продвинутой методы обнаружения скрытых и неизвестных угроз, как песочница. Ранее подобные инструменты были доступны только в рамках «тяжёлых» решений, например KATA (Kaspersky Anti Targeted Attack) или KEDR (Kaspersky Endpoint Detection and Response).

3. Kaspersky Expert Security

Если у компании есть вероятность столкнуться с реальной АРТ-атакой и организациям требуется эффективная защита от сложных атак, лучше установить

не только автоматизированные средства борьбы с киберугрозами, но и развитые средства анализа и расследований преступлений в этой области.

Для удовлетворения запросов крупных ИБ-департаментов и команд SOC с хорошей хорошей и развитой развитым экспертизой экспертным опытом в этой области «Лаборатория Касперского» предоставляет единую платформу безопасности, которая позволяет справиться со сложнейшими современными угрозами и целевыми атаками.

Центральный элемент единой платформы безопасности — решение класса SIEM Kaspersky Unified Monitoring and Analysis Platform (KUMA). Для борьбы с угрозами и целевыми атаками KUMA собирает и анализирует данные из всех подключённых к нему источников — продуктов «Лаборатории Касперского» и решений сторонних производителей.

Компоненты экосистемы дополняют друг друга и обмениваются информацией. В итоге ИБ-специалисты получают полную картину происходящего в инфраструктуре и оперативно отражают кибератаки любой сложности.

Решение Kaspersky Managed Detection and Response позволяет активировать передовые функции защиты без необходимости нанимать дополнительных сотрудников и обучать существующих. В частности, оно даёт возможность делегировать «Лаборатории Касперского» поиск угроз и реагирование на инциденты, чтобы можно было направить ограниченные ресурсы штатных ИБ-специалистов компании на решение других важных задач.

Системный интегратор должен иметь широкий опыт работы в этой сфере, чтобы верно рассчитать рентабельность затрат и релевантность внедряемого продукта. ARinteg специализируется на подборе и установке таких оптимальных ИБ-решений уже более 25 лет, в частности, на установке и внедрении решений мирового уровня, таких как продукты «Лаборатории Касперского», позволяющих решить организациям разного масштаба задачу любой сложности независимо от типов потенциальных угроз.



Валерий КУЛИКОВ
обозреватель BIS Journal

ONE IDENTITY MANAGER РАЗРЕШАЕТ ВЗЛЕТ

О СОЗДАНИИ IAM-СИСТЕМЫ В ДИНАМИЧНО
РАЗВИВАЮЩЕМСЯ АЭРОПОРТУ ШЕРЕМЕТЬЕВО

На фоне утверждений о расширении источников и коварстве внешних киберугроз глубоко погружённые в тему информационной безопасности (ИБ) специалисты единодушны во мнении, что главные угрозы для конфиденциальности информации и целостности/доступности информационных ресурсов и информационных систем таятся внутри организации. При этом для большой, динамично развивающейся компании упомянутые угрозы зачастую могут исходить не от враждебных сил, а возникать вследствие несовершенства системы для управления идентификацией и правами доступа (IAM). А то и вследствие фактического отсутствия такой системы именно как системы, меняющейся синхронно с изменениями в основном ядре деловых процессов в компании/организации.

ПОДТВЕРЖДЕНИЕ ТЕЗИСА

В то же время можно использовать такой подход к созданию, эксплуатации и поддержке IAM-системы, который обеспечит экономически эффективное её внедрение, простоту администрирования и обеспечение должного уровня ИБ в контексте процессов управления идентификацией и доступом к различным ресурсам компании/организации.

Подтверждение этого тезиса можно найти в опыте внедрения IAM-системы на основе платформы One Identity

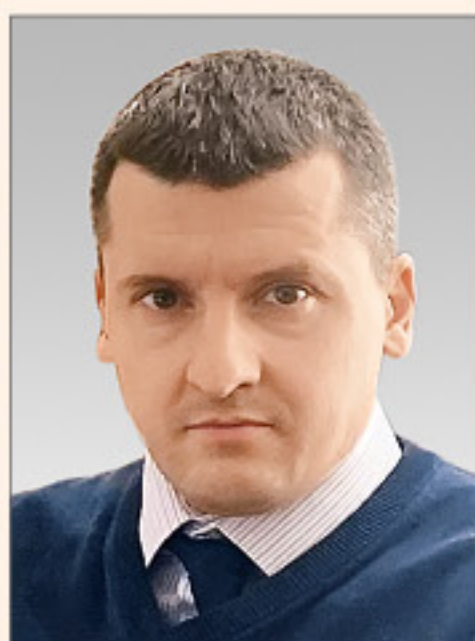
Manager в аэропорту Шереметьево. Эта платформа сочетает в себе законченность «коробочного» решения и возможности кастомизации и развития силами самой организации. Впрочем, слово «силами» возможно слишком сильное определение для потребных ресурсов (прошу прощения за тавтологию), ибо в конкретном примере речь идёт о нескольких специалистах (меньше пяти, их количество менялось по ходу выполнения проекта), в то время, как общие масштабы и человеческие ресурсы аэропорта Шереметьево хорошо представляют, полагая, большинство читателей этого материала.

СТАРТОВЫЕ УСЛОВИЯ

Какими были стартовые условия? Рассказывает начальник Службы информационной безопасности аэропорта Шереметьево Андрей Корабельников: «Во-первых, мы недавно вошли в большую лигу аэропортов с

пассажиропотоком более 40 млн пассажиров в год. Во-вторых, у нас существовал ручной режим управления доступом с периодическими проверками прав доступа. В-третьих, основная задача, которая у нас была на момент старта проекта, — это прекращение избыточного доступа».

По сути, стартовые условия, в которых было принято решение о начале проекта по внедрению новой системы комплексного и непрерывного управления идентификацией и правами доступа, — это движение, переход. Переход от состояния организации, замершей в какой-то момент в своём развитии, организации со стабильным в количественном и персональном измерениях коллективом, к состоянию, когда меняется и развивается базовая инфраструктура и деловые процессы аэропорта, проводится кадровая реорганизация, появляются новые отделы, открываются



Андрей Корабельников,
начальник Службы информационной
безопасности аэропорта Шереметьево:

«В 2018 году у нас появилось понимание, чего мы хотим от IdM-продукта и какие характеристики важны. При выборе коммерческого решения для создания IAM-системы аэропорта Шереметьево рассматривалось несколько «претендентов». One Identity Manager выиграл «гонку» по сумме критериев».



в конкретных временных рамках новые проекты и для этого привлекается дополнительный персонал, и завершаются старые проекты, а задействованные в них сотрудники переходят на новые места с иными требованиями к использованию ресурсов компании.

В новых условиях «ручное» управление процессами идентификации и правами доступа стало не поспевать за меняющимися требованиями к коррекции прав доступа, требованиям к своевременности прекращения избыточного доступа, не поспевать за динамикой требований к управлению идентификацией и правами доступа новых сотрудников, находящихся в разных трудовых отношениях с компанией.

ЖЁСТКАЯ КОНКУРЕНЦИЯ

Почему была выбрана именно компания One Identity? Рассказывает **Андрей Корабельников**: «В 2018 году у нас появилось понимание, чего мы хотим от IdM-продукта и какие характеристики важны. При выборе коммерческого решения для создания IAM-системы аэропорта Шереметьево рассматривалось несколько «претендентов». One Identity Manager выиграл «гонку» по сумме критериев. Можно отметить следующие важные особенности One Identity Manager, которые были важны для нас:

- ♦ хорошая документированность системы;
- ♦ высокий уровень зрелости продукта;
- ♦ готовность системы к самостоятельному сопровождению и развитию. Многие вещи мы смогли сделать самостоятельно;
- ♦ открытость интерфейса для глубокой кастомизации;

♦ *глубокая интеграция с системой SAP».*

Другим достоинством One Identity Manager, оцененным специалистами аэропорта Шереметьево, стала открытость кода платформы, что позволяет производить кастомизацию конечного решения в ходе конкретного проекта и оперативно актуализировать возможности уже работающей IAM-системы аэропорта с использованием agile-подхода по мере появления новых потребностей.

В ДВА ЭТАПА

Создание IAM-системы в Шереметьево, которая, как уже доказано практикой, удобно обеспечила сотрудникам компании постоянный доступ к требуемым приложениям, платформам, системам и данным, происходило в два этапа, без предпроектного «консалтинга».

С апреля по октябрь прошёл пилотный проект, в результате которого организация получила надёжно работающую и высокоавтоматизированную IAM-систему, которая к тому же освободила базовые ИТ-службы от поддержки системы управления идентификацией и правами доступа.

После этого, менее чем через год, по мере роста зрелости процессов в организации, был выполнен расширенный проект.

В ЧИСЛЕ ПРОЧЕГО

Результатом выполненных работ оказалась, в числе прочего, возможность для пользователей в компании управлять личным доступом через веб-портал самообслуживания без вмешательства ИТ-специалистов. При необходимости с помощью этого портала пользователи создают запросы на предоставление

доступа к ресурсам компании, выбрав необходимый ресурс и «положив» его в корзину, после чего запрос проверяется. Руководитель может самостоятельно одобрять или отклонять поступающие запросы, не обращаясь за помощью к ИТ-специалистам — для этого достаточно использовать графический редактор. При этом One Identity Manager поддерживает режим моделирования, который позволяет оценить последствия изменений до того, как они будут внедрены в работу и выявить на какие объекты, пользователей, правила и процессы такие изменения повлияли.

Встроенные в One Identity Manager инструменты аудита позволяют отслеживать любые действия, выполняемые с любыми объектами в рамках любых процессов, а также все производимые изменения объектов и процессов. Функция «аудиторского следа» позволяет получить информацию о том, что было изменено, каким образом, кем и в какое время. Полученная информация может быть представлена в удобной для анализа форме, с помощью создаваемых в графическом редакторе отчетов.

ПРОВЕРЕНО ПРАКТИКОЙ

Что на сегодня? Рассказывает **Андрей Корабельников**: «Мы считаем, что мы достаточно плавно прошли этап появления роли владельца ресурса в компании. Пользователи на практике убедились и усвоили, что если все делать правильно, по процессу, то они в итоге тратят меньше времени.

Процесс идет. Сейчас у нас команда управления доступом состоит из двух человек. В ближайшее время планируем подключить к IdM порядка десяти ИТ-систем, которые необходимы в рамках выполнения требований 187-ФЗ по защите критической инфраструктуры».

В заключение уместно заметить, что на основе One Identity Manager выполнено немало успешных проектов, в мире более 700 и около 40 проектов в России и СНГ, что позволяет российским заказчикам предварительно ознакомиться с возможностями «боевых» решений на основе этой платформы. В качестве «вишенки» на торте перед окончательным выбором One Identity Manager возможно проведение бесплатного «пилота» на тестовой среде.



Илья ОСАДЧИЙ
директор по развитию бизнеса,
Тайгер Оптикс



Владимир СОЛОВЬЁВ
руководитель направления
внедрения средств защиты
АО «ДиалогНаука»

ХАНИПОТЫ И DECEPTION

КАК МЕНЯЮТСЯ ТЕХНОЛОГИИ АКТИВНОЙ ЗАЩИТЫ НА ОСНОВЕ КИБЕРОБМАНА

ВВЕДЕНИЕ В ТЕХНОЛОГИИ КИБЕРОБМАНА

Несмотря на существенные усилия, которые компании прилагают к предотвращению успешных взломов, реальность такова, что, если продвинутые киберпреступники нацеливаются на определённую организацию, они найдут способ проникновения во внутренний контур.

Обмануть злоумышленника и заставить его думать, что он получил доступ к ценным данным, — это совсем не новая идея в сфере ИБ. Первая сеть ханипотов была разработана ещё в 1999 году в рамках Honeynet Project. Тогда эта идея была инновационной и результативной, но за последние 20 лет ИТ-инфраструктура компаний стала гораздо сложнее, а злоумышленники набрались опыта.

У современных ханипотов, как и у Deception-технологий нового поколения (таких как, например, система Illusive), есть свои преимущества, и очень важно понимать разницу между этими двумя классами решений — это позволит выбрать оптимальный способ защиты компании от злоумышленников, которые смогли обойти первый эшелон средств защиты и незаметно проникнуть внутрь сети.

ТРАДИЦИОННЫЕ СРЕДСТВА ЗАЩИТЫ ПАСУЮТ ПЕРЕД СОВРЕМЕННЫМИ ХАКЕРАМИ

Злоумышленники всё чаще обходят такие классы решений, как NGFW, песочницы, антивирусы, EDR и

XDR — независимо от того, насколько высоко эти решения находятся в квадрантах аналитических компаний и насколько хорошо они настроены. Эксперты рекомендуют считать, что вы уже взломаны, и ваша задача — как можно скорее найти и остановить злоумышленника в своей сети до того, как он нанесёт реальный ущерб.

Поэтому своевременное выявление и грамотное реагирование на активную атаку являются залогом успеха. Ханипоты и Deception-технологии нового поколения заметно отличаются от традиционных средств и подходов к киберзащите. Там, где традиционные продукты стремятся отреагировать на кибератаку и как можно скорее изолировать её, ханипоты и Deception-системы нового поколения занимают более активную позицию, детектируя не атаку, а самих киберпреступников в процессе их работы.

ВЫЧИСЛЯТЬ ХАНИПОТЫ — ПРИВЫЧНОЕ ДЕЛО ДЛЯ ЗЛОУМЫШЛЕННИКОВ

Понимание способностей злоумышленников важно для построения системы защиты, которая сможет их выявить. Вот несколько способов, которыми злоумышленники определяют наличие ханипотов:

- ♦ если доступ к системе кажется слишком простым, вероятно, это подделка;
- ♦ обычно системы, подключённые к Интернету, не имеют ненужных портов и служб; любое отклонение от этой

конфигурации может указывать на ловушку;

- ♦ если в системе всё ещё есть настройки по умолчанию, это увеличивает вероятность использования ханипота;

- ♦ если на жёстком диске много свободного места или установлено очень мало программного обеспечения, это может быть ханипот;

- ♦ если названия папок тривиальны (например, «Зарплаты», «Данные клиентов», «Пароли»), очевидно, что системы нацелены на заманивание злоумышленников.

Все эти сигналы говорят злоумышленникам, что система может быть ненастоящей.

DECEPTION-ТЕХНОЛОГИИ СРЫВАЮТ ПЛАНЫ ЗЛОУМЫШЛЕННИКОВ ПО ВСЕЙ СЕТИ

Атаки с использованием социальной инженерии и нацеленного фишинга служат примером того, как можно обойти любые классы решений, в том числе ханипоты. Многие современные атаки начинаются с того, что пользователю доставляют «приманку», например фишинговое письмо, которое он открывает на компьютере, что позволяет вредоносному ПО проникнуть во внутреннюю сеть, а злоумышленнику — перейти к планированию и выполнению следующего этапа атаки.

Ханипоты не способны взаимодействовать с целенаправленной фишинговой атакой так, как это делают

пользователи. Следовательно, ханипоты не смогут спровоцировать и выявить атаку, использующую такой вектор. В отличие от ханипотов, обманные технологии нового поколения могут автоматически изменять обманную среду, не оставляя её статичной, как и подobaет настоящей сети, в которой пользовательские и сетевые данные естественным образом меняются. При этом Deception-технологии выявляют злоумышленника всего за три или четыре его шага по сети, даже если обманные элементы развёрнуты не на каждом узле.

Практический опыт внедрений авторов статьи показывает, что даже непосредственные администраторы систем киберобмана не всегда могут определить, какие артефакты реальные, а какие являются результатом работы Deception-систем.

Технологии обмана нового поколения дают пользователям мощную функциональность обнаружения атак и сбора форензики в реальном времени, практически без ложных срабатываний, а атакующие никогда не узнают, что они находятся под наблюдением. Ханипоты тоже эффективны при поимке злоумышленников, но они обладают гораздо меньшей степенью обнаружения реальных угроз, генерируют гораздо больше ложных срабатываний и не предоставляют форензику с реальных узлов, используемых злоумышленниками для атаки.

RED TEAM ПОДТВЕРЖДАЮТ: ТЕХНОЛОГИИ КИБЕРОБМАНА ПРЕУСПЕВАЮТ ТАМ, ГДЕ ХАНИПОТЫ НЕ СПРАВЛЯЮТСЯ

В недавних параллельных тестах Red Team ханипоты продемонстрировали сравнительно низкие показатели обнаружения, но высокие издержки на обслуживание и управление. Ханипоты не предоставляют контекста, они одномерны, и их сложно масштабировать в динамической среде.

Обманные технологии нового поколения были разработаны с учётом современного ландшафта угроз. В тестах Red Team эти технологии получили высокие оценки по всем показателям:

- ♦ участники Red Team сообщают, что обойти современные технологии

Практический опыт внедрений авторов статьи показывает, что даже непосредственные администраторы систем киберобмана не всегда могут определить, какие артефакты реальные, а какие являются результатом работы Deception-систем

киберобмана крайне сложно. Попытки горизонтального продвижения Red Team по сети генерировали тысячи алертов. Технологии киберобмана позволили легко отследить траекторию атаки и не дали Red Team достигнуть конечной цели;

- ♦ киберпреступники компрометируют системы, горизонтально перемещаясь от одного узла к другому. Защитные обманные технологии обнаруживают горизонтальное движение на ранних этапах, собирают данные форензики в реальном времени и составляют «портрет» атакующего;

- ♦ большое внимание уделяется векторам атаки злоумышленника, благодаря которым их можно застать врасплох: приманки появляются там, где они не могли бы появиться при использовании ханипотов, поэтому у атакующих практически нет возможности узнать, что они действуют по фальшивому сценарию.

БОЛЬШЕ МЁДА, МЕНЬШЕ ДЁГТЯ: ЛЁГКИЕ И УДОБНЫЕ ТЕХНОЛОГИИ КИБЕРОБМАНА

Подходы ханипотов и Deception-технологий значительно различаются как с точки зрения злоумышленника, так и с точки зрения специалиста по ИБ. Ханипоты — это статические системы, которые устанавливаются в выбранной подсети. Они действуют как своего рода песочницы, пытаясь заманить злоумышленников наличием конфиденциальных данных, а затем отслеживая их действия.

С другой стороны, Deception-технологии представляют собой «королевство кривых зеркал». Ложная информация оказывается повсюду на пути злоумышленников, которые используют её на стадии горизонтального продвижения. Злоумышленники методичны — они собирают данные,

анализируют их и рассчитывают свой следующий шаг, неустанно продвигаясь по сети.

Обманные технологии Illusive учитывают такую методичность злоумышленников и извлекают из неё пользу, органично вплетая искусно подобранные «приманки» в реальную инфраструктуру компании, привлекая хакеров, уведомляя специалистов по ИБ и блокируя атаку. При этом компании могут не только останавливать атаки до того, как нанесён реальный ущерб, но и получать критически важную информацию о них в виде форензики, которая может пригодиться в расследованиях.

ЗАКЛЮЧЕНИЕ

Архитектура с применением ханипотов была передовой технологией для своего времени. Она заложила основу для более проактивного подхода к киберзащите и позволила держать злоумышленников на безопасном расстоянии. Однако современные киберпреступники уверенно обходят традиционные СЗИ, при этом избегая ханипотов. Очевидно, что компании, которые хотят защищаться от продвинутых и нацеленных атак, больше не могут фокусировать все свои ресурсы только на этих системах защиты.

* * *

Организациям нужно внедрять и продукты, направленные на внутреннюю поверхность атаки, например, такие как Deception-технологии Illusive. Такая превентивная технология позволяет отслеживать и блокировать злоумышленников, обошедших первую линию обороны, что является важным шагом на пути к современной системе кибербезопасности.



Наталия КАЗАНЬКОВА
старший менеджер
по продуктовому маркетингу
Positive Technologies

СПЕЦИАЛЬНО НА ВАС

КАК ФИНАНСОВЫЕ КОМПАНИИ ЗАЩИЩАЮТСЯ ОТ ЦЕЛЕВЫХ АТАК

Число целевых атак в мире растёт из квартала в квартал. По данным Positive Technologies, во II квартале 2021 года 77% атак были целевыми. Мишенью хакеров становятся и российские компании. Мы провели анонимный опрос среди специалистов по ИБ компаний различных отраслей и размеров. Результаты нашего исследования показали, что треть компаний подвергалась таргетированным атакам. Давайте обсудим, как такие атаки сказываются на финансовых организациях, насколько они защищены от них и какие тенденции в использовании средств защиты можно выделить.

Целевой считается кибератака, направленная на конкретную компанию, отрасль экономики или ограниченный круг частных лиц. Прежде чем атаковать, злоумышленники, как правило, проводят предварительную разведку и собирают информацию о выбранной жертве.

В ходе опроса мы выяснили, что финансовые организации чаще других страдают от целевых атак — об

этом сообщили 44% респондентов сферы, на втором месте — ТЭК (33%), тройку замыкают государственные компании (29%).

ЧЕМ ОПАСНЫ

В качестве основной цели, ради которой злоумышленники могут атаковать финансовую компанию, большинство опрошенных рассматривают кражу ценной информации (78%). Второй по популярности ответ — кража финансовых средств (63%). Эти две причины остаются главными мотивами атак хакеров на организации (рис. 1).

Почти половина представителей финансовых компаний (44%) уже сталкивались с целевыми атаками. Чаще всего это приводило к утечке информации, простоя инфраструктуры и нарушению бизнес-процессов.

Лидирующую позицию среди вредоносного ПО, применяемого в атаках на организации, занимают программы-вымогатели. В 17% случаев финансовые компании заплатили выкуп злоумышленникам. Мы рекомендуем не идти на поводу у атакующих и обращаться к специалистам для устранения последствий

атаки — нет гарантий, что злоумышленники восстановят работоспособность инфраструктуры, прекратят шантаж и не потребуют дополнительных денег.

ЗАЩИТА В ФИНАНСОВОМ СЕКТОРЕ

Специалисты по ИБ используют широкий набор инструментов защиты от атак: более половины респондентов выявляют угрозы с помощью антивирусов, систем выявления вторжений, межсетевых экранов, SIEM-систем, песочниц и веб-файрволов. SIEM-системы по уровню использования (75%) почти догнали антивирусы. Треть специалистов применяют системы анализа трафика (network traffic analysis, NTA). Компании больше не полагаются только на базовые средства защиты периметра, они осознают необходимость мониторинга безопасности внутренней сети — это хорошая новость (рис. 2).

Ещё один позитивный тренд: в ближайшие 1–3 года 40% специалистов планируют начать использовать комплексные решения для защиты целевых атак — это значит, что у них будет больше шансов обезопасить себя от таких угроз.

Решение Anti-APT от Positive Technologies (PT Anti-APT) включает в себя возможность глубокого анализа сетевого трафика (PT Network Attack Discovery) и систему для выявления атак с применением современного вредоносного ПО (PT Sandbox). Эти два компонента позволяют выявить действия атакующего как на периметре, так и уже в инфраструктуре.

Почти половина представителей финансовых компаний (44%) уже сталкивались с целевыми атаками. Чаще всего это приводило к утечке информации, простоя инфраструктуры и нарушению бизнес-процессов

АНАЛИЗ ФАЙЛОВ И ТРАФИКА

В инфраструктуре злоумышленники могут скрыть следы своего присутствия, но стереть их в трафике невозможно. Эту особенность использует система глубокого анализа трафика (NTA) PT Network Attack Discovery. Она замечает любую сетевую активность и анализирует обо всех подозрительных. PT NAD анализирует не только внешний, но и внутренний трафик, поэтому она детектирует перемещения злоумышленников внутри сети, попытки эксплуатации уязвимостей, атаки на конечных пользователей в домене и на внутренние сервисы.

Атаки с использованием вредоносного ПО по-прежнему занимают первое место в арсенале киберпреступников, их доля во II квартале 2021 года составила 73%. Одна из причин успеха таких атак — злоумышленники совершенствуют вредоносное ПО так, чтобы его не смогли обнаружить базовые средства защиты (антивирусы, межсетевые экраны, IPS, почтовые и веб-шлюзы). Поэтому есть отдельный класс решений для выявления вредоносных — песочница. Она запускает файл в изолированной виртуальной среде, анализирует его действия в системе и выносит вердикт — безопасен он или нет.

Благодаря гибкой настройке виртуальных сред в соответствии с реальными рабочими станциями компании PT Sandbox поможет эффективно выявлять ВПО, которое используется в целевых атаках.

РЕЗЮМЕ

Результаты опроса специалистов по ИБ подтвердили: вне зависимости от отрасли компания может стать жертвой целевой атаки. Опыт специалистов показывает, что такие атаки наносят ощутимый урон и могут напрямую повлиять на работу компании, в том числе на её финансовые результаты.

Есть и позитивные тенденции: компании понимают необходимость повышения уровня безопасности, так как планируют расширять арсенал средств защиты, включать в него специализированные комплексные решения для выявления целевых атак.

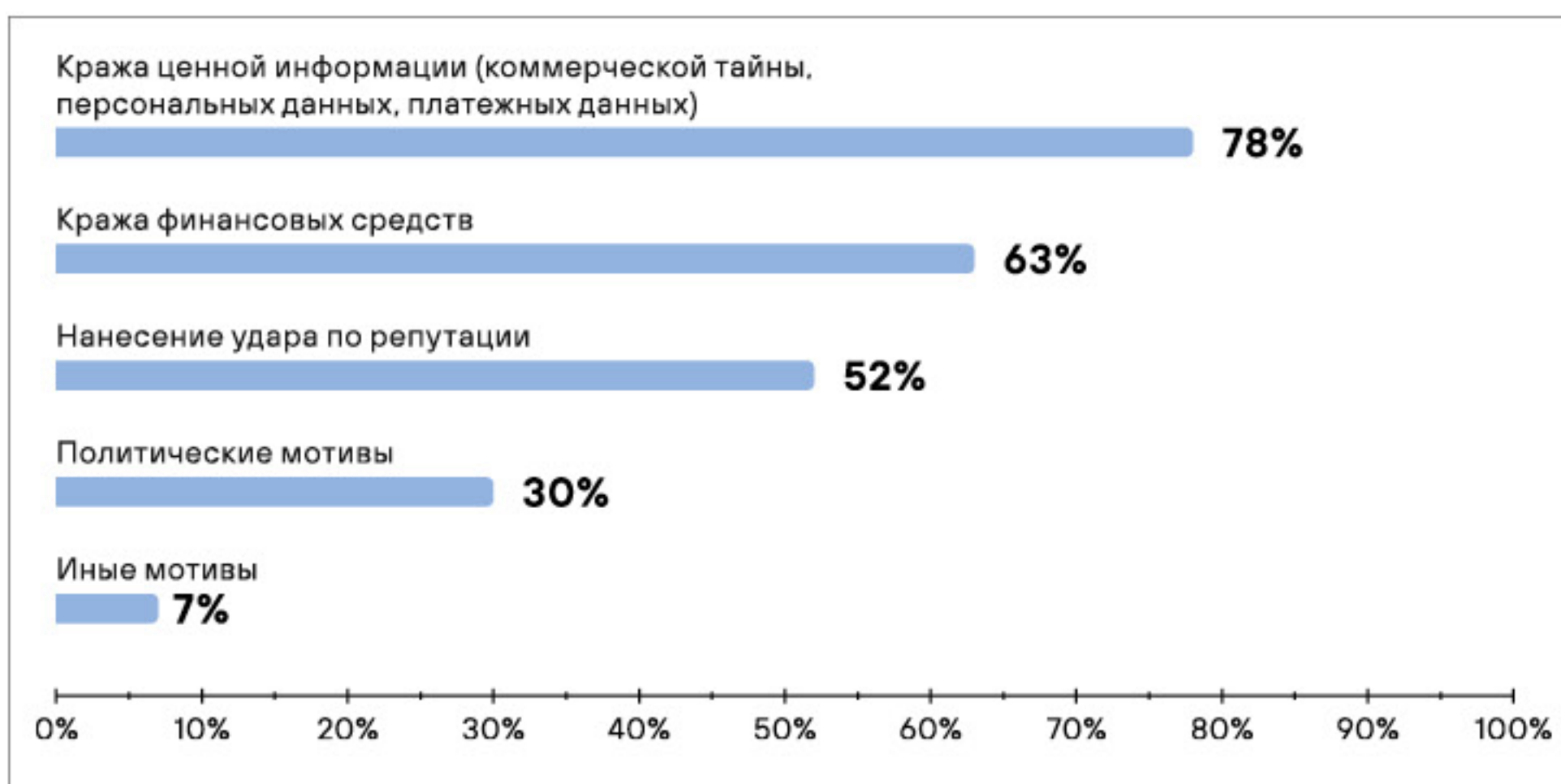


Рисунок 1. Цели, ради которых атакуют финансовые компании

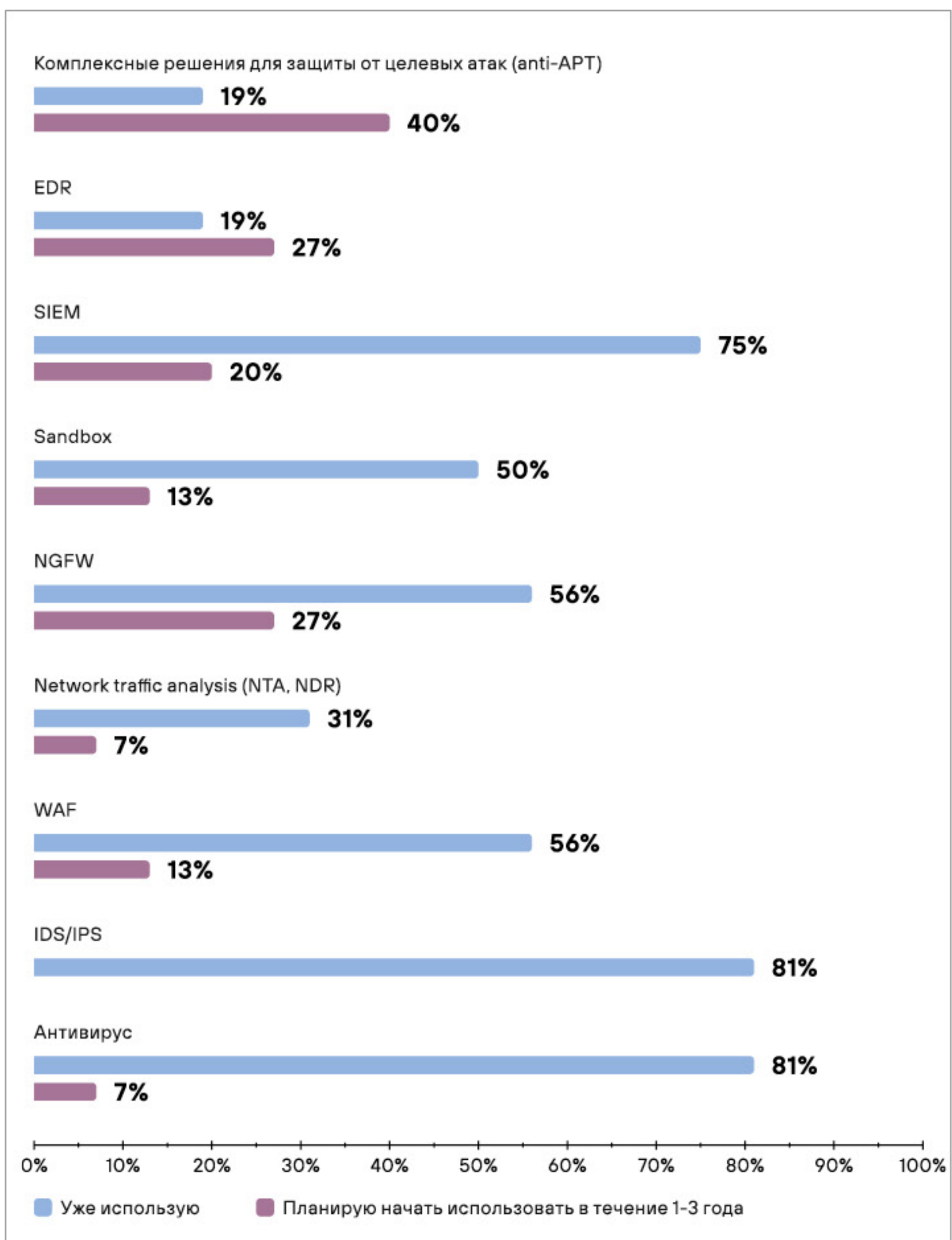


Рисунок 2. Инструменты защиты от атак, используемые специалистами информационной безопасности



Евгения КОЛОДИНА
директор по развитию
ГК «ЦИБИТ»



Алексей ВЕЛЯКИН
руководитель Департамента
аттестационных работ
ГК «ЦИБИТ»

РАЗБИРАЕМСЯ В ПРИКАЗЕ ФСТЭК РОССИИ № 77

О НОВОМ ПОРЯДКЕ АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

10 августа 2021 года был зарегистрирован Приказ Федеральной службы по техническому и экспортному контролю от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну». Документ внёс существенные изменения во все процессы, связанные с проведением аттестационных работ на соответствие требованиям по защите информации. Сегодня разбираем главные изменения.

ЧТО НУЖНО ЗНАТЬ О НОВОМ ПРИКАЗЕ

Алексей Велякин: «Итак, согласно Приказу, с 1 сентября этого года в силу вступили следующие изменения:

- ♦ аттестат соответствия выдаётся бессрочно (ранее документ выдавался на 3 года);
- ♦ каждые 2 года юридическое лицо обязано подтверждать факт проведённых периодических контролей аттестованных объектов информатизации;
- ♦ сохраняются требования по проведению ежегодного периодического контроля;
- ♦ ФСТЭК России ведётся реестр аттестованных объектов информатизации, в котором отражается статус аттестата соответствия;

♦ органы по аттестации обязаны в пятидневный срок после подписания аттестатов соответствия срок высылать их копии во ФСТЭК России для формирования данного реестра;

♦ все аттестаты, выданные до 01.09.21, действуют согласно прежним нормам и имеют срок действия 3 года.

Мы проанализировали Приказ и думаем, что документ подразумевает усиление контроля со стороны ФСТЭК России по отношению как к аттестующим органам, так и к самим объектам информатизации».

Евгения Колодина: «Без сомнений, новые правила, которые введены в действие данным документом, в целом повлияют на рынок и позволят сократить количество недобросовестных аттестационных центров, которые предоставляют услуги низкого качества.

Теперь регулятор может без дополнительной проверки приостановить действие выданного аттестата соответствия в случае выявления ошибок при выдаче аттестата или неподтверждения проведения необходимых контрольных испытаний».

ОБЛАСТЬ ПРИМЕНЕНИЯ

Алексей Велякин: «В пункте 3 Приказа указано, что его действие распространяется на проведение аттестационных мероприятий:

- ♦ государственных и муниципальных информационных систем (в том числе

информационных систем персональных данных);

♦ информационных систем управления производством, используемых организациями оборонно-промышленного комплекса;

♦ защищаемых помещений для ведения конфиденциальных переговоров;

♦ при решении проведения аттестации для значимых объектов КИИ, информационных систем персональных данных, автоматизированных систем управления производственными и технологическими процессами на критически важных объектах».

ПОРЯДОК АТТЕСТАЦИИ

Алексей Велякин: «Согласно новому документу, процесс аттестации можно разделить на шесть этапов:

1. Орган по аттестации назначает аттестационную комиссию.
2. Владелец объекта информатизации предоставляет органу по аттестации всю необходимую документацию.
3. Аттестационная комиссия изучает документы.
4. Разрабатывается программа и методики аттестационных испытаний, согласовывается с владельцем объекта информатизации.
5. Проводятся аттестационные испытания.
6. По результатам испытаний выдаётся аттестат соответствия».

Алексей Велякин: «В данном приказе отмечено: аттестационные испытания могут завершаться без выдачи аттестата соответствия в том случае, если на объекте информатизации выявлены существенные недостатки в области защиты информации, которые невозможно устранить в рамках проведения аттестационных мероприятий. В такой ситуации выдаётся отрицательное заключение и работы прекращаются. Если владелец объекта информатизации не согласен с выданным заключением, он может направить претензию во ФСТЭК России. Далее регулятор рассматривает жалобу и делает вывод, легитимно ли решение органа по аттестации. Стоит отметить: пакет документов, которые владельцу объекта информатизации необходимо предоставить для проведения аттестационных работ, соответствует уже бывшим в действии стандартам в соответствии с «Положением по аттестации объектов информатизации по требованиям безопасности информации» (утверждено председателем Гостехкомиссии России 25 ноября 1994 года) и «ГОСТ Р О 0043–003–2012. Защита информации. Аттестация объектов информатизации. Общие положения. Москва, Стандартинформ, 2012».

Перечень документов следующий:

- ◆ технический паспорт;
- ◆ акт классификации информационной системы;
- ◆ организационно-распорядительная документация;
- ◆ при наличии: модель угроз безопасности информации, техническое задание на создание ОИ, проектная документация, эксплуатационная документация, результаты анализа уязвимостей.

В этом ключе новый приказ ФСТЭК России № 77 не отменяет действующие документы, скорее выступает дополнением».

ГЛАВНЫЕ НОВОВВЕДЕНИЯ

Евгения Колодина: «Мы отмечаем несколько принципиальных пунктов, которые могут оказать сильное влияние на рынок в целом.

Самое первое — аттестат соответствия теперь выдаётся на весь срок экс-

плуатации объекта информатизации. И если для государственных информационных систем эта норма не нова, то теперь новый документ вводит её и для защищаемых помещений.

Далее стоит обратить внимание на то, что во ФСТЭК России теперь ведётся реестр аттестованных объектов информатизации. В том числе в него вносятся сведения обо всех аттестованных объектах информатизации, которые попадают под действие данного Приказа, с указанием действующего статуса».

Алексей Велякин: «ФСТЭК России особое внимание уделяет контролю аттестованных объектов информатизации: теперь органы по аттестации отчитываются регулятору по каждому аттестованному ОИ в течение 5 рабочих дней. В свою очередь, владельцы объектов информатизации каждые два года обязаны направлять информацию о проведённых контролях эффективности. Это значит, что теперь ФСТЭК России получает данные по каждому аттестованному объекту информатизации и контролирует его.

Наконец, одно из самых главных изменений, продиктованных новым Приказом, заключается в том, что ФСТЭК России может приостанавливать и даже отменять действие аттестатов на основании экспертной проверки предоставленных документов или факта непредоставления необходимой документации.

Многие из эксплуатантов объектов информатизации являются лицензиатами ФСТЭК России по разным направлениям деятельности: монтаж или разработка средств защиты информации, аттестация, проведение контролей и так далее. Чтобы соответствовать требованиям положений по лицензированию, у таких организаций должны быть защищаемые помещения для ведения конфиденциальных переговоров.

Если компания-лицензиат не предоставляет данные или проводимая аттестация не соответствует требованиям регулятора, что приводит к приостановке аттестата соответствия, то ФСТЭК России, опираясь на актуальные данные из реестра, может

санкционировать более тщательную и детальную проверку на соответствие лицензионным требованиям.

К тому же теперь каждые два года объект информатизации обязан направлять отчёт во ФСТЭК России об осуществлении периодического контроля».

ЧТО ПРЕДЛАГАЕТ ЦИБИТ?

Евгения Колодина: «ЦИБИТ внимательно следит за всеми нововведениями. Мы оказываем только актуальные услуги, отвечающие запросам времени. Для удобства клиентов мы сформировали выгодное спецпредложение, учитывающее новые особенности в порядке организации и проведения аттестации объектов информатизации, продиктованные Приказом ФСТЭК России № 77.

Нами разработана многоступенчатая система скидок¹ в рамках комплексной услуги по сопровождению объектов информатизации, включающей все необходимые плановые мероприятия: аттестацию, ежегодные контроли эффективности, постоянную поддержку и консультирование.

ЦИБИТ предлагает заключить долгосрочный договор с фиксированными ценами сразу на несколько лет, в рамках которого специалисты проведут аттестацию и будут каждый год проводить периодический контроль объекта информатизации по выгодной цене. Кроме того, в случае заключения такого договора каждый 4-й периодический контроль эксперты Департамента аттестационных работ ГК «ЦИБИТ» сделают бесплатно».

¹ Предложение действует до 31.12.2021



ГРУППА КОМПАНИЙ
ЦИБИТ

КОНТАКТЫ

Телефон: +7 (495) 792-80-80

E-mail: info@cibit.ru

Сайт: www.cibit.ru



Дмитрий ЛАРИН
директор по разработке
продукта «Гарда БД»
в «Гарда Технологии»

ОТ МОСКВЫ ДО ВЛАДИВОСТОКА

ГЕОРАСПРЕДЕЛЕННАЯ СИСТЕМА ЗАЩИТЫ БАЗ ДАННЫХ

Базы данных компании — один из ключевых активов, требующих непрерывной защиты от несанкционированного доступа. И если компании с одним офисом могут организовать защиту СУБД штатными средствами, то для больших организаций, имеющих лаборатории и офисы в разных городах, задача становится нетривиальной. При масштабировании компании и открытии геораспределенных филиалов появляются дополнительные риски появления неучтенных копий баз данных, открытия неконтролируемых портов интеграции и ещё ряд проблем, связанных с возможностью внешнего вторжения в базы данных.

Чтобы предотвратить эти риски, контролировать доступ к данным во всех дата-центрах сети компании нужно централизованно. При централизованном контроле геораспределенной инфраструктуры служба безопасности

получает возможность видеть параметры и закономерности удалённых подключений в базы данных, что нивелирует риски нелегитимного доступа к конфиденциальной информации из других филиалов и помогает контролировать все дата-центры без постоянной передачи данных из одного в другой.

Именно поэтому в новой версии DAM-решение «Гарда БД» получило возможность наращивания геораспределенной архитектуры взамен кластеризации.

ОТ КЛАСТЕРНОГО МАСШТАБИРОВАНИЯ К ГЕОРАСПРЕДЕЛЕННОЙ ЗАЩИТЕ

При кластерном росте инфраструктуры защита баз данных может быть обеспечена без сетевых помех только внутри одного центра обработки данных. В таких условиях поступающие на обработку в систему хранения объекты не передаются между узлами и не нагружают

сеть. Но при построении системы контроля нескольких территориально распределённых дата-центров такой подход обретает целый ряд сложностей:

- ♦ Необходимо обеспечить максимально отзывчивую сеть для защиты данных в ЦОДах.

- ♦ При возникновении сбоя на сетевом мосту — комплекс становится недоступен для оператора.

- ♦ В итоге кластерная архитектура не подходит для компаний с большой инфраструктурой, разнесённой между разными городами (SOC).

Геораспределенная система пришла на смену кластерного решения и позволила решить задачу комплексного контроля всех дата-центров компании из главного центра управления и разграничить доступ к данным между ними, не нагружая сети.

ПРИНЦИП РАБОТЫ ГЕОРАСПРЕДЕЛЕННОГО РЕШЕНИЯ

Основной задачей новой архитектуры «Гарда БД» стало построение сети для перехвата и обработки данных из нескольких дата-центров с возможностью контроля с единого узла управления. Такое решение позволило объединить источники данных удалённых узлов хранения в единый информационный поток. Специалистам, отвечающим за безопасность данных, больше не нужно искать запросы в нескольких дата-центрах одновременно.

АПК «ГАРДА БД» ОТ «ГАРДА ТЕХНОЛОГИИ»

Аппаратно-программный комплекс класса DAM/DBF для безопасности СУБД и независимого аудита операций с базами данных и бизнес-приложениями. Ведёт непрерывный мониторинг обращений к базам данных и выявляет подозрительные операции в режиме реального времени.

- ♦ Защита от утечек хранящейся в БД информации.
- ♦ Контроль привилегированных пользователей.
- ♦ Аудит всех операций в БД и веб-приложениях в реальном времени.
- ♦ Выявление и предотвращение попыток внешнего вторжения.
- ♦ Блокирование нежелательных запросов к БД и веб-приложениям.

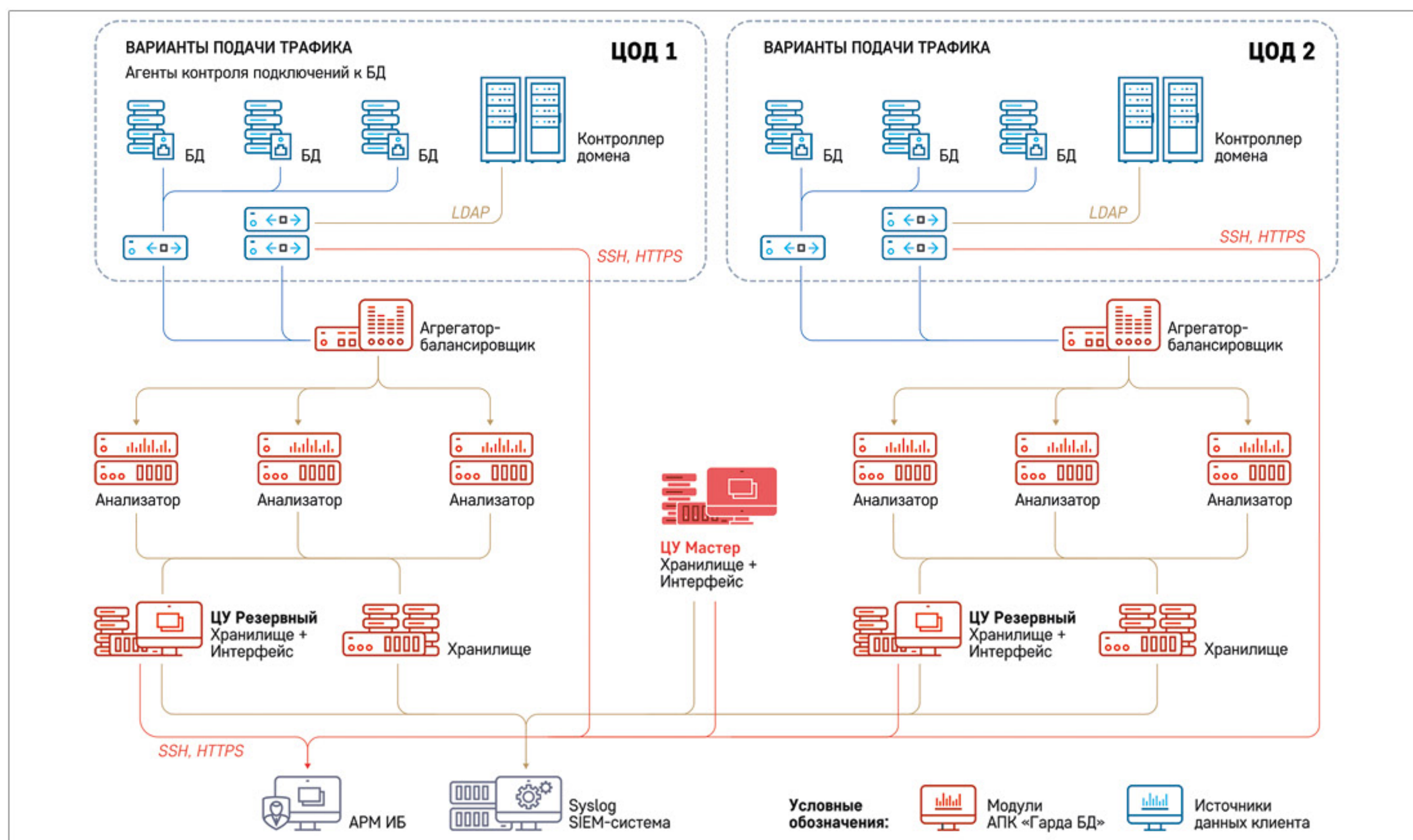


Рисунок 1. Работа геораспределенного решения на инфраструктуре, где одну и ту же задачу выполняют два или более идентичных ЦОД (основной и резервный)

Рассмотрим, как работает геораспределенное решение на инфраструктуре, где одну и ту же задачу — оплата покупок и банковские операции — выполняют два или более идентичных ЦОД (основной и резервный). Если в классической системе работа сотрудников будет затруднена наличием нескольких пультов управления в каждом дата-центре, то при внедрении геораспределенной системы запросы потребителей будут равномерно распределяться между узлами (рис. 1).

Геораспределенное решение даёт ряд преимуществ по сравнению с традиционным:

- ♦ Поискные запросы можно выполнять из единого центра управления без учёта расположения хранилищ и оператора.
- ♦ Выход из строя сетевого моста между узлами не приводит к полной неработоспособности пульта управления (временно будут доступны данные только с подключённых узлов).
- ♦ Ускорение выполнения поисковых запросов, так как нет необходимости подгрузки данных на центральный узел, — данные моментально выводятся оператору.

- ♦ Повышение надёжности работы узлов в период пиковой нагрузки за счёт минимальной сетевой связанности.

Геораспределенная система защиты баз данных «Гарда БД» построена на работе механизма Cross-cluster search. То есть, узлы хранения не связаны единой экосистемой, а поиск осуществляется благодаря агрегатору поисковых запросов. Такое архитектурное решение позволяет снизить нагрузку на управляющий узел во время индексации поисковых данных внутри комплекса. Настройки перехвата данных по всем дата-центрам хранятся в базе PostgreSQL. Их резервирование происходит на уровне узла благодаря предусмотренному RAID-массиву, что обеспечивает работу комплекса даже в случае выхода из строя управляющего узла дата-центра.

ПРАКТИКА ПРИМЕНЕНИЯ ГЕОРАСПРЕДЕЛЕННОЙ ЗАЩИТЫ АПК «ГАРДА БД»

В крупной банковской сети дата-центры расположены в разных городах — в Москве и во Владивостоке. Ранее

доступ к базам данных филиалов без передачи данных с сервера на сервер можно было контролировать только локально — внутри дата-центра. При условии, что передача данных с сервера на сервер между городами осложнена высокой нагрузкой на сеть — остро встал вопрос геораспределенного доступа без загрузки данных филиалов в головной ЦОД. Внедрение геораспределенного решения защиты баз данных «Гарда БД» позволило без увеличения нагрузки на сервер обеспечить контроль доступа ко всем базам данных всех дата-центров компании, а, в случае сбоя одного из них, — восстановить данные без их потери.

Геораспределенная защита баз данных «Гарда БД» помогает автоматизировать и централизовать контроль доступа к базам данных внутри дата-центров вне зависимости от их месторасположения. Это позволяет значительно оптимизировать работу служб информационной безопасности.



Михаил ИВАНОВ
генеральный директор
ООО «С-Терра СиЭсПи»

«С-ТЕРРА СИЭСПИ»: СДЕЛАНО В РОССИИ

ШИФРОВАНИЕ ДЛЯ ЦОД И НЕ ТОЛЬКО

Любому бизнесу важно обеспечить высокую доступность сервисов, непрерывность и безопасность бизнес-процессов. А в условиях нынешней экономической и политической ситуации в стране и в мире, не теряет своей важности ещё и тема импортозамещения.

ИМПОРТОЗАМЕЩЕНИЕ — ЭТО НЕ ТЕХНОЛОГИЧЕСКАЯ ИЗОЛЯЦИЯ

В ИБ-отрасли продукция российского производства почти вытеснила иностранное ПО и постепенно приходит на смену зарубежному оборудованию, то есть аппаратные устройства тоже всё чаще используются отечественные. Мы в компании «С-Терра СиЭсПи» придерживаемся мнения, что импортозамещение — это не технологическая изоляция, и для безболезненного перехода на «всё российское» не стоит отказываться от лучших мировых практик, а нужно адаптировать их под наш рынок. Именно этим мы руководствуемся,

используя в архитектуре решений С-Терра проверенные мировые технологии (стек протоколов IKE/IPsec) в сочетании с российскими современными ГОСТ криптоалгоритмами. По сути, мы помогаем российскому бизнесу плавно перейти на отечественные системы защиты информационной инфраструктуры.

ТОРП, КИИ, ЕПТ... И ДРУГИЕ ИНТЕРЕСНЫЕ АББРЕВИАТУРЫ

VPN-решения С-Терра обеспечивают конфиденциальность и целостность передаваемых данных за счёт шифрования на российских криптоалгоритмах. Тем самым нивелируется риск перехвата или изменения информации при передаче её по открытым каналам, и при этом обеспечивается выполнение требований регуляторов в сфере информационной безопасности.

Для бизнеса сертификация и нахождение в реестрах — это соответствие

требованиям нормативных документов. Для нас же — это подтверждение, что решения С-Терра обеспечивают надёжную защиту информации, и, конечно, возможность применения их в финансовых организациях, государственных органах, на предприятиях, входящих в число субъектов КИИ и т.д. Кроме того, это позволяет компании «С-Терра СиЭсПи» уверенно чувствовать себя на российском рынке информационной безопасности.

Поэтому продукты С-Терра сертифицированы ФСБ России и ФСТЭК России, входят в Единый реестр российских программ для ЭВМ и БД (реестр Минцифры). Мы взаимодействуем с отечественными производителями аппаратных платформ, ведём работу по включению своих устройств в реестр Минпромторга России (радиоэлектронного оборудования, ТОРП). Компания «С-Терра СиЭсПи» — один из трёх вендоров, чьё оборудование рекомендовано для защиты подключения к системе межведомственного электронного взаимодействия РФ (СМЭВ РФ), к Информационной Системе «Единый портал тестирования в области промышленной безопасности, безопасности гидротехнических сооружений, безопасности в сфере электроэнергетики» (ИС ЕПТ).

Таким образом, решения С-Терра обеспечивают безопасность информации

Для бизнеса сертификация и нахождение в реестрах — это соответствие требованиям нормативных документов. Для нас же — это подтверждение, что решения С-Терра обеспечивают надёжную защиту информации

в ключевых процессах цифровизации различных областей российского народного хозяйства.

ЦОДЫ ПОД ЗАЩИТОЙ СКОРОСТНОГО ШИФРОВАНИЯ

Переход в цифровое пространство, рост количества информационных процессов в обществе и в бизнесе влечёт за собой увеличение хранимого и обрабатываемого объёма данных. Вслед за этим меняются и требования к каналам связи: увеличивается пропускная способность, повышается надёжность и дальность передачи информации.

Клиенты компании «С-Терра СиЭсПи» уже могут защищать российским шифрованием связь между ЦОД, магистральные и другие высокопроизводительные каналы. 10 Гбит/с, 25 Гбит/с, 40 Гбит/с — это вехи, по которым прослеживается путь развития высокопроизводительных решений С-Терра. До 50 Гбит/с на одном VPN-шлюзе — это уже реальность, и самое ближайшее будущее — защита с производительностью 100 Гбит/с на одном устройстве. Причём, на российской аппаратной платформе этот результат тоже достигим.

Больше того, мы первыми (совместно с РКЦ и Ростелекомом) продемонстрировали возможность высокоскоростного шифрования с применением технологии квантового распределения ключей (КРК) на действующей волоконно-оптической линии связи «Ростелеком». Сегодня все высокоскоростные VPN-шлюзы С-Терра Шлюз DP могут поддерживать эту технологию.

НЕ ЦОДОМ ЕДИНЫМ... МАЛЕНЬКИЕ ТОЖЕ В ЦЕНЕ

Но не только ЦОДы и мощные средства защиты стремительно развиваются. В последние два года рынок ИБ оказался, можно сказать, на передовой в современном мире, с его «удалёнкой», баталиями в информационном пространстве и выросшей интенсивностью киберпреступлений. И самый миниатюрный в России VPN-шлюз С-Терра Юнит оказался на пике актуальности.

С его помощью организованы защищённые удалённые подключения тысяч сотрудников российских компаний,

С-Терра Шлюз DP — линейка криптошлюзов, специально предназначенных для защиты высокопроизводительных каналов связи. В С-Терра Шлюз 10G/25G/40G реализовано шифрование L2-трафика, но сохраняется возможность работы по L3-каналам связи.

Реализация отказоустойчивых схем подключения позволяет обеспечить бесперебойную работу системы даже при сбое одного из устройств или канала связи.

Яркий пример применения высокопроизводительных шлюзов С-Терра — реализация проекта по защите оверлейной сети между тремя ЦОДами. Это нестандартная задача, поскольку С-Терра Шлюз DP предназначен для работы в схеме «точка-точка». Здесь же понадобилось организовать «треугольник» из

VPN-шлюзов, причём пропускная способность канала по каждой стороне этого «треугольника» составляла 20 Гбит/с.

Специалисты компании «С-Терра СиЭсПи» нашли изящное и рациональное решение, использовав три шлюза С-Терра Шлюз 40G, доукомплектованных необходимыми интерфейсами. Оверлейная сеть обеспечила взаимодействие ЦОДов в режиме «каждый-с-каждым» (простейший пример такой сети — GRE туннели). При этом каждый VPN-шлюз С-Терра обеспечил защиту сразу двух каналов 20 Гбит/с.

Это решение позволило надёжно и эффективно защитить каналы связи между тремя ЦОДами, при этом сэкономив средства заказчика и обеспечив оптимальную загрузку оборудования.

проводятся конфиденциальные переговоры по видеоконференцсвязи и IP-телефонии, происходит обмен данными с персональными мобильными устройствами, защищаются интерфейсы управления серверами и платформами (iLO, CIMC, IPMI).

С-Терра Юнит оказался очень востребован на рынке, но мы не останавливаемся на достигнутом, и продолжаем его совершенствовать. Уже сейчас мы готовим бескорпусную модификацию, которая позволит ещё эргономичнее встраивать криптошлюз в банкоматы и IP-видеокамеры, использовать его в измерительных и контрольных устройствах системы ЖКХ.

В БУДУЩЕЕ — С УВЕРЕННОСТЬЮ В УСПЕХЕ

Каждый день приносит нам новые вызовы, новые задачи, требует концентрации сил и принятия оперативных и, порой, нестандартных, решений. Мир меняется, всё больше погружается в цифровое и виртуальное пространство. Ещё недавно мы утверждали, что периметра больше нет. Но размытый, вроде бы, периметр всё-таки до сих пор сохраняет довольно определённый контур, который требует защиты,

причём с соблюдением национального суверенитета.

Компания «С-Терра СиЭсПи» непрерывно развивается, почти два десятилетия занимая прочные позиции в тройке лидеров российского рынка средств защиты информации. По итогам 2020 года выручка компании выросла в 2 раза, мы увеличили темпы производства, стали ещё быстрее и эффективнее реагировать на запросы клиентов, стараемся чутко прислушиваться к рынку и опережать его потребности.

В октябре 2021 года компания стала резидентом ОЭЗ «Технополис Москва», расположившись в помещениях на площадке «Алабушево». Это знаковое для нас событие, накладывающее некоторые обязательства, но, учитывая налоговые и таможенные льготы, удобную инфраструктуру и логистику ОЭЗ, дающее дополнительные возможности для увеличения производственных мощностей, создания новых рабочих мест, реализации новых проектов.

В будущее мы смотрим с уверенностью в успехе. И главное — мы продолжаем создавать функциональные, удобные и производительные решения для защиты информации российских предприятий и организаций.



Владимир УЛЬЯНОВ
руководитель аналитического
центра Zecurion

ДСАР, КАП, КАП

НЕОТЪЕМЛЕМЫЙ КОМПОНЕНТ DLP ДЛЯ БОРЬБЫ С УТЕЧКОЙ ИНФОРМАЦИИ

ДСАР — достаточно молодой класс продуктов в области корпоративной безопасности, который не очень хорошо знаком потребителям, а эксперты до сих пор спорят о терминах и не могут сойтись даже на перечне решаемых задач. При этом ДСАР часто отводится роль компонента DLP. В данной статье оценим применимость таких систем для предотвращения утечки информации, разберём другие возможности и попытаемся очертить профиль их использования.

ТОЛЬКО ДЛЯ ДЖЕНТЕЛЬМЕНОВ

Обнаружение, категоризация и защита конфиденциальных данных часто фигурируют в списке основных задач ДСАР. Кажется, это обособленный и законченный процесс. Но стоит сразу разрушить иллюзии, ДСАР — это не защита от утечек, а лишь дополнение к ней. Использование ДСАР автономно, в качестве DLP оно будет сродни воротам в поле — красиво, но легко обходится, стоит лишь сойти с дорожки (рис. 1). В то же время глупо отрицать пользу



Рисунок 1. Джентльмен в обход не пойдёт

ДСАР, ведь в грамотно построенном решении этот продукт может взять на себя роль системы раннего оповещения и даже предотвращения угроз. С фокусом на данных (Data Centric) и связанных с ними событиями и сущностями.

ПРИЧИНЫ ДОЛГОЙ ЮНОСТИ

Дата-центричная модель защиты существует уже не один десяток лет, но сегмент ДСАР молод и слабо распространён. В чём кроется причина? Наверное, в основном это возможность решать задачи ДСАР другими инструментами и отсутствие остроты проблемы. Тем более здесь специалист может продемонстрировать свои компетенции (настроить права доступа на папки) и сэкономить деньги компании. Информация уже хранится и люди с ней как-то работают. По факту же получается, что такая экономия оказывается сомнительной. Файловые хранилища всё более разрастаются, структура папок усложняется, появляются всё новые и новые копии тех же файлов, количество версий превосходит все разумные рамки, поиск нужного файла становится нерешаемой проблемой (проще сделать документ с нуля), актуализация вообще никак не происходит. И это только верхушка айсберга, ведь обеспечить безопасность подобной файловой помойки представляется затруднительным. Избыточные копии и права доступа, нелогичные места хранения ещё более усложняют дело.

Другими причинами пренебрежения ДСАР могут быть недостатки самих продуктов. Это тоже можно объяснить

в условиях, когда рынок ещё не сформировался, и подходы к разработке продуктов, их архитектуре и особенностям работы и у разных вендоров сильно отличаются. Например, гибридная модель работы, когда в продукте есть и сетевой компонент, и агент — скорее исключение. Хотя именно такой подход даёт лучший результат и контроль над данными в отличие от установки исключительно сетевого или только локального модулей.

КАТАЛИЗАТОР СИНЕРГИИ

Следующий этап — это взаимодействие с остальными компонентами корпоративной безопасности. Чаще всего продуктам ДСАР приходится работать в связке с DLP и SIEM — это ближайшие союзники. В свою очередь полезными для ДСАР являются IRP и UBA/UEBA-системы. IRP в виде отдельного продукта либо как функциональность, встроенная в ДСАР, помогает управлять системой и координировать деятельность ответственных сотрудников, что особенно актуально для крупных компаний. Впрочем, даже единственный сотрудник находит применение IRP в качестве встроенного планировщика задач для себя самого. UBA, хотя и не является обязательным компонентом, предоставляет данные для анализа закономерностей и профилей поведения. Синергетический эффект такой связи позволяет прогнозировать и выявлять сложные угрозы, то, что недоступно другим системам или не отслеживается политиками, основанными на стандартных условиях можно/нельзя (рис. 2).

О ВРОЖДЁННОЙ ИНТЕГРАЦИИ

DCAP — это вообще не про статичную картину в моменте. Будучи компонентом DLP, система позволяет выявлять неочевидные связи между сотрудниками, которые выстраиваются не напрямую, а через файлы. Более того, таким образом можно отследить пути появления, точки изменений, всю историю файлов, что одинаково полезно при расследовании прошлых инцидентов и прогнозировании рисков, выявлении сложных схем мошенничества, распространившихся с момента начала пандемии, когда люди почувствовали неуверенность в завтрашнем дне. Поэтому важен двусторонний обмен данными между DCAP и DLP, обогащение информации, собираемой сенсорами каждой из систем. На практике такой обмен расширит горизонт применения связки, даст возможность детектировать новые типы угроз, настраивать новые виды реакций. А с точки зрения управления — это единые политики, упрощение настройки и эксплуатации, бесшовная защита. Всё это указывает на необходимость врождённой, а не приобретённой интеграции между компонентами единой системы.

Следующий шаг — интеграция DCAP и DLP в рамках одной платформы. Это позволит исключить избыточность и использовать общие ресурсы. DLP уже обладает набором технологий контентного анализа, включая морфологию, шаблоны, цифровые отпечатки, метод опорных векторов и многие другие. Соответственно, DCAP может использовать эти технологии для симметричной категоризации файлов.

ВИРТУОЗ В РАБОТЕ С ДАННЫМИ

Возвращаясь к возможностям самого DCAP, продукт по своей сути должен быть наглядным. Ведь он не изменяет данные, не создаёт новых, не меняет структуру хранения и является только надстройкой над данными. Суть задачи — упростить работу с данными, поэтому и сам он должен быть простым и наглядным. Как в автомобиле, вместо того, чтобы прилагать усилие напрямую к рычагам, проще воспользоваться рулём, не рассчитывая

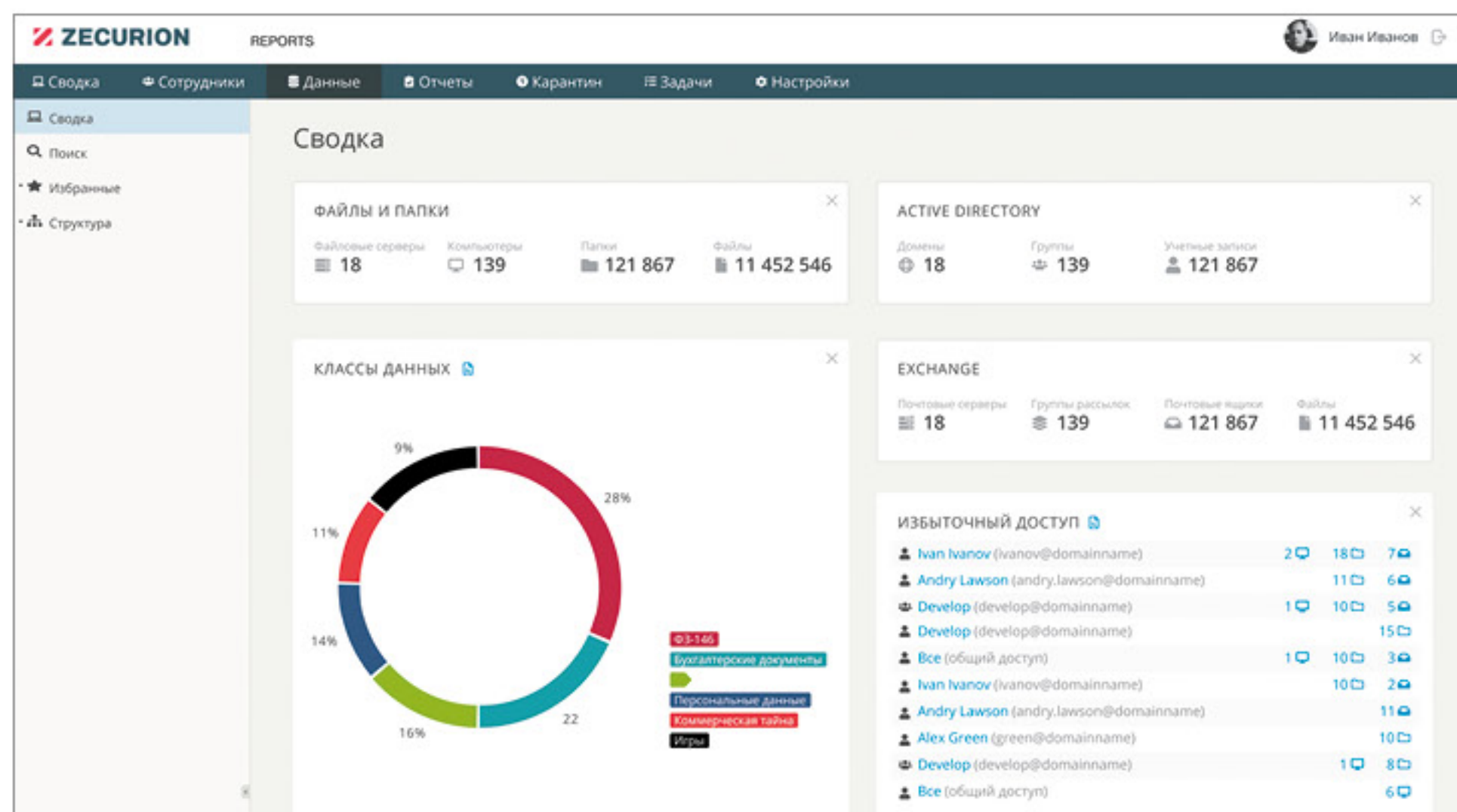


Рисунок 2. DCAP обладает наибольшей ценностью, являясь компонентом DLP

нужные вектор и силу. В этом контексте DCAP в одном окне показывает структуру и классы данных, в том числе из разных источников/силосов сразу, как файлов, так и почтовых и AD-объектов. При этом подсвечивает нарушения прав, избыточные или неиспользуемые, фактических владельцев данных, действия с объектами. В обязательном порядке — дашборды для оценки текущей ситуации и отслеживания изменений, а также отчёты, в том числе в режиме онлайн, графики, статистика и... снова приходим к профилированию UBA и обогащению данных из других источников.

ОБ ИСПОЛЬЗОВАНИИ

После того как мы очертили контуры функциональности DCAP, обратим внимание на практику использования. Сегодня необходимым набором является поддержка Windows, Linux, Exchange, Active Directory — это база. Endpoint-агенты, адекватные enterprise-архитектуре заказчика, с централизованной установкой и способные работать самостоятельно в самых больших масштабах, ведь enterprise — это не тысячи, а десятки тысяч рабочих мест. Ну и, конечно, разумная защита от админа, исключая злоупотребление служебным положением, тоже должна быть реализована.

ПОДВЕДЁМ ИТОГИ

DCAP почти всегда — это работа с большими объёмами данных, поэтому даже в небольших компаниях требования не

сильно отличаются от enterprise. При этом само решение должно быть понятным и удобным, полнофункциональным уже из коробки для того, чтобы справиться с анархией данных, которая часто встречается в реальных компаниях. DCAP выявляет риски избыточного, некорректного и неактуального доступа и даёт возможность эффективно управлять правами с минимальными трудозатратами. А параллельно предоставляет полезную информацию для защиты от других внутренних угроз.

DCAP — это полезный модуль DLP. Синергия совместного использования продуктов двух классов позволяет находить новые угрозы и собирать более полные отчёты и досье. А технологии контентного анализа, скорее всего, в DLP развиты даже лучше. В случае если DLP и DCAP поставляются одним вендором, это упрощает работу со связкой, унифицирует политики безопасности и отчёты, экономит ресурсы на внедрение и интеграцию, а самое главное — даёт больше сценариев для выявления корпоративных угроз.

При использовании DCAP без DLP теряется львиная доля смысла, особенно в части защиты от утечки. Причём этот симбиоз полезен и для DLP, поэтому DLP-вендоры сейчас активно развивают функциональность в своих продуктах, и именно эти решения будут доминировать на рынке в ближайшие годы.



Александр ГАЛИЦКИЙ
соучредитель компании
ЭЛВИС-ПЛЮС

ЭЛВИС-ПЛЮС — 30 ЛЕТ!

НА ВОПРОСЫ BIS JOURNAL ОТВЕЧАЕТ СОУЧРЕДИТЕЛЬ
КОМПАНИИ АЛЕКСАНДР ГАЛИЦКИЙ

— Александр Владимирович, поздравляем Вас с юбилеем компании ЭЛВИС-ПЛЮС, желаем и Вам, и компании крепкого здоровья, активного долголетия, верных друзей и надёжных партнёров. Расскажите, пожалуйста, как всё начиналось.

— Всё начиналось очень просто. Наивность 90-х годов, когда ты ещё не знаешь, что будет впереди, развал Советского Союза, большие компании преобразуются непонятно во что. И я, достаточно молодой человек, отвечающий за большой блок вопросов оборонной промышленности, относящейся к космосу, который должен принимать решения...

В 1990-м я был Главным конструктором уникального предприятия НПО ЭЛАС, лидера в области специальных электронных систем для космических оборонных систем СССР. Экономика перестала складываться. Наш Генеральный конструктор Г. Я. Гуськов поддерживал реорганизацию четырёх головных направлений, и моё отделение — комплекс 9 (ОК-9) — было преобразовано в научно-производственный центр ЭЛВИС (Электронные Вычислительные и Информационные Системы). Мы пытались сохранить весь объём работ отделения комплекса. Я руководил НПЦ ЭЛВИС достаточно долго, и даже после прекращения деятельности НПО ЭЛАС, но потом передал компанию своему заместителю Олегу Тимофееву, а позже компанию возглавил Ярослав Петричкович, который смог сохранить часть направлений и заказчиков ОК-9. Ярослав, как руководитель отдела по

разработке элементной базы в ОК-9, смог сохранить и развить именно направление по разработке микроэлектронной элементной базы. Этим и известен НПЦ ЭЛВИС сегодня.

Компания прошла путь от подразделения славного НПО ЭЛАС, государственного унитарного предприятия, до частной компании, являющейся лидером российского микропроцессорного рынка. Как бы там ни было, я не имею отношения к сегодняшнему НПЦ ЭЛВИС с конца 90-х годов. Я благодарен Г. Я. Гуськову и О. А. Тимофееву, что, увидев моё разочарование в государственном направлении, они дали мне возможность сконцентрироваться на частном бизнесе.

Именно 1990 год стал определяющим. Образовался НПЦ ЭЛВИС, нам разрешили встречаться с иностранцами, и в октябре 1990-го в Москве состоялась наша встреча с Биллом Джоем, сооснователем легендарной компании того времени (как Google середины 2000-х) Sun Microsystems. Эта встреча поменяла мою жизнь, а через год дала жизнь компании ЭЛВИС-ПЛЮС. За год произошло много событий: в жизни страны, НПО ЭЛАС, моей и ведомого мною коллектива инженеров. Я побывал несколько раз в США, в Кремниевой долине, мы пытались реанимировать проект низкоорбитальной спутниковой связи «Курьер», отказались от переезда в США после августовского путча...

Представители Sun Microsystems были так впечатлены нашими достижениями, что в сентябре 1991-го прислали мне на

личный адрес 20 SPARC-станций стоимостью 20–30 тыс. долларов каждая. Принять технику на баланс НПО ЭЛАС или НПЦ ЭЛВИС не позволяло законодательство, и непонятно было, что со всем этим делать.

Один из моих сотрудников посоветовал: а что, стартани компанию! И мы стартанули. Условия для старта у нас, действительно, были очень неплохие: специалисты экстра-класса, современная вычислительная техника и крупные заказы от Sun Microsystems...

— А как компания стала заниматься информационной безопасностью?

— Ну, к информационной безопасности мы пришли позже. Сначала было то, что сейчас называется Wi-Fi. Дело в том, что ещё в 1990-м году, когда представители Sun Microsystems впервые приехали в Россию, они увидели, как мы через космос качаем IP-протокол. Это их впечатлило, так как интернета ещё как такового не было. И позже, в декабре 1991-го, они спросили: можете ли вы сделать такую плату, которая позволит компьютерам коммуницировать между собой по протоколу 802.11.

Мы лихо за это взялись и в октябре 1992-го показали прототип. В марте 1993-го мы стали первой компанией, в которую Sun впервые в своей истории проинвестировала деньги, а в октябре 1993-го, влив в стандарт PCMCIA радио- и цифровую часть, выиграли соревнование у Motorola, и даже показали свой продукт на выставке INTEROP в Париже — 12 компьютеров, работающих в одной локальной

сети. Это произвело шок и движение вокруг этой темы. Но мы тогда были очень наивными и не понимали, как запустить все наши достижения в массовое производство.

Не хочу вспоминать, как я ходил по министерствам, что-то доказывал, и в итоге пришёл к выводу, что заниматься железом в российских условиях невозможно. Руководство Sun предложило эту тему компании Ericsson — самой продвинутой в то время компании в области цифровой связи. Но в Ericsson тоже не понимали, зачем нужна связь по радио со скоростью выше ста килобит в секунду. Тогда ведь передавалась только текстовая информация, и никто не предполагал, что будет видео, графика и многие другие вещи.

Тем не менее мы получили от Sun Microsystems инвестиции, об этом было объявлено с помпой в Долине, и мы получили большую известность. Собственно, это и был наш первый успех. Но это был, я бы сказал, пока ещё чисто инженерный успех.

А потом мы начали смотреть, что можно делать в софте. Мы поняли, что интернет движется вперёд, тогда уже начали говорить, что виртуальные сети — это единственная защищённая тема, с которой можно работать. А компания Sun Microsystems в 1995 году продвигала интернет в бизнес и интернет-протокол как систему для бизнес-коммуникаций, но она не могла реализовать свой VPN на протоколах SKIP и IPsec для Windows-среды.

Наша команда смогла напрямую взломать драйверы компании Microsoft (к слову, потом это позволило мне привлечь внимание Билла Гейтса), что было признано большой победой, так как, например, в Sun долго пытались, но у них не получалось. И в 1996 году мне позвонил Эрик Шмидт, в то время СТО компании Sun Microsystems, и сказал: «А давайте-ка мы у вас купим ваши продукты и технологии». И мы подписали соглашение. По сути, так в мире и появился первый Windows VPN-клиент под торговой маркой SunScreen E+. Это был второй большой успех, и это была чисто российская разработка. Она наделала много шума как в технологическом, так и в политическом мире в 1997 году.

Наша команда смогла напрямую взломать драйверы компании Microsoft. И это было большой победой, потому что, например, в Sun долго пытались, но у них не получалось

— Можете ли Вы представить историю ЭЛВИС-ПЛЮС через периодизацию? Какими этапами компания пришла к своему 30-летию? Это тем более интересно, что её история — это часть истории отечественной и мировой IT-индустрии. И, конечно, отечественной информационной безопасности.

— Знаете, этапы очень разные. В последние 10–15 лет жизнь заметно изменилась. Молодёжь начала жить международной жизнью, путешествовать, смотреть. Реальным ресурсом знаний, частью жизни, стал интернет. А в 90-е мы были очень наивными, мало кто знал, что такое электронная почта или венчурный бизнес. Я, например, был уверен, что венчурные капиталисты — это просто-напросто спекулянты...

Тогда я считал, что зазорно бегать и продавать что-то, надо разрабатывать инженерные идеи. Я гордился нашими инженерными достижениями, и только столкнувшись с реальным миром бизнеса, и то не сразу, понял, что инженерное решение — это всего лишь 25 процентов человеческих и финансовых затрат. А превращение этого решения в продукт, вывод его на рынок — это ещё 75 процентов.

Поэтому, если говорить об этапах, сначала у нас был чисто инженерный этап. Период восторга от самих себя, когда мы совершали прорывы в мировых технологических направлениях. Сначала в области радио, потом в области VPN. Казалось, нам всё подвластно. Мы интересовались множеством технологий. Например, ещё до появления в Microsoft Office возможности передавать факс-сообщения через интернет, мы сделали в 1993 году свой факс-гейт, и, помню, гоняли из Москвы за рубеж и по России туда-сюда срочные контракты для балерин из Перми, так как иначе они не могли вести дела с зарубежными партнёрами. Отсюда, кстати, родилась компания ЭЛВИС-ТЕЛЕКОМ.

Мы сделали первый профессиональный веб-сервер. Была такая компания

ИнфоАрт в далёком 1995–96 году — первый провайдер новостей, и мы полностью построили её цифровую среду. Для меня всё это было отдушиной после ночных воспоминаний о моих масштабных космических проектах, которые я оставил навсегда, а в душе продолжал ими жить. В 1998 году я создал за пределами России свою первую компанию TrustWorks Systems, и началась моя постоянная международная бизнес-жизнь.

Хотя она была и раньше, но было по-другому. Например, в 1996 году Скотт Макнили познакомил меня (я был в офисе Sun в то время по своим делам) с делегацией российского Центробанка. Они приехали в США и обратились за оказанием помощи и консультацией в области телекоммуникаций через интернет, UNIX-серверов Sun и операционной системы Солярис. Скотт позвал меня и сказал: у вас под боком работают лучшие специалисты в этой сфере. Таким образом мы начали работать с Центробанком. А в 1996 году мы выиграли тендер на 30 млн долларов по созданию для ЦБ телекоммуникационной системы.

Так у нас появилось новое направление — системная интеграция. Проекты в области коммуникаций, UNIX-среды и безопасности. Совместно с компанией Jet Infosystems мы написали для ФСТЭК России стандарты на сетевые экраны и т.д. С этого начался системно-интеграционный этап с постепенным уходом всё больше в безопасность.

— Какие наиболее яркие эпизоды из истории компании Вам запомнились?

— Часть я уже назвал: история прототипа того, что потом назвали Wi-Fi, VPN-овская история, проект с Центробанком... После 1998 года я уже занялся другими компаниями, но ЭЛВИС-ПЛЮС продолжает радовать яркими проектами. Пару лет назад создали для ЕГР ЗАГС РФ систему VDI, что было непросто, т.к. загсовская информация — материя весьма тонкая. Приятно удивляют проекты, которые

компания ведёт в Центробанке, ФНС России. Недавно Ростелеком стал участником в ЭЛВИС-ПЛЮС. Надеюсь, это станет стимулом к новым, масштабным свершениям.

— **Кем Вы особенно гордитесь в компании за всю её историю?**

— Мне повезло работать с талантливыми и хорошими людьми. Если вспомнить Wi-Fi, то это Алексей Сухов, Саша Охотников, Валера Купличенко, Виктор Кондратьев... В VPN-овской истории — тот же Алексей Вопилов, он сегодня трудится в Microsoft, Канат Алимжанов — тот самый человек, который взломал эти NDIS-драйверы, Валера Смыслов и Саша Гаврилов, склеивший всё вместе... Ещё и Коля Царёв, соучредитель ЭЛВИС-ПЛЮС, он очень серьёзно продвинул файервольную историю... Благодаря этим людям инженерная часть нам очень удалась.

Конечно, не могу не вспомнить Сергея Рябко, который потом создал компанию С-Терра, Алексея Лесных, Марка Кошелева, Олега Вернера, Андрея Архипова, с которыми мы строили уже TrustWorks Systems. Были люди, которые могли подхватить и вести всё дело: Саша Соколов, Виктор Басин, Максим Филиппов, который сегодня трудится в Позитив Текнолоджиз. Не могу перечислить всех, их очень много, но я всегда вспоминаю их всех: как мы решали проблемы, выходили из тупиков, что-то придумывали... Сегодня компания держится на том же Юрии Ивашкове, Сергее Панове... Я всегда вспоминаю Валеру Смыслова — он написал множество международных протоколов, был соавтором протоколов по квантовой безопасности... Много имён, людей, которые эту компанию поднимали, держат и продвигают.

— **Вы, пожалуй, один из немногих, кто представляет себе реальную картину отечественной IT-индустрии, её масштаб. В связи с этим три вопроса: что это за картина? Хотя бы эскиз. Как она выглядит на международном фоне? Какое место в этой картине занимает ЭЛВИС-ПЛЮС?**

— Начну с ЭЛВИСа. Когда-то, году в 1998, вышла статья «Технологический бутик Александра Галицкого». Бутик

в том смысле, что в нашей команде — классные специалисты, которые могут выполнить любой заказ красиво и на высшем уровне. Да, сегодня ЭЛВИС-ПЛЮС не так заметна на мировом рынке, как в 90-е — начале 2000-х. Сегодня это такая бутиковая компания в области безопасности для российского рынка. Её уважают, с ней считаются, но ситуация уже совсем другая. И эта ситуация характеризует рынок в целом.

К сожалению, многие российские ресурсы не были использованы, и мы так и не перешагнули черту, не вышли на большой международный рынок. Его опробует Яндекс, какие-то другие компании, но это не значит, что Россия вышла на мировые просторы широким фронтом, как могла бы. Сегодня вопрос «что считать российской компанией?» весьма запутан. По юридическим и другим причинам многие замечательные российские проекты реализуются и оседают в виде компаний... за пределами Российской Федерации. Российские это компании или кипрские, ирландские и т.д.? Но это только часть проблемы, причём проблема эта не исключительно российская, она характерна и для других стран. И дело в том, что в мире сегодня всего два больших рынка, куда все стремятся, — это США и Китай, где потребление инноваций поставлено на конвейер.

Можно долго объяснять, почему российская IT-индустрия характеризуется всплесками, почему её проекты и специалисты уходят за рубеж, но факт остаётся фактом: мы не нашли своего пути. Есть хорошие команды, есть даже понимание рыночных задач, но оглядка на госкомпанию сильнее: какой заказ нам дадут, не обойдут ли нас?

Положение у нас простое: Россия — это всего 2–3% от мирового IT-рынка. И главный вопрос: куда мы можем устремиться со своим потенциалом, не расплёскивая его и сохраняя свои корни? Оставаясь калининградскими, екатеринбургскими или московскими компаниями.

Российским айтишникам нужен большой рынок. Но, чтобы на него выйти, наша позиция должна быть проста и понятна. Мы говорим, что будем использовать у себя только отечественное, а Казахстану (это условный пример) предлагаем: используйте наше. Но

Казахстан — это тоже суверенное государство, и оно тоже может принять решение использовать только своё.

Выход на большой международный рынок, включая необходимость решать множество противоречий, — это, по-моему, сегодня основной вызов для российской инновационной индустрии. А ЭЛВИСу найти лидирующее место в этой истории уже довольно трудно, так как для этого нужны большие амбиции и ресурсы.

— **Какая ситуация с компанией ЭЛВИС-ПЛЮС на сегодня?**

— Недавно она стала партнёром Ростелекома. После подписания соглашения о продаже пакета акций ЭЛВИС-ПЛЮС Ростелекому обе компании выстраивают свои общие планы. ЭЛВИС-ПЛЮС занимается информационной безопасностью — своим традиционным бизнесом, в котором он преуспел и завоевал авторитет. Теперь надо ждать от компании только более амбициозных проектов. Я всегда любил ставить очень амбициозные цели, ну, надеюсь, что руководство компании тоже будет это делать.

— **Какие планы и перспективы у компании на ближайшие пять лет?**

— Этот вопрос скорее к менеджменту. Мне хотелось бы, чтобы ЭЛВИС обрёл новое дыхание, поднялся до новых высот. Насколько такие планы осуществимы, определяется как раз менеджментом компании, который день за днём ею управляет.

— **Можете дать футуристический прогноз, каким Вы видите мир и нашу страну через 30 лет?**

— Понятно, что многие профессии исчезнут. Механическую простую работу уже через 5–10 лет будут делать роботы. Это вопрос себестоимости: роботы совершенствуются и дешевеют с каждым днём. А через 30 лет мир перейдёт в состояние геймификации, по аналогии с компьютерными играми. Развитие технологий приведёт к тому, что множество операций мы будем совершать, не вставая с домашнего стула. Уже сегодня управление боевыми дронами и роботами по доставке интернет-заказов осуществляется не на поле



боя или в непосредственной близости от робота-курьера, а удалённо.

Но считать, что мы все переложим на роботов и искусственный интеллект, наивно. Кто-то должен будет принимать решения и нести ответственность за действие всех этих автоматов — автомобилей без водителей, самолётов без пилотов, больниц без врачей, столовых без поваров и т.д. Самой массовой профессией станет профессия оператора, по сути, компьютерного игрока. Сегодня именно такие игроки, просиживающие часами в виртуальной реальности, ближе всех к нашему будущему.

Какое место займёт в таком мире Россия? Думаю, целый пул возможностей ещё открыт. Когда-то я говорил, что мы всегда опаздываем на уходящий поезд. Надеюсь, на этот раз мы не опоздаем и впрыгнем в тот самый вагон, где идёт пересмотр и переформатирование мира. В частности, мира IT.

Хотя тревога не покидает. Наступает уже постклаудное время, а мы только пытаемся клауд у себя строить. В разгаре постклаудные отношения — по-

Считать, что мы все переложим на роботов и искусственный интеллект, наивно. Кто-то должен будет принимать решения и нести ответственность за действие всех этих автоматов

следние события с Facebook толкают мир в сторону, где очевидна необходимость новых структур для больших систем и больших облаков. Которые, скажем, разбираются на озёрца, динамически объединяющиеся в большие озёра, либо остаются маленькими, либо симметричными, либо ещё какими-то. И вопрос системной безопасности соответственно выходит на новый уровень. Например, сейчас интенсивно развивается интернет вещей, у нас много про это говорят, но куда это движется? Такое ощущение, что мы снова остаёмся в стороне, хотя, я знаю, многие российские предприятия об этом уже задумываются.

Движение идёт в мире, в разных странах. Сможем ли мы стать его участни-

ками, сможем ли выйти к миру с открытым забралом, сказать: вот наши законченные системные решения, вот мы открыты, у нас тут ничего внутри нет, что может вам навредить. Поверят ли нам, захотят? Это вызов времени. Если мы с ним справимся, через 30 лет мы окажемся в том мировом пространстве, в котором нам будет место, и мы не будем колонизированы каким-то определённым решением, транснациональной компанией или чужим государством. Потому что сегодня просто взять и закрыться в какой-то островок — невозможно. Это невозможно было и много лет назад, а сейчас тем более.

*Вопросы задавал
Игорь Некрасов*



РКИ-ФОРУМ РОССИЯ 2021

ЭЛЕКТРОННАЯ ПОДПИСЬ В ЭПОХУ ПЕРЕМЕН

В сентябре в Санкт-Петербурге состоялся «РКИ-Форум Россия 2021» — XIX международная конференция по проблематике инфраструктуры открытых ключей и электронной подписи. Участниками стали представители регуляторов, удостоверяющих центров, ИТ-разработчиков, научных учреждений, компаний — пользователей электронных подписей. Многочисленные изменения в отрасли, новые вопросы регулирования, современные технологии обсуждались в рамках тематических сессий, круглых столов, а также в неформальном общении во время деловой и неофициальной программ.

РКИ-Форум прошёл при поддержке Минцифры России, при участии Минэкономразвития, Минфина, ФНС России, Роскомнадзора, ФСО России и Казначейства России. Организатором мероприятия стала Медиа Группа «Авангард». Форуму оказали поддержку партнёры — «Газинформсервис»,

Avanpost, «АКТИВ», «КриптоПро», Infotecs, «Аладдин Р.Д.», Ассоциация «РОСЭУ». На Форум зарегистрировалось более 300 человек, многие выступления вызвали бурную полемику, свидетельствующую о живой заинтересованности участников отрасли в разрешении насущных вопросов РКИ.

РКИ ГЛАЗАМИ РЕГУЛЯТОРОВ

В начале мероприятия были зачитаны приветственные слова председателя Программного комитета РКИ-Форума, первого заместителя генерального директора — научного руководителя АО «НИИАС» Владимира Матюхина. За прошедший год произошёл ряд знаковых для отрасли событий. Российское законодательство в области ЭП, как и рынок РКИ в целом, находится в процессе глобальной реформы. Главными темами Форума спикер назвал машиночитаемые доверенности и документы о полномочиях, мобильные решения и облачную ЭП, доверенную третью сторону, длительное архивное хранение

документов с ЭП, новый статус доверенных лиц действующих аккредитованных УЦ.

Выступление директора правового Департамента Минцифры России Романа Кузнецова было посвящено вопросам практической реализации обновлённого 63-ФЗ. Речь шла о нюансах применения нового 476-ФЗ «О внесении изменений в Федеральный закон «Об электронной подписи»».

Представитель ФСБ России Александр Логачев продолжил тему изменений законодательства в связи со вступлением в силу 476-ФЗ. Так, новый закон расширил полномочия ФСБ в части установки ряда требований, определил методы идентификации заявителя при подаче заявления на создание сертификата, ввёл новый идентификатор заявителя и понятие доверенной третьей стороны. Ведомство отреагировало на изменения рядом нормативных документов. В настоящий момент ведётся разработка комплексного Приказа об облачной ЭП.



Выступление директора правового Департамента Минцифры России Романа Кузнецова

Александр Баранов, академик Академии криптографии Российской Федерации, рассказал о нюансах реализации проекта «Госключ». По его мнению, главная проблема кроется в удалённой идентификации клиента. Во многих случаях возрастает вероятность целенаправленного обмана с использованием электронной подписи. Андрей Корольков, начальник Научно-исследовательского центра Академии, посвятил свой доклад столетней годовщине Криптографической службы РФ.

Алексей Домрачев, представитель ФГУП «ГРЧЦ» (организации, подведомственной Роскомнадзору), акцентировал внимание на необходимости ухода от ручного труда и использовании современных средств (AI, ML) при анализе информационного пространства и мониторинге угроз безопасности. На этих принципах разрабатывается новая «Автоматизированная система прогнозирования рисков и угроз» Роскомнадзора.

Заместитель директора Департамента развития цифровой экономики Минэкономразвития России Алексей Минаев рассказал о проекте Федерального закона «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты РФ» в части регулирования вопросов конвертации электронных документов, их хране-



Выступление академика Академии криптографии Российской Федерации Александра Баранова

ния, создания электронных и/или материальных дубликатов документов. Законопроект призван обеспечить юридическую равнозначность документов в бумажной и электронной формах.

ОБ ОБНОВЛЁННОМ 63-ФЗ

Значительная часть обсуждений на PKI-Форуме была связана с реформой 63-ФЗ «Об электронной подписи». Так, из-за новых требований к удостоверяющим центрам количество этих учреждений в России снизилось в 20 раз: с 500 до примерно 25 (на настоящий момент). По словам заместителя генерального директора «Аладдин Р.Д.» Алексея Сабанова, успехом PKI в России можно назвать широкое применение КЭП в госорганах, на площадках спецоператоров, торговых площадках. Вместе с тем в развитии PKI ещё много проблем, которые можно разрешить только совместными усилиями экспертного сообщества.

Начальник отдела криптографической защиты АО «Гринатом» Николай Беленький посвятил доклад семантике отраслевых терминов. Он предложил участникам форума рассмотреть вопрос о приведении действующей терминологии в соответствие с реальными процессами хранения и передачи информации.

Елена Ткаченко, руководитель экспертного совета «Электронные документы — эффективная экономика»

ECR-RUS, отметила, что бизнес пока плохо готов соответствовать новым требованиям к электронному подписанию документов. Так, бизнесу необходимо видеть утверждённые нормативные акты и поправки к 63-ФЗ, чтобы на их основе выстраивать свою работу.

Ведущий эксперт по управлению документацией компании «ЭОС» Наталья Храмцовская перечислила основные проблемы и риски мошеннических действий на основе нововведений 63-ФЗ. Риски касаются как юридических, так и физических лиц. Например, для физлиц это могут быть оформление и использование подписи под угрозой увольнения, использование подписи без ведома физлица, попытки «присваивания» УКЭП лиц, ищущих работу.

Нина Соловяненко, старший научный сотрудник Института государства и права РАН, подняла тему прогнозируемой ответственности субъектов ЭДО и применимых юридических конструкций, сопровождающих Федеральный закон «Об электронной подписи».

Евгений Галкин, системный архитектор компании «Аванпост», указал на то, что на фоне популяризации онлайн-сервисов (e-commerce, дистанционные коммуникации, удалённая работа) повышается важность вопросов управления сертификатами информационных систем и сервисов. Подходы к управлению сертификатами рассма-



Круглый стол «Деятельность УЦ для участников обновлённой отрасли после завершения реформы 63-ФЗ: цели, прогнозы, экономическая целесообразность»

триваются как на технологическом, так и на бизнес-уровне.

Научный сотрудник Академии криптографии РФ Антон Гуселев совместно с заведующим лабораторией ПСОКиБИТ Академии Александром Бондаренко продемонстрировали механизмы контроля целостности и подтверждения авторства электронной цифровой подписи. Докладчики рассмотрели цифровую подпись с математической точки зрения.

ПРАКТИКА В НОВЫХ УСЛОВИЯХ

Убедиться в жизнеспособности организационных и технологических преобразований в отрасли электронной подписи можно только на практике, в рамках реализации различных проектов и инициатив. Так, Михаил Чеканов, директор по развитию АО «Промышленные Криптосистемы», раскрыл особенности машиночитаемых доверенностей

на примере платформы SmartFuel компании «Газпромнефть».

Заместитель директора НИИ «Восход» Андрей Пьянченко рассказал о следующих инициативах: о проектировании единого цифрового контура на основе усиленной электронной подписи, ЕСИА, биометрических технологий аутентификации; о готовящемся запуске в промышленную эксплуатацию Национального удостоверяющего центра; о разработке сервиса проверки неквалифицированных сертификатов для платформы «Госключ», а также о «цифровом» паспорте.

Алексей Ольшаников, руководитель группы доверенных сервисов АО «Гринатом», посвятил доклад практике создания платформы доверенных сервисов в госкорпорации «Росатом».

УЦ В НОВЫХ УСЛОВИЯХ

Участники круглого стола «Деятельность УЦ для участников обновлённой

отрасли после завершения реформы 63-ФЗ: цели, прогнозы, экономическая целесообразность» сделали прогнозы развития удостоверяющих центров в новых условиях. Согласно опросу участников РКІ-клуба, через 3–5 лет отрасль УЦ будет намного более национализирована. Ключевая функция УЦ будет инфраструктурной (сервисной, обслуживающей), а не связанной с получением бизнес-прибыли. «Необходимо было выбирать между доступностью для граждан дистанционных услуг и экономической прибылью. Сегодня для нас очевидно важнее доступность дистанционных услуг», — пояснил Роман Кузнецов, директор Правового Департамента Минцифры России.

Большая часть экспертов позитивно оценили изменения на рынке РКІ. По их словам, отрасль переформируется согласно новым «правилам игры», игроки получают новый опыт. Роль коммерческих УЦ меняется, а об итогах реформ говорить ещё рано.

Далее с докладом о реализации Федеральным казначейством функций УЦ для госсектора выступил начальник Управления режима секретности и безопасности информации Федерального казначейства Вячеслав Бражко. Основными стратегическими задачами ФК ставит для себя внедрение удалённой (облачной) ЭП, дистанционное открытие лицевых счетов, использование Единой биометрической системы для идентификации, интеграция УЦ с ЕИС УКС и «Госключом», переход на схему работы «УЦ во фронте», единые форматы контейнеров ключей ЭП, единые средства ЭП и защиты канала на мобильных устройствах.

На круглом столе «Трансформация региональной инфраструктуры УЦ в условиях реформы 63-ФЗ: обеспече-

ПРЕМИЯ РКІ-ФОРУМА

В рамках мероприятия состоялось награждение победителей традиционной Премии РКІ-Форума. Дипломы получили: пилотный проект по обмену электронными товароспроводительными документами при трансграничной торговле между хозяйствующими субъектами РФ и Республики Беларусь с применением механизма ДТС (ФНС России, «Газинформсервис», «СберКорус», «ИнфоТеКС Интернет Траст») в номинации

«Проект года»; Елена Ткаченко, руководитель экспертного совета «Электронные документы — эффективная экономика», в номинации «Эксперт года»; решение Aladdin LiveOffice в номинации «Продукт года»; Фонд «Сколково» (центр компетенций федерального проекта «Нормативное регулирование цифровой среды») в номинации «Организация года»; Фёдор Новиков, начальник управления электронного документооборота ФНС России, в номинации

«За вклад в развитие отрасли»; Болеслав Изотов, первый заместитель генерального директора НТЦ «Атлас», в номинации «За вклад в становление отрасли ЭП».

Также памятные дипломы, отражающие вклад в развитие отрасли, получили компания ИнфоТеКС и Ассоциация «РОСЭУ». Лучшим докладчиком «РКІ-Форума Россия 2021» был признан Станислав Смышляев, заместитель генерального директора «КриптоПро».



Сессия «Наиболее острые аспекты реформы 63-ФЗ»

ние полномочий и клиентского сервиса доверенных лиц» представители крупнейших УЦ поделились развитием филиальной сети УЦ в регионах после 1 июля 2021 года. Участники сошлись во мнении, что для работы по новым законодательным требованиям аккредитованным УЦ пришлось предпринять существенные организационные и технологические преобразования: от ужесточения взаимоотношений с региональными представителями до доработки и внедрения новых программных инструментов. Новый опыт появился и в плане клиентского обслуживания. Например, большинство клиентов крайне негативно оценивают новые требования к обязательной фотофиксации.

ДИСТАНЦИОННАЯ ЭП

На секции РКІ-Форума, посвящённой дистанционной электронной подписи, Станислав Смышляев, заместитель генерального директора компании «КРИПТО-ПРО», отметил ряд преимуществ хранения ключей пользователей на серверной стороне. По словам спикера, сегодня для дистанционной подписи сформированы принципы построения защищённой системы, разра-

ботана модель функционирования общей инфраструктуры.

Иван Аристархов, заместитель начальника Отдела специальных исследований и разработок компании «СФБ Лаб», охарактеризовал внутреннего нарушителя в системе дистанционной подписи. Основными угрозами, исходящими от внутреннего нарушителя АУЦ, названы угрозы нарушения целостности и конфиденциальности ключа ЭП, доступности ключа, конфиденциальности персональных данных, содержащихся в поручении, конфиденциальности подписываемой информации, целостности и доступности информации о результате исполнения поручения.

Денис Гребеньков, управляющий директор ПАО ВТБ, рассказал о создании Единой цифровой платформы подписания и хранения документов, которая разрабатывается Минцифры РФ, компанией «Ростелеком» и Банком ВТБ. Ключевые возможности платформы — подписание и удостоверение юридической значимости, облачные сервисы по управлению доверенностями и документами, хранение документов в защищённом облачном архиве, развитие маркетплейса.

Антон Мелузов, заместитель генерального директора по развитию бизнеса АО «Инфотекс Интернет Траст», представил практические аспекты применения технологии дистанционной электронной подписи в рамках оказания услуг УЦ. В рамках развития дистанционного взаимодействия он предложил систематизировать понятие идентификации гражданина, обеспечить единую правовую норму идентификации и градацию ответственности, совершенствовать существующие и внедрять новые механизмы идентификации.

Тема удалённой ЭП получила продолжение на круглом столе «Вопросы РКІ и электронная подпись на мобильных устройствах». Участники обсудили ключевые требования к организации использования мобильной подписи, особенности реализации схем дистанционной подписи на мобильных устройствах, поделились практикой применения удалённой электронной подписи.

РКІ И ИНТЕРНЕТ ВЕЩЕЙ

Интернет вещей может стать перспективной нишей для участников рынка электронной подписи, уверены участ-



Круглый стол «Вопросы PKI в IoT»

ники круглого стола «Вопросы PKI в IoT». На нём эксперты обсудили развитие PKI для IoT, необходимость новых стандартов, изменения в требованиях регуляторов. Только в России до 2025 года прогнозируется двукратный рост числа IoT/M2M устройств, подключённых к облачным и корпоративным системам управления — до 50 млн. Растёт необходимость обеспечения этих устройств и инфраструктур эффективными технологиями ИБ.

Соруководитель рабочей группы ТК26 «Криптографические механизмы для промышленных систем», АО «ИнфоТекС», Ольга Шемякина

ративным системам управления — до 50 млн. Растёт необходимость обеспечения этих устройств и инфраструктур эффективными технологиями ИБ. Соруководитель рабочей группы ТК26 «Криптографические механизмы для промышленных систем», АО «ИнфоТекС», Ольга Шемякина

перечислила особенности протоколов передачи данных, применяемых в IoT: LoRa, UNB, XNB, NB-Fi, NB-IoT. Криптографические алгоритмы в них должны быть быстрыми, с низким энергопотреблением, иметь минимальный набор алгоритмов и небольшое количество добавленных байтов. Спикер отметила, что сегодня в России нет форматов сертификатов ЭП, подходящих для M2M и IoT/IIoT.

Павел Смирнов, директор по развитию компании «КРИПТО-ПРО», поделился реальными сценариями применения IoT (классические датчики, бортовые устройства на транспорте, различные счётчики) для получения телеметрии: это электронная пломба при перевозке груза, экстренный вызов с автомобиля, страховая телематика с автомобиля.

Генеральный директор компании «Аладдин Р.Д.» Сергей Груздев в докладе «Российская элементная база и криптография для обеспечения доверия и безопасности IoT-устройств для объектов КИИ» обратил внимание на то, что требования, которые сегодня прописываются в конкурсной доку-

ОТЗЫВЫ ОРГАНИЗАТОРОВ И УЧАСТНИКОВ

Сергей Кирюшкин, заместитель председателя Программного комитета PKI-Форума, советник — начальник удостоверяющего центра ООО «Газинформсервис»:

PKI-Форум в очередной раз стал ключевым событием для рынка электронной подписи — три дня пролетели в активных переговорах, общение продолжалось и после окончания деловой программы. Что касается практических итогов, которые повлияют на негативные тенденции рынка, то Программный комитет традиционно готовит итоговую Декларацию, основанную на предложениях участников форума.

Мы направим её прежде всего регуляторам и проконтролируем, как она отразится на законодательной деятельности. Уже сейчас можно сказать, что влияние профессионального сообщества на позицию регуляторов заметно. Например, в Telegram-чате PKI-Форума присутствуют представители соответствующих министерств и ведомств,

которые реагируют на вопросы и замечания, оставляют комментарии.

Мы много работали, чтобы Форум стал площадкой, интересной для всех участников рынка PKI. Всё получилось. Спасибо коллегам за то, что они проявили интерес и неравнодушие!

Алексей Минаев, заместитель директора Департамента развития цифровой экономики Минэкономразвития:

Мероприятия, подобные PKI-Форуму, конечно, способствуют более глубокому пониманию государством потребностей рынка и задач, которые перед нами стоят. Законодательные активности обсуждаются на них много, компетентно и в основном конструктивно, в доверительном ключе. Мы видим, что профессиональное сообщество воспринимает происходящие изменения максимально заинтересованно, а иногда и болезненно. Это ещё раз

подчёркивает, как важно нам всем работать вместе.

С одной стороны, программа Форума показалась мне интересной и актуальной, докладчики были хорошо подготовлены, прозвучали свежие идеи. С другой стороны, на сессиях акцент делался в основном на презентациях, а не на обмене мнениями. Думаю, что не только в кулуарах, но и в рамках деловой части спикерам было бы важно получить обратную связь, обоснованные замечания...

Алексей Прошин, генеральный директор «ИнфоТекС Интернет Траст»:

В условиях трансформации рынка PKI, на мой взгляд, программа PKI-Форума оказалась предельно актуальной. Были подняты действительно рабочие вопросы. Например, мы увидели, как много изменений произошло со стороны государства: приняты новые нормативные акты, Минцифры сделало

ментации, недостаточны для безопасности IoT-устройств и создаваемой инфраструктуры. Без доверенной российской элементной базы невозможно добиться должного уровня безопасности IoT-устройств.

ЗАРУБЕЖНАЯ ПРАКТИКА

PKI-Форум традиционно не обходится без участия зарубежных экспертов. С одной стороны, необходимо перенимать успешный опыт других стран. С другой — без тесного взаимодействия и понимания особенностей зарубежных рынков PKI невозможно говорить о трансграничном обмене документами с использованием электронной подписи.

В этом году на европейском рынке PKI ведётся активное обсуждение новой редакции регламента eIDAS 2.0. Об этом на форуме рассказала руководитель проектов Asseco Data System Алла Столярова-Мыц. eIDAS — это регламент Евросоюза об электронной идентификации и доверительных услугах для электронных транзакций на Едином европейском рынке, действующий с 2016 года. Сегодня документ под-

лежит пересмотру в соответствии с новыми потребностями рынка.

Игорь Фургель (Dr. Igor Furgel), делегат от ФРГ в рабочей группе WG IV «Электронная коммерция» комиссии ООН по праву международной торговли (ЮНСИТРАЛ), представил результаты деятельности рабочей группы — юридические аспекты трансграничного признания управления идентификационными данными и услуг доверия.

Доклад генерального директора ООО «Новое пространство торговли», эксперта UNNExT Екатерины Силантьевой был посвящён роли электронной подписи в цифровой торговле. Электронная подпись — основа трансграничной безбумажной торговли. Она обеспечивает резкое сокращение времени на обработку и увеличение прозрачности всего процесса.

Екатерина Ермина, ведущий инженер компании «Газинформсервис», привела сравнение понятия доверенной третьей стороны в европейской (ТТР, по ITU-T X.842) и российской (ДТС, по ФЗ-63) терминологии.

Дмитрий Москалёв, заместитель начальника Национального центра

электронных услуг Республики Беларусь, продолжил разговор об интероперабельности при организации трансграничного обмена электронными документами. По его словам, ДТС позволяет «подружить» специфические для каждой страны схемы информационного взаимодействия.

Дмитрий Класс, управляющий директор компании «РЭЙЛ ЭКСПЕРТ», привёл точку зрения бизнеса на внедрение сервисов трансграничной ЭП в транспортном секторе. В результате проекта по созданию трансграничной ЭП компании удалось сократить сроки подписания и уменьшить почтовые расходы на отправления между Россией и Казахстаном.

* * *

На основе предложений экспертного сообщества, прозвучавших на Форуме и отправленных Программному комитету по дистанционным каналам, будет сформирована итоговая Декларация Форума. Документ будет размещён на сайте Форума и направлен более чем в 20 ведомств.

шаги в сторону внедрения ЭП для обеспечения потребностей граждан...

Сегодня мы сосредоточены на большом проекте по разработке мобильного приложения «Госключ» совместно с ВТБ, «Ростелекомом» и Минцифры. Эта инициатива пока воспринимается по-разному, и нам хотелось рассказать о ней подробнее. Вместе с тем мы являемся не только удостоверяющим центром, но и разработчиком технологий электронного документооборота. Очень рады, что проект по трансграничному электронному документообороту с Беларусью был признан победителем Премии PKI-Форума в номинации «Проект года». Это первый шаг к тиражированию подобных технологий.

Алексей Сенченков, коммерческий директор АО «Аналитический центр»:

Мы ежегодно принимаем участие в PKI-Форуме, так как считаем, что это ключевая площадка для обсуждения наболевших вопросов, встречи с регуляторами и бизнес-партнёрами. Здесь мы имеем возможность высказать своё мнение и ожидать, что нас услышат. Замечательно также, что оргкомитет не акцентируется только на проблемах удостоверяющих центров, а всегда

находит темы, которые интересны и вендорам, и их клиентам.

Михаил Кудрявцев, научный сотрудник Академии криптографии РФ:

В программе форума был сделан акцент на наиболее актуальных вопросах, которые сейчас ставятся цифровой экономикой. В этом смысле мероприятие расширило мой кругозор и оказалось очень полезным. Для Академии криптографии РФ важно понимать, какие перспективные направления научных исследований сегодня наиболее актуальны, какие криптографические механизмы требуют стандартизации. Например, мы очень плодотворно обсудили со специалистами, заинтересованными в развитии беспилотного транспорта, вопросы, связанные с реализацией в нём криптографических механизмов защиты.

Илья Моргасов, генеральный директор ООО «Фирма ИнфоКрипт»:

Я участвую в PKI-Форумах ежегодно. Данная площадка сегодня единственная, где проблемы отрасли открытых ключей и ЭП обсуждаются максимально концентрированно, сфокусированно. Поэтому я очень её ценю. В этом году для нашей организации

наиболее актуальны были темы M2M и непосредственно удостоверяющих центров, и мы получили исчерпывающую информацию.

Николай Афанасьев, ведущий менеджер по развитию продукта «Аладдин Р. Д.»

Мы гордимся тем, что наша компания — в лице заместителя генерального директора Алексея Сабанова — стояла у истоков PKI-Форума. Сегодня отрасль динамично преобразуется, и Форум позволяет нам не только обмениваться опытом с бизнесом, но и напрямую обратиться к регуляторам, ведь многие вещи, с которыми мы работаем, завязаны на нормативно-правовых актах. Кроме того, мы как вендор заинтересованы в продаже наших продуктов в составе различных комплексных решений. На PKI-Форуме мы находим точки соприкосновения с партнёрами, прорабатываем их.

В начале пандемии мы увидели большой спрос со стороны бизнеса и госорганов на инструмент для безопасной дистанционной работы и недавно представили продукт LiveOffice, который кардинально решает проблему. И мы, конечно же, рады, что наше решение стало победителем Премии PKI-Форума-2021 в номинации «Продукт года».

CYBER POLYGON 2021

БЕЗОПАСНОСТЬ ДОЛЖНА БЫТЬ ВСТРОЕННОЙ

При сравнении ряда «однотипных» мероприятий (с точки зрения решаемых задач в интересах повышения квалификации участников в сфере ИБ) бросается в глаза яркая официальная составляющая тренинга Сбера Cyber Polygon. Что неудивительно, ведь это инициатива межгосударственного масштаба. Cyber Polygon проводится при поддержке Центра кибербезопасности Всемирного экономического форума и Интерпола. И в программе конференции «при» Cyber Polygon много имён тех, чьи компетенции выходят за рамки национальных границ.

Правда, есть у Cyber Polygon и черты, общие для «однотипных» мероприятий. В частности, информация о событиях на собственно киберполигоне закрыта для массовой аудитории и вовне выдаётся строго дозированно.

НЕМНОГО О ЗАКУЛИСЬЕ

В «первые часы» трансляции мероприятия 9 июля было объявлено, что команды участвуют в работе по двум сценариям — Защита и Реагирование. А «под занавес» прошло сообщение о завершении работы по первому сценарию киберучений, о закрытии «синей» командой Сбера «всех 5 уязвимостей» и её вхождении в «топ» 5–6 команд, которые смогли «всё пропачить». Ну и было анонсировано начало работ по второму сценарию. В общем, с информацией, то

бишь с гласностью, вышла просто беда, «полный глушняк».

Попытка по прямым каналам получить развёрнутые комментарии о собственно учениях потерпела фиаско. Всё, что устроители сочли возможным вынести на свет по результатам учений, уложилось в пару абзацев: «Судя по словам участников, тренинг был для них полезен — мы получили много позитивных отзывов. Кому-то он показался сложным, однако были и такие команды, которые справились со всеми заданиями без единой подсказки. Большинство участников планируют присоединиться и в следующем году. По правилам тренинга Cyber Polygon мы не разглашаем информацию о том, как выступили команды. Результаты, выводы и рекомендации мы представим в подробном отчёте о прошедшем тренинге осенью этого года. Но места команд мы не раскрываем по правилам тренинга».

Ну и что ещё стало известно до начала тренинга, это то, что «технический тренинг был полностью реализован командой BI.ZONE — мы разрабатывали концепцию и идею, собирали инфраструктуру, продумывали задания сценариев, выступали в роли Red Team. IBM на протяжении трёх лет является нашим технологическим партнёром и предоставляет «облако» для развёртывания технической инфраструктуры первого сценария тренинга.

...из-за ограничений инфраструктуры в этом году тренинг не смог принять к участию всех желающих. Из более чем 1200 заявок пришлось подтвердить только 200 участников. В 2022 году планируется внести некоторые изменения и дать возможность участвовать намного большему числу организаций».

КОНФЕРЕНЦИЯ «ПРИ» CYBER POLYGON 2021

В отличие от практической части мероприятия, конференция «при» Cyber Polygon 2021 уже летом предоставила пищу для размышлений о судьбах людей в условиях агрессивной цифровизации всех сторон жизни, включающей формирование связей между ними, иногда очевидно недобровольных, нежелательных, навязчивых, утомительных, а то и просто опасных.

А в корпоративном сегменте развивающимся трендом стали атаки из киберпространства через партнёрские связи жертвы. И именно отражение таких таргетированных supply chain атак стало темой технического тренинга Cyber Polygon 2021.

ВЕРНОЙ ДОРОГОЙ ИДЁМ, ТОВАРИЩИ!

Из выступлений на Cyber Polygon 2021 таких высокопоставленных персон, как премьер-министр РФ Михаил Мишустин и Клаус Шваб, основатель и президент Всемирного экономического форума, следовало, что «наверху» прекрасно осведомлены об опасном влиянии роста киберугроз на устойчивость экономики и неприкосновенность частной жизни и «экономики» частных лиц. Осведомлены, но не рассматривают иной альтернативы, кроме как обеспечение «прорывов в экономике» за счёт цифровизации и развития так называемых прорывных технологий (Михаил

В корпоративном сегменте развивающимся трендом стали атаки из киберпространства через партнёрские связи жертвы. И именно отражение таких таргетированных supply chain атак стало темой технического тренинга Cyber Polygon 2021

Мишустин). Тем более что именно цифровизация позволила «сохранить экономику в нынешней ситуации» (один из аргументов Клауса Шваба).

Ну а что касается киберугроз, то премьер-министр РФ порекомендовал правильно оценивать риски и поддерживать инициативу России о создании единой основы для управления киберрисками.

По мнению же г-на Шваба, комфортность и безопасность цифрового образа жизни сможет обеспечить «Закон о Цифре ЕС» (дословная терминология перевода). Хотя президент Всемирного экономического форума не забыл и о важности технологических преобразований, упомянув о том, что для комфортности и безопасности цифрового образа жизни одних «масок» недостаточно, нужна будет и «вакцинация»! И критическая информационная архитектура должна будет иметь встроенные «антитела» уже на этапе её внедрения.

Тема о «вакцинации» ИТ и «антителах» в ней нашла продолжение в дискуссии об устойчивости supply chains, к которой были привлечены топ-менеджеры нескольких ведущих ИТ-компаний, работающих в сфере защиты информации. Россию в ней представлял глава «Лаборатории Касперского». Конечные же выводы этой дискуссии в обобщённом виде звучали приблизительно так: информационным технологиям пора отдавать свои долги. Безопасность должна быть встроенной. Будет хуже, прежде чем станет лучше. А пока в тактической перспективе следует задуматься над совершенствованием критических инфраструктур для упрощения их защиты.

НЕ ФАНАТ...

Интересная информация к размышлению прозвучала в диалогах Стива Возняка с Германом Грефом.

В них была затронута тема важности единства аппаратных и программных компонент в ИТ-мире для устойчивости КИИ и просто информационных инфраструктур к киберугрозам. При этом естественным центром кристаллизации таких экосистем является «железо», обрастающее разработками ПО. В качестве примеров вполне естественно «всплыли» Apple- и Microsoft-сообщества, и Стив Возняк упомянул в качестве источника

Информационным технологиям пора отдавать свои долги. Безопасность должна быть встроенной. Будет хуже, прежде чем станет лучше. А пока в тактической перспективе следует задуматься над совершенствованием критических инфраструктур для упрощения их защиты

киберугроз шлейфы «унаследованного» кода в одной из этих экосистем.

При смещении фокуса диалога к теме «искусственного интеллекта» (ИИ) Стив Возняк формулировал свои комментарии в ключе, скорее негативном для ИИ. Оценивая, в частности, конкретные результаты проверки «беспилотных» функций своего автомобиля, он уверенно использовал для ИИ такое определение, как «алгоритм идиотизма», и заявил, что технологиям нельзя позволить думать за нас.

Завершающей темой диалогов Германа Грефа с одним из отцов яблочной компании стала биометрическая идентификация. Как и в случае обсуждения ИИ, Стив Возняк не слишком высоко, но дипломатично оценил уровень развития биометрии. В качестве примера уместно привести следующие слова гуру: «Раньше технология распознавания лиц была «сырой». Сейчас это работает лучше».

В целом позицию Стива Возняка по отношению к нынешним хайпам в сфере ИТ трудно было оценить словами «фанат технологий», термином, который в канву беседы ввёл Герман Греф.

ВЯЗКИЕ ТЕМЫ

В дискуссии «Цифровое государство будущего — какое оно?», к участию в которой были приглашены представители «Ростелеком-Солар» и «Майкрософт», организаторы конференции намеревались, похоже, представить слушателям светлое будущее гражданина «цифрового государства».

Заглянуть в далёкое будущее не пришлось, так как, по признанию одного из участников беседы, нынешняя глубина планирования — это недели и месяцы. Не дальше... Что же касается уровня киберугроз для электронного «государствоустройства», то, по заявлению

Игоря Ляпунова, через 5 дней после появления нового элемента «в множестве gov.ru» на него совершается первая кибератака. И ресурсы, выделяемые на атаку инфраструктуры gov.ru, могут составлять 1,5 млн долларов.

Ещё одна «панель» конференции была посвящена теме криптовалют и «цифровых денег» в целом. Россию на дискуссии представлял заместитель председателя ЦБ РФ Алексей Заботкин, зарубежье — президент Mastercard Europe Марк Барнетт и глава стратегических партнёрств, старший вице-президент Visa Мэттью Дилл.

Позиция «Запада»: наша цель — помочь клиентам платить и получать оплату удобным способом.

Позиция ЦБ РФ: в цифровизации деньги не должны отставать от людей. Однако «криптовалюты» — это опасный суррогат, большие риски и не самое эффективное средство для торговли. А одна из реальных перспектив «цифровых денег» в нашей стране — цифровой рубль.

* * *

Завершить же этот краткий обзор онлайн-конференции во время киберучений Cyber Polygon 2021 уместно комментарием устройств (это к вопросу о гласности): «онлайн-конференция с участием высокопоставленных спикеров готовилась совместно компанией VI.ZONE и Сбером и прошла при активной поддержке со стороны Всемирного экономического форума и Интерпола. Трансляция мероприятия шла в социальных сетях данных организаций (Facebook и Twitter). Общая аудитория составила более 7 миллионов зрителей из 78 стран».

ИНФОТЕКС ТЕХНОФЕСТ МОСКВА — 2021

ЕСТЬ КОНТАКТ!

Компания ИнфоТеКС провела в Москве конференцию для технических специалистов ИнфоТеКС ТехноФест-2021. Мероприятие прошло во второй раз и собрало около 500 специалистов по ИБ. Программа включала три потока, спикеры представили более 30 докладов. Специалисты ИнфоТеКС рассказали о концепции ZTNA, защите мобильных коммуникаций, сертифицированной защите КИИ, решениях на базе распределённых реестров и смарт-контрактов, о системе обнаружения угроз и реагирования на них. В общем, камерное узкопрофильное мероприятие. Заслуживающим широкого отраслевого внимания его сделали, ИМХО, два момента: активная обратная связь и Квантовый лекторий.

ОБРАТНАЯ СВЯЗЬ — ГЛАЗА В ГЛАЗА

Главным достоинством мероприятия стало не только отсутствие официоза, но и возможность прямого общения с техническими экспертами, непосредственно связанными с разработками. Это превращает мероприятия ИнфоТеКС ТехноФеста в своеобразную систему обратной связи, обеспечивающей повышение и качества продуктов компании, и качества их поддержки в ходе эксплуатации.

В связи с этим весьма показателен комментарий заместителя генерального директора ИнфоТеКС Дмитрия Гусева:

— Интерес к нашей технической конференции крайне высокий... Наша профессиональная сфера развивается стремительно, нужно постоянно держать

руку на пульсе. Понимая это, мы считаем нужным и важным делиться своими знаниями, которые, безусловно, представляют ценность для ИБ-специалистов... Информации в открытых источниках сегодня много, но в такой сфере, как кибербезопасность, лучше получать её из первых рук. Мы предлагаем всем желающим пообщаться лично с нашими разработчиками и задать любые вопросы. Нам важна обратная связь от потребителей наших продуктов, это помогает нам совершенствовать их и развивать... Мы обходимся без официальной части и торжественных речей, переходим сразу к полезному контенту о продуктах компании, с мастер-классами, how to и практикумами.

После знакомства с таким комментарием уместно вспомнить, что одним из вопросов, с которым лучше

ПО ПОВОДУ КАЧЕСТВА ПРОДУКЦИИ И ОБРАТНОЙ СВЯЗИ

Один из негативных «трендов» современной ИТ-индустрии — падение качества продукции, связанное с появлением методик Agile и DevOps, направленных на сокращение длительности циклов разработки ПО до нескольких недель или даже дней. Зачастую такие продукты представляют собой незавершённые «поделки», которые под прикрытием упомяну-

тых идеологий предлагаются для бета-тестирования.

Не отличается высоким качеством и прилагаемая техническая документация, нередко она неточна и/или неполна. И это на руку поставщикам: чем меньше сказано в руководствах и описаниях, тем меньше ответственность перед потребителем.

При этом неэффективным оказывается и сервис «поддержки по те-

лефону»: многие вендоры разорвали прямые связи между заказчиками и разработчиками, поместив между ними множество «прокладок». Напрямую теперь можно контактировать с прослойкой «технических представителей», слабо осведомлённых в части технической конкретики, которые, в свою очередь, транслируют (зачастую в искажённом виде) вопросы заказчиков на следующий уровень под-

знакомиться из первых рук, является развитие технологии квантового распределения ключей.

СЧАСТЬЕ — ЭТО КОГДА ТЕБЯ ПОНИМАЮТ

Вековая история выхода современной физики из лабораторий в практику содержит немало курьёзов, связанных с оценками обывателями того, чем наука занимается и что предлагает. Один из таких курьёзов случился два года назад, когда ИнфоТеКС и Центр квантовых технологий (ЦКТ) физфака МГУ продемонстрировали работу первой в России линии голосовой телефонии с криптозащитой на «квантовых ключах».

К сожалению, тогда не все присутствующие поняли, что изюминка демонстрации — не обыденные телефонные аппараты, а две невзрачные «коробочки». Одна внутри корпуса, напоминающего системный блок ПК, другая отдельно, в конструктиве формата 3U. На них никто не обратил внимания, все по привычке были заняты телефонными аппаратами, идущими на самом деле, как говорится, в комплекте. А квантовые технологии тем

временем работали внутри именно этих «коробочек».

Сегодня ИнфоТеКС стал одной из первых отечественных компаний, которые ввели систему квантового распределения ключей в опытную эксплуатацию. И на нынешнем ТехноФесте был организован поток Квантового лектория: его участникам подробно рассказали о новом перспективном направлении в технологиях защиты.

КВАНТОВЫЙ ЛЕКТОРИЙ

Эксперты ИнфоТеКС и партнёры компании из Московского государственного университета стартовали с рассказа об общих основах для использования квантовых эффектов в защите информации. Внимание аудитории было обращено на то, что квантовые технологии сегодня выходят на новый технологический уровень, позволяющий манипулировать одиночными квантовыми объектами — атомами, ионами, электронами, фотонами.

Однако рассказ о фантастических перспективах квантовых технологий был сбалансированно разбавлен информацией, позволившей слушателям

перейти от экзальтации по поводу «квантовых вычислений» и «квантовых компьютеров» к реальному сопоставлению этих инноваций с классическими средствами вычислительной техники и криптографической защиты. Причём к сопоставлению не в чёрно-белых категориях «лучше/хуже», а в контексте большей пригодности с учётом требований к условиям использования, стоимости и другим объективным ограничениям. Для этого в докладах Квантового лектория были приведены числовые оценки возможностей разрабатываемого принципиально нового оборудования.

* * *

Завершился Квантовый лекторий выступлением научного руководителя ЦКТ физфака МГУ Сергея Кулика, который рассказал об истории взаимодействия ИнфоТеКС и МГУ, отметил значительный прогресс в развитии «квантовых технологий», будь то коммуникации или вычисления, и дал высокую оценку складывающейся ситуации в контексте совместных работ с ИнфоТеКС.

BIS-КОММЕНТАРИЙ

держки, при этом надёжно изолируя заказчиков от тех, кто действительно может им помочь.

В качестве нового «инструмента технической поддержки» предлагаются интернет-форумы. Но нередко заданные вопросы остаются там без ответа неделями и месяцами, а если ответ всё же приходит, то часто оказывается некомпетентным или просто бесполезным.

Причиной падения качества является пришедший из-за рубежа тренд построения «экономичного бизнеса» (leaning out of companies), культивируемый «эффективными» менеджерами — управленческой бюрократией, озабоченной лишь экономическими материями.

Подобный подход ставит под угрозу культуру разработок по всему миру.

Сегодня лишь малое число компаний поддерживает внутреннее системное управление качеством продукции. В ряде случаев такие программы направлены лишь на достижение совместимости версий продуктов, а не на повышение их качества в идеальном понимании этой характеристики. К тому же нередко программы качества реализуются на основе внутренних обсуждений — без учёта мнений заказчиков. А один человек или даже небольшая команда неспособны осмыслить все аспекты разработки до тонкостей. Кроме того, организация труда в компаниях, как правило, не оставляет разработчикам достаточно времени для управления качеством и документацией. В результате вместо качества как си-

стемного явления предлагаются в лучшем случае своеобразные «фрагменты качества».

К этому добавляются объективные обстоятельства — усложнение ИТ-продукции (это касается как аппаратной составляющей, так и программного обеспечения).

* * *

Стабилизировать выходящую из-под контроля ситуацию можно добавлением своеобразного сигнала обратной связи в систему. Вариант этой «технологии» мы наблюдали на ИнфоТеКС ТехноФест 2021.

Валерий КУЛИКОВ
обозреватель BIS Journal

БАНКИ РОССИИ — XXI ВЕК

ТРИАДА КИБЕРБЕЗОПАСНОСТИ НА XVIII МЕЖДУНАРОДНОМ БАНКОВСКОМ ФОРУМЕ В СОЧИ

Если взглянуть на программу форума «Банки России — XXI век», состоявшегося в сентябре в Сочи, то из полутора десятков его официальных мероприятий больше половины так или иначе были связаны с цифровыми технологиями. Даже обсуждение принципов «устойчивого развития» (экологическое, социальное и корпоративное управление) вывело на «цифровую» проблему — необходимости корректных алгоритмов анализа данных. В таком контексте ставки проблем кибербезопасности котировались на форуме довольно высоко — как «очень актуальные». По сути, эти проблемы могут быть сведены к триаде «оборот и обработка данных / искусственный интеллект (ИИ) / мошенничество эпохи цифровой экономики».

ОБОРОТ И ОБРАБОТКА ДАННЫХ

На форуме были озвучены новые термины: «персональные данные корпоративных клиентов» (в дополнение к «классике», отражённой в 152 ФЗ и GDPR) и «мнения» (субъективная информация из социальных сетей). Растёт тезаурус, а с ним и вся система.

Но в основном обсуждались оборот и «монетизация» ПД людей, попавших в поле зрения разных информационных систем. Мнения разделились. По словам главы Банка России, ПД у нас находятся практически в открытом доступе, все ими могут свободно воспользоваться, и эта ситуация является нетерпимой.

Подопечные же БР смотрят на ситуацию спокойно, прикрываясь рассуждениями об «обезличенных» ПД и обработке данных только для «заявленных целей». Это и понятно, ведь это зона реальности, где «закон, что дышло...» и «строгость российских законов искупается необязательностью их исполнения».

Уместно заметить, что в этой «нетерпимой» ситуации сами «владельцы» ПД свободно разбрасываются своими данными и по социальным сетям, и там, где доброжелательные клерки перед оказанием услуг требуют паспорт и согласие на обработку данных.

И всё же та последовательность, с которой регулятор внедряет свои мнения в жизнь, позволяет надеяться на положительные сдвиги в деле защиты ПД, хотя бы в финансовой сфере.

Термин «персональные данные корпоративных клиентов» (КПД) был введён в оборот на форуме Д. А. Аксаковым, исполнительным директором ВЭБ.РФ. Опыт работы в иностранных инвестиционных компаниях позволил ему обратить внимание на неэффективность работы иностранцев с КПД, на засилье «ручных» технологий сбора, примитивного Excel-анализа и, как следствие, низкую эффективность прогнозирования сделок. По его словам, достижения отечественного финтеха в сфере «интеллектуального» анализа ПД дают надежду избежать таких ошибок.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

Статью по мотивам круглого стола «Человек и искусственный интеллект: единство и борьба противоположностей» читайте на стр. 26 в разделе «Тема номера / Искусственный интеллект в банках».

МОШЕННИЧЕСТВО

На круглом столе «Киберугрозы и обеспечение информационной безопасности: проблемы и решения» обсуждалась тема более узкая, чем ожидалось. Сформулировать её можно как «Меры по борьбе с кибермошенничеством и перспективы межведомственного взаимодействия, способы противодействия социальной инженерии».

И именно по поводу «социальной инженерии» было сделано первое маленькое «открытие». Оказывается, сегодня

«обычный человек» нередко выступает «фронтом» привычных мошеннических схем. Например, «обычный человек» оформляет несколько банковских карт на своё имя и передаёт их за малую толику денег третьим лицам. Тут тебе и заработок, и полная непричастность к возникшим последствиям, ведь передавать карты третьим лицам законом не запрещено.

А второе открытие ещё интереснее. Оказывается, информационная инфраструктура, созданная для официальной цифровой экономики, полностью пригодна для выполнения целей и задач неофициальной — теневой — цифровой экономики. Как говорится, потрудились на славу!

И пока профессиональное сообщество безуспешно борется с технологией подмены телефонных номеров (хвала IP-телефонии!), средний «чек» мошеннических операций через официальные социальные сети уже превосходит ту же характеристику для телефонных «операций». Что, впрочем, не снимает с повестки дня так и не решённый вопрос о выводе из цифровой инфраструктуры страны операторов связи, специализирующихся на прокате «серого» и «чёрного» трафика.

ВИДЫ НА УРОЖАЙ

И напоследок цитата руководителя Банка России:

«Есть инновационные банки, и есть те, и их немало, кто не инвестирует в собственную цифровую трансформацию и смотрит на это как на необязательную составляющую бизнеса, понимая, что эти инвестиции не дешёвые. На взгляд регулятора, такая цифровая трансформация неизбежна. В этом году у банков будет большая прибыль. И призываю вас подумать о том, чтобы частично направить эту прибыль именно в инвестирование инноваций, в собственную трансформацию, подкрепляя свои будущие бизнес-модели».

BIS SUMMIT 2021

О ТЕХНОЛОГИЧЕСКОМ ОПТИМИЗМЕ И СМЕНЕ ПАРАДИГМЫ

Слоган BIS SUMMIT 2021 — «Технологический оптимизм и смена парадигмы» — вызвал вопросы. Например, в организационном плане мероприятие вернулось на офлайн-площадку, сохранив при этом и своё присутствие онлайн, что существенно расширило аудиторию. Стало меньше театральных эффектов, набор обсуждаемых тем приобрёл компактность. Но можно ли такие изменения назвать сменой парадигмы? Вряд ли.

ЗАПАД НАМ НЕ ПОМОЖЕТ

Александр Шойтов, замминистра цифрового развития, связи и массовых коммуникаций РФ, заявил, что лично ему очевидна необходимость включения вопросов информационной безопасности в явном виде в каждый из разделов документов, касающихся цифровой экономики.

К сожалению, один замминистра в поле не воин, а корни проблем киберустойчивости цифровой инфраструктуры страны растут ещё из тех времён, когда цифровизацией заправляли совсем другие люди, убеждённые, что Россия богата и всё купит. В таком контексте тема импортозамещения звучала на форуме рефреном, и в какой-то момент разговор пошёл о последствиях запретов или ограничений для зарубежных ИТ-вендоров работать с нашей страной.

Г-н Шойтов оценил такую ситуацию как критическую, если подобного рода санкции будут объявлены «завтра». Но выразил убеждённость, что страна сможет преодолеть проблемы разрыва поставок и прекращения технической поддержки, если введение санкций будет отложено на среднесрочную перспективу.

СТАРОЕ ВИНО В НОВЫХ БУТЫЛКАХ

Другой вариант интерпретации рамочной темы саммита можно поискать в утверждениях некоторых экспертов о «вале технологий», который гонит ИТ-отрасль.

Если «вал технологий» существует, то, пребывая в лирическом настроении, это

явление, наверное, и можно было бы назвать «технологическим оптимизмом». Но блицопрос аудитории такого явления не выявил. Более того, отчётливо проявилось мнение, что технологии, которые многие считают современными, извлечены из старых заглазников: и блокчейн, и искусственный интеллект, и робототехника — всё это академические открытия давно минувших лет. А идеи «безопасного программирования» вообще извлечены из запыхлённых советских ГОСТов.

Поэтому «технологический раздел», на котором и рассматривались вопросы Open Source, искусственного интеллекта, DLP, безопасного программирования и т.п., можно рассматривать как процесс дегустации старых вин, поданных в новых бутылках, но никак не «вал технологий».

ДУМАЙ О РОДИНЕ!

Внимание «безопасному программированию» уделит и Виталий Лютиков, замдиректора ФСТЭК России (панельная дискуссия «Киберустойчивость цифрового мира»). Триггером спора стало упоминание о том, что вопрос о необходимости принятия отраслью этого подхода был поставлен регулятором ещё в 2016 году, но многие компании пропустили этот сигнал мимо ушей. В ответ оппоненты заявили, что для «безопасного программирования» нет исчерпывающего набора методических документов, а представители отрасли ещё и напирали на экономическую неэффективность этого метода.

В ходе дискуссии Виталий Лютиков набросал «эскиз» маршрутной карты для внедрения «безопасного программирования» и дал твёрдый отпор «фракции экономистов». Недопустимы, по

его мнению, компромиссы в пользу экономических соображений, когда речь идёт о безопасности страны.

ПРО ИИ

Доклад Шамиля Ульбашева из НЛМК высветил узкое место методологии Data Science в контексте ИБ. Это ставшее стандартом де-факто широкое использование сторонних «опенсорсных» приложений для «датамайнинга», код которых — очевидный «чёрный ящик» и с точки зрения рисков прямых ошибок программирования, и с точки зрения методологических ошибок в используемых алгоритмах анализа первичных данных.

OPEN SOURCE

Частое обращение к теме Open Source на BISS 2021 вышло за рамки обычного хайпового шума. Одним из поводов для этого стали санкционные угрозы. Евгений Ковнир, гендиректор АНО «Цифровая экономика», предположил, что применение Open Source-решений может стать элементом обеспечения безопасности от санкций и помочь закрыть дыры в тех нишах, где нет отечественных проприетарных решений.

Соглашаясь с «духом» этого мнения, хотелось бы получить более развёрнутые комментарии о реалистичности и сроках исполнения «определённых планов по тому, как делать серийные, массовые устройства на Open Source-системном доверенном стеке». Но BISS 2021 не дал ответа на этот вопрос.

Однако замдиректора ФСТЭК России анонсировал более детальное обсуждение темы на грядущей конференции под патронажем Института системного программирования.

Отчётливо проявилось мнение, что технологии, которые многие считают современными, извлечены из старых заглазников: и блокчейн, и искусственный интеллект, и робототехника — всё это открытия давно минувших лет

**Владимир ДРЕЛИХОВ**

первый заместитель начальника
Центра инженерного анализа
и специальных разработок
АО «Институт точной механики
и вычислительной техники
им. С.А. Лебедева РАН»,
кандидат физико-математических наук

**Игорь КУПАЛОВ-ЯРОПОЛК**

начальник Центра инженерного
анализа и специальных разработок
АО «Институт точной механики
и вычислительной техники
им. С.А. Лебедева РАН»

ПРОЕКТ «КОНУС» В ДЕЙСТВИИ

ПУТИ ПОВЫШЕНИЯ ЗАЩИЩЁННОСТИ ОТЕЧЕСТВЕННЫХ СЕТЕЙ ПОДВИЖНОЙ РАДИОТЕЛЕФОННОЙ СВЯЗИ

Комплекс средств и систем подвижной радиотелефонной связи (ПРТС), называемой также мобильной или сотовой связью, является важной и неотъемлемой частью информационных сетей во всём мире. Повсеместное внедрение удобных и оперативных услуг и сервисов мобильной связи, информационных систем и вытекающая из этого «цифровизация» большого объёма разнообразных данных (включая персональные и конфиденциальные данные), которые передаются, обрабатываются и хранятся в сетях мобильной связи, обуславливают необходимость решения задач комплексного обеспечения информационной безопасности подвижной радиотелефонной связи, защиты информации, данных абонентов и операторов сетей от различных групп угроз, реализуемых как в сфере программных технологий, так и специальными техническими средствами.

АКТУАЛЬНОСТЬ ЗАДАЧИ

Разработка и реализация действенных мер противодействия современным угрозам информационной безопасности имеют особую значимость и актуальность для мобильных сетей связи на территории нашей страны. Это определяется прежде всего тем, что практически всё программное и аппаратное

обеспечение, включая оборудование управления и обработки данных, используемое сотовыми операторами на территории России, — иностранной разработки и производства. Такая же ситуация наблюдается и на российском рынке окончательных мобильных устройств.

Кроме того, в связи со сложными условиями современной политической ситуации в мире и политикой санкций и ограничений, проводимой рядом иностранных государств и направленной на оказание давления на Россию, их спецслужбы могут использовать всевозможные способы и методы деструктивного воздействия.

О ДОВЕРЕННЫХ ЭЛЕМЕНТАХ БЕЗОПАСНОСТИ

В сложившейся ситуации с доминирующим иностранным оборудованием в российских ПРТС ключевым вопросом при разработке и реализации решений по информационной безопасности и защите мобильных сетей связи является определение в экосистеме ПРТС мест встраивания доверенных элементов безопасности, которые обеспечат безопасное хранение долговременных секретных ключей и надлежащее функционирование криптографических алгоритмов. Отчуждение из информационной системы модуля (модулей), выполняющего хранение и обработку

критической информации, и замена его защищённым модулем позволяет решить ряд задач, в том числе задачу безопасной взаимной аутентификации сим-карты абонента и ядра сети, выполнение процедур, связанных с применением квалифицированной электронной подписи, а в перспективе и других функций безопасности, вне зависимости от состава и модели оборудования оператора сети, страны происхождения и фирмы-производителя, а также вне зависимости от модели мобильного устройства и его операционной системы.

Проведённые исследования показали, что со стороны абонента таким элементом безопасности, вне зависимости от типа и происхождения мобильного устройства, может являться только встраиваемое надлежащим порядком в SIM-карту, точнее в её чип-модуль, специальное программное обеспечение, реализующее защищённое хранилище криптографических алгоритмов, долговременных ключей абонентов, ключей электронной подписи, другой конфиденциальной информации.

Важным является то, что доверенная SIM-карта с неизвлекаемым ключом с аппаратным модулем защиты памяти защищена от внутреннего нарушителя, что делает её элементом безопасности для аутентификации пользователей различных цифровых

сервисов, в том числе и суперсервисов. Дополнительный фактор аутентификации пользователя — фактор обладания защищённой SIM-картой с личным ключом УКЭП.

Однако используемые в настоящее время на территории Российской Федерации SIM-карты не смогут выполнять роль элемента безопасности отечественных сетей связи, поскольку они практически все — иностранного производства. Это означает, что все технологические операции производства SIM-карт, включая инициализацию и персонализацию, выполняются за рубежом или на производственных площадках иностранных компаний в России по закрытой для российской стороны технологии. В ходе этих операций в чип-модуль SIM-карты за пределами России производится загрузка программного обеспечения (ПО), включающего операционную систему и важнейшие компоненты обеспечения безопасности — специальное программное обеспечение, криптографические алгоритмы и секретные ключи и т.п. При этом не представляется возможным установить безопасность долговременных секретных ключей абонентов, записываемых иностранными производителями в чипы SIM-карт, поставляемых в Россию.

Анализ имеющихся случаев утечки информации и данных абонентов подтверждает, что спецслужбы ряда иностранных государств, прежде всего США, имеют возможность доступа к базам данных крупнейших мировых производителей SIM-карт (Thales, Giesecke+Devrient и др.) и, прежде всего, к данным SIM-карт, поставляемых в Российскую Федерацию. Эти возможности позволяют иностранным спецслужбам осуществлять мероприятия по контролю трафика ПРТС России, получению доступа как к данным российских абонентов, так и к содержанию их переговоров и другой информации.

Со стороны оператора, то есть в оборудовании сети, установленном у операторов мобильной связи, функции доверенного элемента безопасности имеют ряд отличий. Долговременные секретные ключи на стороне оператора хранятся в специальной базе данных HSS, а доверенным компонентом для

Используемые в настоящее время на территории Российской Федерации SIM-карты не смогут выполнять роль элемента безопасности отечественных сетей связи, поскольку они практически все — иностранного производства

хранения ключевой информации, реализации криптографических протоколов, используемых для аутентификации сим-карт и выработки сеансовых ключей является блок AuC, причём в зависимости от производителя компоненты HSS и AuC могут быть разделены в аппаратном исполнении либо реализованы виртуально, что в последнее время практикуется наиболее часто.

Эти критически важные с точки зрения обеспечения информационной безопасности компоненты оборудования операторов сотовой связи — устройства HLR/HSS (включая встроенные или отдельные модульные устройства AuC), не могут удовлетворять требованиям, предъявляемым к доверенным элементам безопасности систем ПРТС Российской Федерации, поскольку поставляются иностранными производителями в составе основного оборудования фактически как «чёрные ящики», функциональность которых в полной мере неизвестна потребителям и не сертифицирована компетентными экспертными организациями Российской Федерации. Отметим, что многие иностранные производители обязательным компонентом сервисного обслуживания вводят удалённый онлайн-мониторинг работы устройств с целью, как официально заявляется вендорами, ускоренной реакции на инциденты, упрощённого порядка обновления программного обеспечения и оперативного устранения сбоев в работе оборудования, тем самым оставляя себе возможность внешнего воздействия на оборудование систем ПРТС, установленного у российских операторов.

Загрузка секретных ключей в оборудование оператора происходит также по проприетарной процедуре, встроенной в программное обеспечение HLR/HSS конкретного иностранного

производителя. Как уже отмечалось, программное обеспечение HLR/HSS не проходило какой-либо сертификации в Российской Федерации на предмет отсутствия недеklarированных (скрытых) функций и может быть использовано иностранными компаниями для съёма служебной и иной информации и данных для спецслужб иностранных государств.

Таким образом, если рассматривать в целом комплекс организации и реализации мобильной связи на территории России на оборудовании и технологиях иностранного происхождения, в настоящее время нет возможности убедиться в том, что:

- ♦ операционная система и реализация криптографических алгоритмов в SIM-карте, а также операционная система, специальное программное обеспечение и реализации криптографических алгоритмов в комплексах HLR/HSS (AuC) выполняют только те функции, которые они должны выполнять, и не имеют недеklarированных возможностей, направленных на исполнение дополнительных функций;

- ♦ в реализации криптографических алгоритмов в SIM-карте, HLR/HSS или операционных системах не оставлены возможности для утечки данных, запуска программ-закладок или блокировки работы абонента, оператора или сети мобильной связи в целом;

- ♦ использование долговременных секретных ключей является безопасным, в том числе ключи не повторяются для различных SIM-карт;

- ♦ долговременные секретные ключи неизвестны тому, кто их сгенерировал или инициировал чип-модули для производства SIM-карт, а также исключена возможность передачи ключей третьим лицам;

- ♦ процедура доставки (транспортировки) и загрузки долговременных



секретных ключей, а также регламенты хранения и уничтожения носителей ключей обеспечивают их безопасность и отсутствие возможности утечки.

ПРАКТИЧЕСКИЕ ШАГИ К ЗАЩИЩЁННОЙ СРЕДЕ

Проблемы повышения защищённости российских систем мобильной связи не являются новыми и находятся под пристальным вниманием государственных органов России. В соответствии с решением Совета Безопасности РФ от 01.10.2014 был подготовлен и представлен для согласования в Правительство РФ перечень первоочередных мер, по результатам согласования которого 29 июня 2015 года министром связи и массовых коммуникаций РФ утверждён «План мероприятий, направленных на повышение защищённости систем связи и передачи данных за счёт использования российских криптографических алгоритмов и аппаратных средств».

В рамках практического исполнения указанного Плана по обеспечению информационной безопасности и криптографической защиты отечественных сетей мобильной связи и абонентов в Российской Федерации был реализован проект «Конус», в том числе разработан и создан комплекс встраиваемых средств криптографической защиты на основе двух доверенных элементов безопасности — со стороны абонента и со стороны оператора.

В качестве элемента безопасности со стороны абонента в рамках проекта «Конус» была проведена разработка доверенной сертифицированной SIM-карты, на которой в защищённой среде реализованы отечественные безопасные криптографические алгоритмы аутентификации и согласования сеансовых ключей с использованием надлежащим образом сформированных и записанных в хранилище долговременных секретных ключей. Обеспечено

защищённое хранение и обработка ключевой и иной конфиденциальной информации, в том числе персональных данных, исключая доступ к ним как изнутри, со стороны операционных систем сим-карты и мобильного устройства, установленных апплетов и мобильных приложений, так и извне, через воздействие из канала связи третьих лиц путём подмены сигналов базовых станций и других угроз.

Разработка доверенной защищённой SIM-карты базировалась на основополагающих принципах информационной безопасности Программы «Цифровая экономика», в результате чего обеспечено:

- ♦ использование только отечественного программного обеспечения;
- ♦ использование отечественных методик обоснования безопасности СКЗИ;
- ♦ применение технологий защиты информации (проверки целостности

сообщений, защиты информации от НСД, аутентификации субъектов информационного обмена) с использованием прошедших исследования российских криптографических алгоритмов, в том числе стандартов РФ и алгоритмов, рекомендуемых профильными авторитетными научными сообществами.

В настоящее время доверенная защищённая SIM-карта проходит сертификацию по требованиям информационной безопасности ФСБ и ФСТЭК России.

Со стороны оператора мобильной связи с учётом того, что в ближайшей перспективе сложно рассчитывать на создание и внедрение у операторов связи отечественного оборудования, принципиально важным решением проекта «Конус» является то, что создан отчуждаемый специальный элемент безопасности — отдельный блок HSM (Hardware Security Module — аппаратный модуль безопасности), в который из функций HLR/HSS и AuC «выведены» криптографические функции процедуры аутентификации и долговременные секретные ключи, используемые в этих процедурах. Разработанный модуль HSM обеспечивает хранение долговременных секретных ключей в защищённой среде и использует в своей работе отечественный криптографический алгоритм выработки аутентификационного вектора.

Сертифицированный по требованиям отечественных регуляторов модуль HSM использует при взаимодействии с оборудованием HLR/HSS любого иностранного производителя специально разработанные алгоритмы и интерфейсы, которые даже в случае наличия в оборудовании HLR/HSS недекларированных функций, «бэкдоров» или возникновения инцидентов типа утечки исключают доступ к долговременным секретным ключам или к специальному программному обеспечению.

Таким образом, в Российской Федерации создан определённый научно-технический задел в виде отечественного защищённого и сертифицированного комплекса элементов информационной безопасности (КЭИБ) в составе национальной доверенной SIM-карты и за-

щищённого аппаратного модуля HSM, то есть практически создана платформа для ускоренной и эффективной разработки и реализации отечественных комплексных технологий безопасного и доверенного применения мобильных устройств в системе ПРТС Российской Федерации.

При разработке и создании компонентов КЭИБ были выбраны и реализованы такие универсальные принципы построения и технические решения, которые позволяют использовать создаваемую КЭИБ защищённую среду в качестве доверенного компонента для обеспечения безопасного, надёжного и удобного для пользователей доступа с мобильных устройств к различным цифровым платформам, как уже действующим в России, так и разрабатываемым в рамках программы «Цифровая экономика», включая внедрение мобильной квалифицированной электронной подписи и других перспективных сервисов, что в полной мере способствует выполнению задач, принятых в Дорожной карте программы «Цифровая экономика Российской Федерации», в частности, вопросов обеспечения организационной и правовой защиты государственных интересов в условиях цифровой экономики (пункт 5.11 Дорожной карты).

Такие широкие возможности и перспективы применения КЭИБ определяются двумя важными особенностями построения комплекса:

1. Аппаратное и программное обеспечение КЭИБ, в том числе защищённого аппаратного модуля HSM (что особенно важно), обладают практически неограниченными возможностями модификации и масштабирования для выполнения различных задач по обработке и хранению разнообразной конфиденциальной информации, ключей и сертификатов.

2. Всё размещённое в КЭИБ программное обеспечение и криптографические алгоритмы, выполняемые операции и процедуры, а также данные, обрабатываемые и хранимые в комплексе КЭИБ, весь свой жизненный цикл находятся в доверенной среде КЭИБ, и, таким образом, за счёт применённых сертифицированных аппаратно-программных технических

решений и алгоритмов обеспечена защита практически от любых угроз и нарушителей, включая защиту от вмешательства со стороны спецслужб иностранных государств.

В этой связи обеспечиваемая с помощью КЭИБ доверенная среда в системе отечественной мобильной связи может использоваться для построения самых разнообразных цифровых сервисов и услуг: дистанционное обращение к государственным порталам, проведение операций онлайн-банкинга, нотариальных или иных действий, требующих подтверждения подлинности документов, созданных на мобильных устройствах или с их применением.

КЭИБ представляется ключевым элементом системы обеспечения безопасности, защиты и доверенного доступа с мобильных устройств в корпоративные компьютерные сети государственных организаций и частных структур и, например, для безопасного обращения к ведомственным или корпоративным базам данных, внутренней электронной почте и т.п.

Инфраструктура КЭИБ может обеспечить выполнение процедур доверенной аутентификации мобильного абонента при его обращении за разрешением доступа к ресурсам внутренней компьютерной сети, включая проверку и подтверждение пароля, согласования ключей шифрования трафика и, при необходимости, блокировку доступа при возникновении инцидента.

Поскольку входящий в состав КЭИБ аппаратный модуль доверия HSM обладает значительными аппаратными ресурсами, при определённой доработке модуля часть ресурсов может быть использована для решения других задач защищённого информационного взаимодействия, требующих выработки ключей криптографической защиты и наличия доверенной среды для хранения защищаемых данных.

При этом перенос в доверенную среду КЭИБ дополнительных криптографических функций позволит выполнять в защищённой среде часть критически важных операций, упростить реализацию криптографических технологий и в определённой мере облегчить требования по информационной безопасности.

Применение КЭИБ в системах обеспечения комплексной информационной безопасности и защиты компонентов российских критически важных инфраструктур, в том числе использующих сети ПРТС, позволит за счёт использования безопасных отечественных криптографических алгоритмов и обработки защищаемых данных в доверенной среде исключить негативное воздействие значительного числа внутренних и, что особо важно, внешних угроз и нарушителей, в том числе исключить возможность воздействия на российские критически важные инфраструктуры со стороны иностранных фирм и спецслужб зарубежных государств, которое они могут пытаться реализовать как напрямую через сети ПРТС, так и через «бэкдоры» и недекларированные функции, заложенные в оборудовании и программных продуктах иностранного производства, используемых в России.

ДРУГИЕ ЗАДАЧИ

Кроме того, как показывают результаты проводимых в настоящее время НИР, комплекс КЭИБ благодаря техническим решениям, заложенным при его разработке, позволяет обеспечить безопасную доверенную среду при реализации многих других важных информационных, социальных и политических мероприятий на базе или с использованием отечественных сетей мобильной связи, например, таких как проведение дистанционных электронных голосований (ДЭГ) на выборах и референдумах различного уровня от муниципальных до федеральных.

В этой сфере применения комплекс КЭИБ обеспечивает не только техническую возможность осуществления дистанционного волеизъявления граждан (с помощью персональных мобильных устройств) при соблюдении системы мер доверенной аутентификации, подтверждения выбора с помощью безопасных алгоритмов усиленной квалифицированной электронной подписи и криптографической защиты сообщений, но и путём присоединения к безопасной среде цифрового доверия аппаратных модулей HSM, выполняющих функции формирования электронных избирательных бюллетеней,

их доставки/приёма участникам ДЭГ, проверки целостности, накопления, обезличивания, обработки, а также верификации и подсчёта голосов, поданных дистанционно в электронном виде.

Доверенная среда хранения и обработки данных с использованием безопасных криптографических функций и алгоритмов в составе КЭИБ обеспечивает выполнение требований российских нормативных актов в части хранения и обработки данных, которые могут быть отнесены к персональным, что позволяет использовать защищённый аппаратный модуль HSM для хранения и обработки данных клиентов финансовых учреждений, включая цифровые образы биометрии, а также долговременные секретные ключи, сертификаты и другие данные, необходимые для аутентификации клиентов финансовых учреждений и авторизации, удалённого доступа к счетам клиентов.

Решения КЭИБ за счёт своей универсальности и высокого уровня безопасности уже в ближайшее время могут быть внедрены, в частности, в действующие и перспективные системы навигации, включая систему «Эра-ГЛОНАСС» и проектируемую в Российской Федерации защищённую систему локальной навигации и позиционирования.

Кроме того, концепция и решения, реализованные в аппаратном модуле безопасности КЭИБ, позволяют использовать такие модули в качестве базовых для своевременных комплексных мер по обеспечению безопасности и защиты российских сетей, сервисов и персональных данных абонентов, для разработки доверенных средств и криптографических систем для перспективных направлений развития систем коммуникации и связи в Российской Федерации, включая сети поколения 5G, технологии «интернет вещей», «умные города» и т.п.

Важным условием для эффективной и успешной практической реализации мер по обеспечению безопасности отечественных сетей мобильной связи на базе российских сертифицированных элементов безопасности КЭИБ является правовое обеспечение, что предполагает разработку и принятие необходимых изменений и дополнений в

отечественную нормативно-правовую базу, определяющую порядок работы сетей ПРТС и её элементов, предоставление услуг и сервисов и порядок взаимоотношения участников экосистемы ПРТС.

Кроме того, необходимо в кратчайшие сроки определить перечень и содержание проектов новых нормативных документов, отражающих актуальные и перспективные требования по обеспечению безопасного функционирования новых технологий, сервисов и услуг на основе ПРТС, включая перспективные сети 5G.

При этом следует учитывать, что, как показывает опыт работы по внесению дополнений и изменений в нормативно-правовую базу для внедрения в сетях ПРТС отечественного аппаратного модуля безопасности HSM, а особенно доверенной SIM-карты, процесс подготовки, согласования и принятия нормативно-правовых актов и изменений к ним вследствие многоэтапных процедур межведомственного согласования является сложным, что значительно удлиняет временной интервал от готовности разработки к серийному производству до её практического внедрения и достижения конкретного значимого результата по обеспечению безопасности и защищённости отечественных сетей ПРТС и их абонентов.

* * *

Однако даже с учётом возможных временных задержек внедрения вследствие длительности согласовательных процедур нормативно-правовой базы реализация концепции повышения безопасности российских ПРТС путём применения отечественного защищённого и сертифицированного комплекса элементов безопасности в составе национальной доверенной SIM-карты и защищённого аппаратного модуля HSM является наиболее эффективным и действенным комплексом мер по уровню получаемого результата как с точки зрения защищённости и безопасности, так и с точки зрения требуемого времени на внедрение, оптимальных финансовых и трудовых затрат.

«Событиям юбилейного года, адресованным детям и юношеству, нужно уделить самое пристальное внимание. Их цель — не только просветить, но и вовлечь молодёжь в изучение и сохранение истории своей семьи и Родины в целом. Для этого следует искать и показывать примеры ещё не известных героев Великой Отечественной, о чьих подвигах знают пока только страницы архивных документов, запускать тематические конкурсы, опросы, используя популярные социальные сети...».

Президент России В. Путин



Артём ЗУБКОВ

директор Фонда содействия развитию безопасных информационных технологий (ФСРБИТ)



Всеволод БЫЛЕВСКИЙ

директор по развитию BIS TV, к.ф.н.

«И НЕ ПОВЕРИТСЯ САМИМ...»

ВСЕРОССИЙСКИЙ КОНКУРС ПРОЕКТНО-ИССЛЕДОВАТЕЛЬСКИХ РАБОТ ШКОЛЬНИКОВ «ШИФРЫ ПОБЕДЫ»

В феврале 2021 года Фонд содействия развитию безопасных информационных технологий (ФСРБИТ) начал новый проект «Криптографический фронт: виртуальный музей»¹. Основная идея проекта состоит в организации коллективной работы по созданию виртуального музея, посвящённого одной из малоизвестных сторон Великой Отечественной войны — достижениям шифровальной и радиоразведывательной служб СССР, их вкладу в Победу.

В современной России историческая память о Великой Отечественной войне является мощным ресурсом патриотического и гражданского развития. Вместе с тем в медийном поле сформировано преимущественно

одностороннее представление о научных и технологических факторах, повлиявших на ход Второй мировой войны. Этому способствовала и сложившаяся в СССР практика тотального засекречивания архивных материалов о деятельности криптографической службы, подразделений шифрованной связи и радиоразведки.

При этом очевиден интерес молодёжи к вопросам безопасности информации. Школьники 8–11-х классов активно участвуют в проводимой более 30 лет олимпиаде по криптографии им. И. Я. Верченко (число участников около 4000 ежегодно, очный тур проводится на площадках более 40 городов). Специально подготовленная Фондом к юбилею Победы в 2020 году видеозадача о шифровании метеосводок в период войны для олимпиады «Готов к жизни в умном городе!» вызвала отклик и в более младшей возрастной группе.

В части проектно-исследовательской деятельности в области истории криптографии отметим опыт проведения в 2007 году конкурса проектов к 100-летию И. Я. Верченко, а также постоянный интерес к этому направлению учителей-предметников. Анализ подобных работ показывает, что большинство из них опирается на зарубежную фактологию и нередко содержит наивные ошибочные трактовки фактов из области криптографии. При этом сведения о деятельности отечественных криптографов отражаются на весьма абстрактном уровне, а материалы военных архивов практически не используются.

Тем самым можно констатировать необходимость соответствующей трансформации медийного поля. Опыт проведения Фондом в 2018–2020 гг. в нескольких городах серии лекций и квестов для школьников по тематике «Криптографический фронт Великой Отечественной» показыва-

¹ Проект поддержан грантом Президента Российской Федерации на развитие гражданского общества № 21–1–009977, предоставленного Фондом Президентских грантов.

Из поздравления сотрудникам и ветеранам криптографической службы России:

«Особо отмечу огромный вклад, который внесли криптографы в достижение Великой Победы. Во многом благодаря их компетентности, ответственности и личному мужеству была обеспечена надёжная зашифрованная связь, в том числе в ходе переломных битв и сражений».

Президент России В. Путин, 5 мая 2021 года

<http://kremlin.ru/events/president/letters/65527>

ет наличие исторического материала о криптографической деятельности, адекватного для восприятия учащимися 8–11-х классов. Собственно, середина XX века — последний период, когда суть применявшихся средств шифрования ещё доступна для понимания без специального образования.

Целью проекта «Криптографический фронт: виртуальный музей» является содействие патриотическому воспитанию молодёжи через вовлечение в сохранение исторической памяти о криптографической и радиоразведывательной деятельности в период Великой Отечественной войны, а его содержательным ядром — поиск в интернет-архиве «Память народа»² документальных материалов для экспозиции виртуального музея.

В рамках проекта организован Всероссийский конкурс проектно-исследовательских работ «Шифры Победы».

Его весенний этап 2021 года завершён в мае, когда отмечались и День Победы, и 100-летие криптографической службы Российской Федерации. К участию приглашались команды учеников 7–10-х классов. Проекты выполнялись под руководством учителей. Всего приняли участие более 80 команд из различных регионов России.

Основное содержание работы участников заключалось в поиске на интернет-портале «Память народа» архивных документов, отражающих различные аспекты криптографической деятельности подразделений Красной армии в 1941–1945 гг. Всего командами было найдено более 8000 таких документов, среди них — инструкции по способам шифрования сообщений и кодирования топографических карт, шифротелеграммы и кодограммы, расписания ключей. Для многих документов созданы карточки-описания, дополняющие с учётом предметной области карточки архива «Память народа». Результаты проделанной школьниками работы представлены

в виде базы данных, она размещена в открытом доступе на сайте конкурса (музейкриптографии.рф). Такая организация работы позволила объединить усилия большого числа участников. Систематизация ссылок на архивные документы позволяет выявлять интересные связи между ними, в том числе хранящимися в разных частях архива. Кроме того, создаются предпосылки для введения в научный оборот новых исторических документов. То есть документ, конечно, уже есть в архиве, но из-за шифрования нет доступа к части или ко всему содержанию сообщения, в том числе к сведениям о его авторах и упоминаемых воинских частях, месте событий.

Специальной подготовки (в области программирования, математики, истории или архивного дела) для участия в конкурсе не требовалось, достаточно было общих навыков работы в интернете. Следует отметить, что поиск и анализ информации в ходе конкурса во многом аналогичен подходам,

² <https://pamyat-naroda.ru/documents/>



Тематический квест (Центральный музей Вооружённых сил РФ, 19 мая 2021 года)



Торжественное награждение участников Московского региона (Центральный музей Вооружённых сил РФ, 19 мая 2021 года)

применяемым в конкурентной разведке в интернете. Имеется большой массив данных в открытом доступе, но, как всегда, имеются и пропуски, опечатки и ошибки метаданных. Поиск зависит от предметной области, без понимания которой не получится составлять результативные поисковые запросы.

Методическая поддержка школьников и руководителей команд обеспечивалась серией вебинаров об основных понятиях криптографии, способах поиска на портале «Память народа», а также консультаций по вопросам участия в конкурсе. Кроме того, для участников конкурса в интернет-формате проведена тематическая викторина (квиз) и подготовлены две видеолекции, их записи размещены на BIS TV.

Торжественное награждение участников Московского региона проведено на базе Центрального музея Вооружённых сил РФ 19 мая 2021 г. В ходе меропри-

ятия школьники прослушали краткую лекцию к 100-летию криптографической службы РФ и приняли участие в тематическом квесте. Для решения его заданий 12 командам (68 чел.) потребовалось реконструировать по розданным архивным документам и топографическим картам два применявшихся в период Великой Отечественной войны шифра. Это оказалось довольно непростой задачей для школьников. Мероприятие проводилось при спонсорской поддержке компании «Код Безопасности».

В ходе проекта издана книга Столпакова Б. В., Никонова Н. В. «Просто о важном. Экскурсия в криптографию без формул». Экземпляры вручались победителям и призёрам конкурса, а тем, кто не смог принять участие в очном формате, разосланы по почте вместе с дипломами. Кроме того, в школы, представленные активно участвовавшими командами, направлены благодарственные письма.

Результаты проведения конкурса следующие. Более 200 школьников смогли в ходе практической деятельности познакомиться с подлинными документами периода Великой Отечественной, отражающими и ход боевых действий, и применявшиеся в то время технологии защиты информации. Создан задел документальной информации для экспозиции виртуального музея «Криптографический фронт».

* * *

Методические наработки по организации конкурса «Шифры Победы» будут развиты в осеннем семестре, а материалы квизов и квеста могут быть предоставлены заинтересованным образовательным организациям для использования в военно-патриотической работе.

**Сергей НЕЙГЕР**директор по развитию бизнеса
компании «Перспективный
мониторинг»

КИБЕРПОЛИГОН AMPIRE

ПОМОГАЕТ ЛЮДЯМ УЧИТЬ ЛЮДЕЙ

ПЯТЬ ЛЕТ ПЕРВЫМ ПРОТОТИПАМ

Ampire — это целая экосистема программных технологий, которая позволяет обучать пользователей методам обнаружения признаков компьютерных атак, анализировать причины их возникновения и, в конечном счёте, внедрять защитные меры для противодействия им. Компания «Перспективный мониторинг» начала разрабатывать первые прототипы киберполигона Ampire в 2016 году. ПМ — пионеры киберучений на специализированных платформах в России. Как коробочный продукт Ampire появился в 2018 году. В 2020 году начались подключения к полигону по модели SaaS.

Основная задача, которая легла в основу идеи разработки Ampire — практическая подготовка специалистов по информационной безопасности, с основным уклоном на работу в центрах мониторинга информационной безопасности (инхауз и аутсорсинговых SOC).

Везде, в любом регионе страны, специалисты по ИБ высказывают одну и ту же мысль: «Мы хотим построить службу мониторинга событий и реагирования на инциденты, но людей нет». И нет центров компетенций, где

таких сотрудников можно было бы готовить. «Перспективный мониторинг» как разработчик киберполигона хочет дать возможность специалистам по ИБ обучать новых специалистов в условиях, приближённых к реальной инфраструктуре организации и её процессам.

ОПЫТ ЗАНЯТИЙ

Очевидно, что без технического и методического обеспечения центр мониторинга не может работать. И сотрудники также должны обладать необходимыми навыками. «Жёсткие» навыки (те, которым можно научить и которые можно измерить) для сотрудников службы мониторинга — это знание технологий атаки и защиты, знание и умение применять средства защиты информации и другие инструменты. Личные качества (т.н. soft skills) — навыки командной работы, умение взаимодействовать с другими членами группы мониторинга и реагирования на инциденты, навыки тайм-менеджмента.

Те люди, которые проходят занятия на Ampire, повышают практические навыки противодействия компьютерным атакам. В ходе занятий акцент делается именно на практику:

- ♦ работа с различными средствами обнаружения атак;

- ♦ анализ логов прикладных сервисов (веб-сервера, базы данных, удалённые средства управления и т.д.);

- ♦ навыки устранения уязвимостей с помощью настройки сервисов, изменения на уровне сети виртуальной организации, внедрения межсетевых экранов, правки исходного кода и т.п.;

- ♦ навыки совместной работы при расследовании инцидентов ИБ.

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

ВНУТРЕННЕЕ УСТРОЙСТВО

Киберполигон Ampire (Cyber Range в терминологии Gartner) содержит в себе несколько необходимых для подготовки специалистов элементов. В первую очередь это модели различных информационных систем общего и отраслевого назначения. Понятно, что для тренировок необходима инфраструктура, повторяющая технологии и сервисы реальных организаций. Данная задача решена в Ampire путём создания отраслевых ИТ-шаблонов. Те люди, которые приходят заниматься на платформе, могут не бояться что-то случайно сломать — у них развязываются руки, появляется возможность экспериментов и проверки гипотез, снимается блок «а вдруг я что-то сделаю не так и всё рухнет».

Обычно участники киберучений на Ampire примеряют на себя две

Везде, в любом регионе страны, специалисты по ИБ высказывают одну и ту же мысль: «Мы хотим построить службу мониторинга событий и реагирования на инциденты, но людей нет»



Киберучения в Волгограде 21 октября 2021 года

роли — сотрудников групп мониторинга и реагирования. Группа мониторинга следит за событиями информационной безопасности, которые фиксируются интегрированными средствами защиты информации различных вендоров. Это могут быть сетевые и хостовые СОА/СОВ, антивирусные средства, SIEM системы, анализаторы логов систем и приложений.

Чтобы учиться противостоять компьютерным атакам нужна эта самая компьютерная атака. В Amprige роль атакующего автоматизирована, хотя есть возможность пригласить и живых людей в качестве RedTeam. Автоматический нарушитель реализует различные сценарии действий атакующего, характерные для шаблона информационной системы. Такие сценарии разрабатывают пентестеры и аналитики коммерческого SOC «Перспективного мониторинга». Киллер-фича последнего стабильного релиза платформы — **конфигуратор**

сценариев тренировок. Благодаря ему преподаватель может самостоятельно, не обладая навыками программирования, в веб-интерфейсе платформы самостоятельно создавать и редактировать сценарии компьютерной атаки на инфраструктуру. В конфигураторе произвольно меняются не только вектора атак и способы эксплуатации уязвимостей, но и состав ИТ-инфраструктуры, на которой проходит занятие.

Разработчики Amprige позаботились и о преподавателях. В новой версии стали более удобными системы управления занятиями и пользователями, появилась расширенная статистика по занятиям и студентам.

ПМ РАЗРАБАТЫВАЕТ, УНИВЕРСИТЕТЫ УЧАТ

Amprige — это решение, у которого есть уже 4 коммерческих внедрения на российском рынке: вуз силового ведомства; РГУ нефти и газа (НИУ) имени

И.М. Губкина; РТУ МИРЭА; вуз, учреждённый Министерством цифрового развития, связи и массовых коммуникаций РФ.

Эти учебные заведения активно эксплуатируют Amprige, обучают собственных студентов и оказывают услуги по дополнительному профессиональному обучению.

* * *

Что главное, когда сталкиваешься с компьютерной атакой в реальном времени? Оснащённость техническими средствами защиты? Принятые в организации политики безопасности? Плейбуки по реагированию на инциденты? Это всё нужно. Но главное — не паниковать. Если специалист знает, что делать, и умеет нажимать нужные кнопки, тогда организация сможет справиться с атакой с наименьшими потерями.

ПРИЁМНАЯ КАМПАНИЯ — 2021. БЫЛО НЕ СКУЧНО

COVID-19, НОВЫЕ ПРАВИЛА И ГРЯДУЩИЕ
ИЗМЕНЕНИЯ В ПОРЯДКЕ СДАЧИ ЕГЭ



Марина БРОДСКАЯ
обозреватель
BIS Journal

В 2020 году был сдвинут традиционный график работы приёмных комиссий, и зачисление на первый курс происходило в последние дни лета, а по дополнительному набору и вовсе ушло в осень. В августе прошлого года Министерство науки и высшего образования утвердило новый порядок приёма на обучение по программам бакалавриата, специалитета и магистратуры, который начал действовать в 2021/2022 учебном году. Учебные заведения получили больше прав и свобод при приёме абитуриентов.

НОВЫЕ ПРАВИЛА

Согласно нововведениям, абитуриент мог подать документы в 5 университетов, при этом выбрав до 10 направлений (вместо прежних трёх) в каждом из учебных заведений. Университеты получили право проводить единый конкурс по нескольким родственным специальностям и выбирать сильных абитуриентов на глобальное направление обучения в целом, а деление на специализации проводить позже.

Университеты самостоятельно устанавливали вступительные испытания по нескольким предметам на выбор. И абитуриент мог выбрать, результат ЕГЭ по какому предмету даст больше шансов попасть на выбранное направление. Например, в большинстве университетов при поступлении на специальность «информационная безопасность» можно было выбрать один из профильных предметов — физику или информатику, и 39 баллов по физике приравнивались к 45 по информатике. В ряде вузов учитывались баллы по иностранному языку или химии.

Университеты получили право регулировать требования к минимальным баллам для тех, кто поступает на бюджет, а кто на платное обучение. При этом число платных мест ничем не лимитировано, тогда как план приёма на бюджет строго регламентирован приказами и согласованиями.

Новыми правилами уточнены требования к баллам за индивидуальные достижения. Многие вузы внесли изменения в правила приёма и ввели дополнительные вступительные испытания для победителей и призёров олимпиад. Также были уточнены требования и по числу мест в пределах квот приёма на обучение по программам бакалавриата и специалитета за счёт бюджета. Не менее 10% мест на бюджете отдано лицам, имеющим особое право на приём. Число мест по целевому обучению определяется вузом самостоятельно или устанавливается учредителем. При этом во многих вузах был проведён отдельный конкурс для претендентов на места по целевому обучению. Также университеты получили право самостоятельно утверждать перечень предметов для внутренних вступительных экзаменов для поступления в вузы выпускников колледжей и техникумов.

ЧТО ПОЛУЧИЛОСЬ НА ПРАКТИКЕ?

Многие абитуриенты подали документы, как и разрешено правилами, сразу в несколько учебных заведений. Но одновременно с этим они дали согласие на зачисление сразу всем, а не одному-единственному университету. В результате при зачислении они оказались в списках сразу нескольких вузов, что привело к нарушениям и бесконечным внесениям изменений в приказы: одних отчисляли, других,

не прошедших по конкурсу, возвращали в списки на освободившиеся места.

Неразбериху внёс и единственный этап приёма. Несмотря на уточнение списков несколько раз в день, многие потенциальные первокурсники-середнячки так и не смогли оценить свои шансы на зачисление в конкретный университет: сложно угадать, куда пойдут конкуренты с высокими баллами, даже после публикации приказов о зачислении принятых вне конкурса. Кому-то повезло, и он смог переложить согласие на зачисление в тот единственный вуз, куда реально пройти на бюджет. У кого-то не выдерживали нервы, и документы перекладывались на платное отделение. А кто-то остался за бортом, не найдя своё имя в приказах о зачислении. Впрочем, и многие университеты обнаружили, что не все места заняты первокурсниками. О дополнительном наборе на первый курс, в том числе на бюджетные места, по окончании приёмной кампании объявили многие столичные и региональные вузы.

После выхода публикации «Вузы ищут себе абитуриентов» в газете «Коммерсант» в СМИ появились комментарии со ссылкой на министра науки и высшего образования Валерия Фалькова, что порядок приёма может быть пересмотрен после обсуждения со всеми заинтересованными сторонами: абитуриентами, родителями и представителями учебных заведений. При этом министр видит преимущества как в действующем порядке приёма, так и в старом, в два этапа. Одновременно глава Минобрнауки заявил о необходимости поднять престиж региональных университетов и ужесточить требования к олимпиадам. Не секрет, что в большинстве учебных заведений основная масса бюджетных

мест уходит без конкурса победителям и призёрам различных олимпиад.

ЧЕМ ЗАПОМНИТСЯ?

Чем ещё запомнится эта приёмная кампания? Возможно, тем, что она пришлась на очередную волну пандемии и соответствующих ограничений, а также тем, что многие выпускники заболели COVID-19 и едва успели сдать профильные предметы в резервный день. А кто-то будет вынужден сдавать ЕГЭ на следующий год. Депрессия — ещё одно последствие COVID-19, которое отразилось на результатах госэкзаменов. Знаю выпускников, которые, переболев весной, не успели морально и физически восстановиться к лету. Итог — невысокие баллы по ЕГЭ и зачисление на платной основе (спасибо родителям).

А может, кампания запомнится тем, что в МГУ поступила девятилетняя Алиса Теплякова, сдавшая выпускные экзамены в 7 лет и из-за бюрократических проволочек получившая аттестат лишь год спустя. Девочка сдала вступительные экзамены в МГУ на факультет психологии и в 9 лет была зачислена на платное отделение, поскольку не набрала баллов на бюджет. Как и чему ребёнок будет учиться среди сокурсников, которые значительно старше его, пока сказать сложно. Но отец Алисы уже заявил, что бакалавриат она закончит за два года.

И здесь вновь хочется поднять вопрос о требованиях к минимальным баллам по ЕГЭ, с которыми можно подавать документы на платное отделение. Например, в том же МГУ на факультете психологии будут одновременно учиться те, кто набрал 370–389 баллов, и обладатели 200 баллов по 4 предметам. Правом ввести нижний порог баллов воспользовался МИФИ, здесь принимают на платное отделение с итогами ЕГЭ не ниже 200 баллов. Притом что проходной балл на бюджетное отделение чуть ниже: в приказе о приёме есть обладатели и 183 баллов. Может быть, по этой причине приём на платное отделение в МИФИ был продлён до 27 августа.

10.00.00: ВСЁ ПО-ПРЕЖНЕМУ

Если обратить внимание на ситуацию по пополнению кадров в сфере ИБ, то никаких кардинальных изменений

и потрясений в этом году не случилось. Специальности по направлениям «информационная безопасность» (10.00.00) пользуются популярностью у абитуриентов и, в отличие от других направлений IT, донбора в этом году, в отличие от специальностей по направлению 09.00.00 «информатика и вычислительная техника», не было. Большинство университетов, где есть специальности по направлениям «Информационная безопасность», требовали от абитуриентов не менее 39 баллов по математике, 39 по физике (или 44 по информатике) и 40 — по русскому. Но были и исключения: в НЯУ МИФИ надо было иметь не менее 68, а по ряду специальностей — 76 баллов по математике. Повышенные требования к царице наук выдвигают НИУ МФТИ, ВШЭ, МВТУ им. Баумана и СПбПУ. Они же требуют высоких знаний по информатике или физике, а также по русскому языку.

Таким образом, несколько престижных вузов оттягивали на себя сильных абитуриентов, и минимальный проходной балл в эти учебные заведения приблизился к максимально возможному с учётом индивидуальных достижений поступающего. Однако, как обычно, в ведущие университеты по общему конкурсу зачислялись единицы — все места заняли победители олимпиад и поступавшие в рамках особых квот и целевого набора.

Твёрдые хорошисты — обладатели порядка 250 баллов — поступили в столичные и региональные технические вузы, а в большинстве региональных университетов можно было поступить на ИБ-направления на бюджет и заурядному троечнику. А на платных отделениях часто достаточно было просто принести аттестат и минимальные баллы по ЕГЭ.

Несмотря на разгоняющуюся инфляцию, в большинстве университетов постарались сохранить прошлогодний уровень цен. Где-то подняли цены для вновь поступивших на 1 курс на 10 тыс. руб. за год, где-то на 30 тыс. руб., а где-то сохранили цены на уровне 2020 года. На 50 тыс. руб. подорожала учёба в ВШЭ по специальности «компьютерная безопасность» (10.05.01), одновременно с этим вырос и проходной

балл — с 278 в прошлом году до 291 в 2021 г.

Сколько из поступивших в этом году студентов успешно завершат учёбу и будут работать по специальности? Вопрос риторический, поскольку ни один вуз не раскрывает контрольные цифры выпуска.

ОТНОСИТСЯ К ТЕМЕ

«В ближайшие три года задания ЕГЭ по большинству школьных предметов претерпят изменения», — заявил руководитель Рособнадзора Анзор Музаев на Общероссийском родительском собрании. По словам чиновника, основные изменения будут направлены на то, чтобы учащиеся не только заучивали учебный материал непосредственно перед испытаниями, но и позже могли применять полученные в школе знания на практике.

Глава комитета Госдумы по информационной политике, информационным технологиям и связи Александр Хинштейн настаивает на необходимости введения в школах курсов по информационной безопасности в интернете, сообщает радиостанция «Эхо Москвы».

В финале IX Национального чемпионата «Молодые профессионалы», который прошёл в Уфе в конце августа, обсудили подготовку сотрудников информационной безопасности, передаёт агентство «Амур Инфо». По словам советника Московского института электроники и математики имени А.Н. Тихонова НИУ ВШЭ Антона Сергеева, в этом году Минтруд сообщил о нехватке в России 18 тыс. специалистов по ИБ. Всего же в мире насчитывается от 3 до 3,5 млн вакансий в сфере кибербезопасности. По словам Сергеева, только один из четырёх специалистов по кибербезопасности обладает всеми профессиональными навыками. Нет и национальных стандартов оценки квалификации для негосударственных специалистов. Проблема не только в нехватке кадров, но и в быстрой смене технологий, требований, оборудования и ПО. «Это значит, что необходимо постоянно обновлять и образовательные программы, а также их систему оценивания», — отметил эксперт.

МГЛУ — BIS JOURNAL: ДИАЛОГ ДРУЗЕЙ

СТУДЕНТЫ ОТКРЫВАЮТ НОВУЮ РУБРИКУ — КИБЕРОБЗОР ИНОСМИ

Что такое информационная безопасность для современной молодёжи? Как они её понимают? В рамках творческого сотрудничества BIS Journal предложил будущим переводчикам — студентам-второкурсникам МГЛУ (Иняз им. Мориса Тореза) — подобрать в СМИ разных стран примеры сообщений о киберинцидентах и по возможности их прокомментировать. Эксперимент оказался успешным: редакция получила сотни примеров, из которых после фильтрации получился довольно насыщенный информационный коктейль — своеобразный гибрид дайджеста и обзора международной прессы.

ПРО ИДЕОЛОГИЮ

Железный занавес как ИБ. В декабре 2020 г. в КНДР введён закон о противодействии реакционной культуре и идеологии, запрещающий жителям КНДР использование, просмотр, хранение и передачу любого культурного контента Южной Кореи. Нарушителям грозит наказание вплоть до смертной казни или лишения свободы до 15 лет, сообщает информационное агентство «Рёнхп» в переводе Анастасии Власовой.

Власти КНДР всерьёз взялись за усиление идеологической работы среди молодёжи. Накануне отмечаемого 28 августа Дня молодёжи в газете «Нодон синмун» вышла статья о важности и значимости идеологии для поколения МЗ (в северокорейском варианте «поколение чанмадан» — рождённые в 1990–2000 гг.). Авторы публикации призывают молодых людей «стать настоящими хозяевами социалистической морали и культуры», иначе «общество будет не в состоянии существовать и развиваться».

«Молодые люди, подверженные скверному влиянию индивидуалистической капиталистической морали и западных культурных ценностей, становятся морально больными и умственно искалеченными, стремятся исключительно к собственному комфорту и удовольствиям и в итоге превращаются во врагов революции и социализма». Именно поэтому, по мнению авторов, основной причиной краха социалистических режимов в XX веке стала «молодёжь, ослеплённая подобными веяниями».

На Ближнем Востоке. Панарабская сеть «Аль-Джазира» сообщила, что летом 2021 г. она подверглась серии

кибератак. И не только она: хакеры пытались нарушить работу нескольких информационных платформ. Пик атак случился накануне показа документального фильма о переговорах между ХАМАС и Израилем. Многие арабские СМИ расценивают работу «катарского канала» по освещению событий на Ближнем Востоке как подстрекательство, читал арабскую прессу Лев Кутовский. По совокупности впечатлений он предположил, что за кибератаками стоят специалисты арабских стран. В то же время, по его мнению, сравнительно небольшое количество новостей о кибератаках в арабском мире говорит о том, что переход на новый уровень ведения войн в регионе только начинается.

О ПРОМЫШЛЕННОМ ШПИОНАЖЕ

Север против Юга. Хакеры из КНДР совершили кибератаку на фармацевтическую компанию Pfizer и предприняли попытку украсть материалы о вакцине от COVID-19, сообщают спецслужбы Южной Кореи через статью в *Washington Post*, которую перевёл Александр Волобуев. Статья, по его мнению, голословная. Информации, была ли атака успешной, найти в ней не удалось, комментариев компании Pfizer тоже. Зато присутствует утверждение южнокорейских спецслужб, что киберактивность со стороны КНДР выросла за последний год на 32%. Используя фишинговую рассылку, идеологические противники с севера совершили ряд кибератак на биофармацевтические компании юга, в том числе на AstraZeneca. Зачем они это сделали, не объясняется, хотя намёк прозрачен: хотят украсть вакцину для тоталитарного режима. При этом каких-либо официальных данных о



заражениях COVID-19 в КНДР тоже не приводится...

7 тыс. «одарённых». Или «обоюдоострых мечей»? Ежедневно на государственные учреждения Южной Кореи проводится около 1,6 млн кибератак, более 90% из которых — работа хакеров из КНДР, сообщает *информационный портал Naver.com в переводе Дианы Тарасовой*. Весной они атаковали СМИ, прервав работу одной из телекомпаний страны. 30 июня взломали защиту аэрокосмической и оборонной компании KAI, разрабатывающей истребитель нового поколения KF-21.

Главными подозреваемыми являются 7 тыс. «одарённых» хакеров из КНДР.

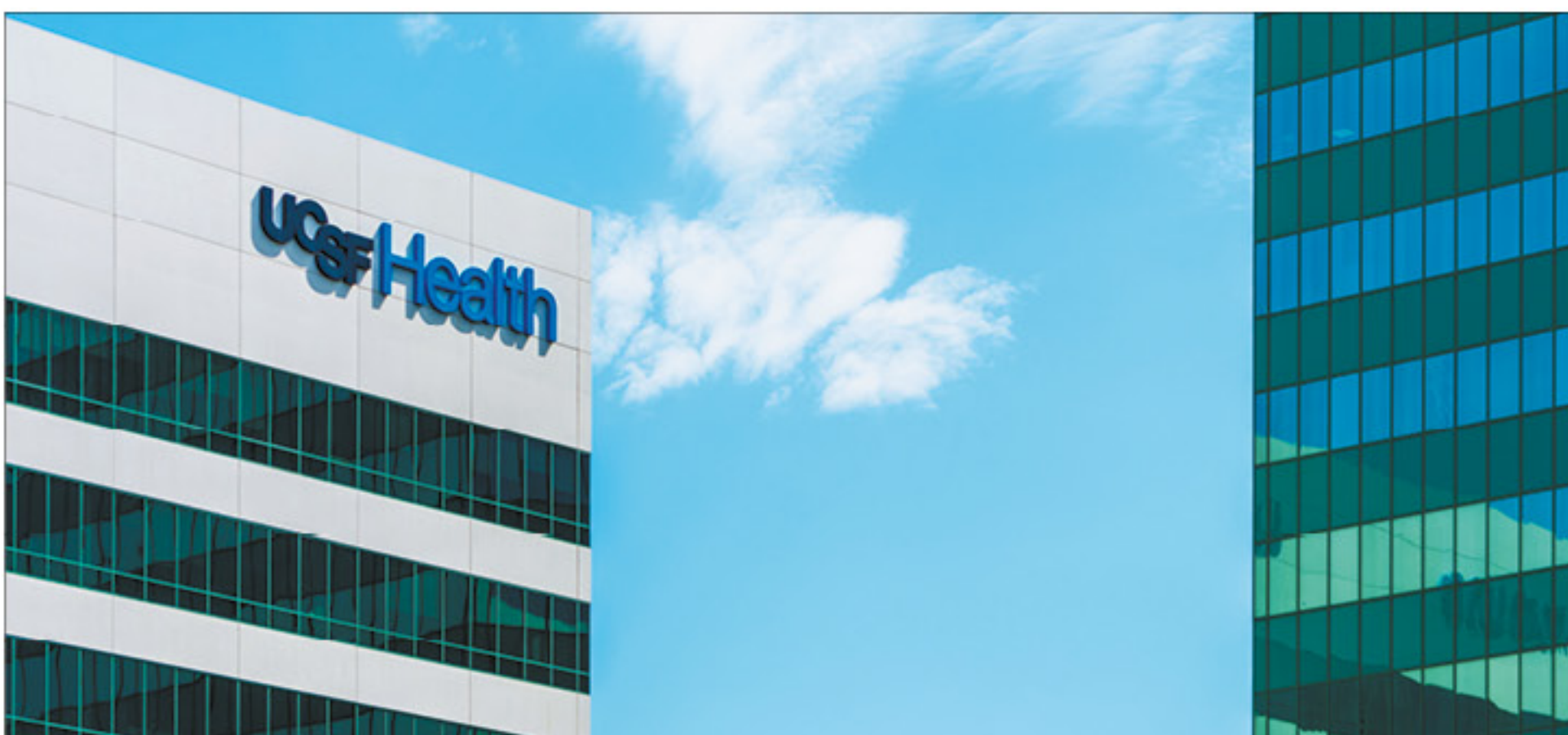
Ещё одну атаку — на банки США в мае 2021 г. — также приписывают «одарённым». Считается, что украденные деньги были использованы для финансирования ядерной программы КНДР.

Кто такие эти «одарённые»? Неподтверждённая легенда гласит: Северная Корея проводит отбор детей, которые проходят спецобучение на элитных курсах в Университете Ким Ир Сена и Индустриальном университете Ким Бука. Несколько северокорейских хакерских организаций базируются в КНДР в статусе генерального бюро разведки КНДР. Эксперты называют их «обоюдоострыми мечами».

Университеты. Запретам вопреки. Хакерам удалось получить \$ 1,14 млн от Калифорнийского университета (UCSF), работающего над лекарством от COVID-19. Деньги были переданы в ходе тайных переговоров, доступ к которым получили корреспонденты BBC (*перевод Маргариты Гуньковой*).

Нападение на сети университета произошло 1 июня 2021 г. Считается, что за атакой стояла группировка Netwalker, она же причастна к другим кибератакам на университеты США. UCSF пошёл на уступки и выплатил часть требуемой суммы в обмен на инструмент для разблокировки данных.

Даже частичный выкуп противоречит политике спецслужб, настаивающих на запрете финансирования хакеров, однако подобные переговоры ведутся по всему миру. И жертв можно понять — порой у организаций нет выбора, чтобы вернуть зашифрованные данные и возобновить рабочий цикл.



В настоящее время UCSF помогает ФБР в расследовании инцидента и работает над восстановлением систем.

Не хакеры, а мошенники. В конце июля нефтяная компания Saudi Aramco сообщила об утечке данных. Вымогатели требовали \$50 млн выкупа за неразглашение. По словам хакеров, они похитили у Saudi Aramco около 1 Тб данных, среди которых информация о сотрудниках, проектах, счетах и т.д.

Saudi Aramco не стала выплачивать выкуп, посчитав данную информацию частью утечки 2020 г., произошедшей у одного из подрядчиков, и назвала хакеров мошенниками. Как показало расследование, представители Aramco были правы, сообщает *Bloomberg в переводе Олеси Романовской*.

Компания уже имеет опыт работы с хакерскими атаками. В 2012 г. сеть компании поразил вирус, удаливший данные с жёстких дисков. Тогда компания была вынуждена отключить всю сеть и уничтожить порядка 30 тыс. компьютеров.

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

В КНР принят новый закон. Китайские власти приступили к модернизации законодательства в сфере персональных данных. Ранее изданные законы «Об информационной безопасности», «О кибербезопасности» и гражданский кодекс КНР были объединены в «Закон о защите персональных данных». Закон был принят 20 августа и вступит в силу 1 ноября 2021 г. Его прочла и проанализировала Анна Акилина. По её словам, Закон направлен на борьбу с «монополией на информацию», незаконным хищением и

уничтожением данных, а также на обеспечение честного использования данных обработчиками.

По мнению властей, меры по контролю данных должны способствовать повышению благосостояния граждан, а также помогать им понять вопросы обеспечения информационной безопасности. Ответственные лица и организации теперь обязаны на регулярной основе предоставлять отчёты о нарушениях ИБ и возможных системных рисках.

Нарушение закона будет караться штрафами от 10 тыс. до 10 млн юаней. Компании, причастные к нарушениям, рискуют потерять лицензию на осуществление коммерческой деятельности или будут закрыты.

Таким образом, китайские власти не только усиливают контроль над обработкой и передачей персональной информации, но и пытаются принудить компании отчитываться о клиентах. Сторонние наблюдатели видят в этом стремление правительства КНР отслеживать действия своих граждан. Возможно, в дальнейшем статьи закона будут привязаны к новым системам социального кредита, влияние которого постепенно распространяется на всех граждан Китая.

Сектор Газа. Задел на будущее. Пропалестинские хакеры группировки DragonForce Malaysia украли персональную информацию сотен тысяч израильских студентов и обнародовали её в своём Telegram-канале. Данные включают имена, номера телефонов, адреса электронной почты и домашние адреса, сообщает *The Times of Israel (перевод Николая Царева)*.



В сообщении на Telegram-канале хакеры призвали своих коллег, правозащитные организации и активистов провести кампанию против Израиля, который называют Israhell (Изра-ад). Хакеры объяснили утечку данных 280 тыс. студентов военными действиями, которые Израиль вёл в секторе Газа летом 2021 г.

По мнению переводчика, «такие методы борьбы с израильскими оккупантами популярны среди пропалестинской оппозиции, так как позволяют бороться с захватчиками без применения реальной силы. Эти атаки опасны ещё и потому, что затрагивают интересы широких слоёв населения, поскольку используются сведения о студентах престижных вузов. Такая утечка данных создаёт опасность деанонимизации, например, упростит в будущем идентификацию новых сотрудников органов безопасности, политиков, военных и т.п.».

«Воровать деньги легко и приятно». Несанкционированное использование docomo account принесло ущерб в размере 28 млн иен крупнейшему японскому оператору мобильной связи NTT DoCoMo, сообщается в отчёте McAfee по итогам 2020 г. (перевод Юлии Журбиной).

Хакеры воспользовались уязвимостью, позволяющей получать доступ и выводить средства со счетов жертв в аккаунте DoCoMo. Как показало расследование, аналогичную уязвимость имеют PayPay, Kyash и LINE Pay.

Оказалось, что главной проблемой для операторов DoCoMo стал баланс между удобным сервисом и информа-

ционной безопасностью: идентификация личности пользователя, не являющегося клиентом компании, была чрезвычайно слабой, но быстрой и удобной. В будущем руководство компании намерено усилить ИБ и сбалансировать её со скоростью предоставления услуг.

О КИБЕРПРЕВОСХОДСТВЕ

Почти как COVID-19. В результате глобальной кибератаки в мае 2021 г. злоумышленники заблокировали доступ к компьютерным системам государственных учреждений и компаний 150 стран, сообщает BBC (перевод Елизаветы Васюхиной). Об остановке производства сообщил французский автопроизводитель Renault, испанские энергетические компании Iberdola и Gas Natural и телекоммуникационный гигант Telefónica, больницы, входящие в систему Национальной службы здравоохранения Англии и Шотландии, и многие другие.

Руководитель Глобального центра исследований и анализа угроз «Лаборатории Касперского» Костин Райо сообщил о 45 тыс. атаках в 74 странах. Он описал используемый хакерами вирус как червя, который размножается и быстро распространяется по электронной почте путём автоматической рассылки до 5 млн писем. Вымогатель требовал с жертвы эквивалент \$ 300 в Bitcoin для разблокировки доступа и данных.

Представители Европола указали, что масштаб атаки требует международно-го расследования.

Пока неизвестно, кто стоял за атаками и были ли они скоординированы.

Компания Microsoft выпустила патч для исправления эксплуатируемой вирусом уязвимости, однако на многих системах это обновление не было установлено, что и привело к печальным последствиям.

Испанский ответ. Другая майская кибератака также поставила под угрозу работу многих организаций в Испании. Атакам подверглись серверы и сайты государственных и муниципальных структур в Мадриде и провинциях. Киберпреступникам с помощью программы-вымогателя Zerpelin удалось зашифровать доступ к некоторому объёму информации, но, несмотря на масштабность нападения, нет никаких свидетельств утечки данных.

«Не стоит забывать, что обеспечение безопасности — это процесс, который сосредоточен не только на предотвращении, но и на раннем выявлении возможных угроз. Наши системы безопасности позволили обеспечить полную конфиденциальность информации, а также приступить к восстановлению некоторых данных», — сообщает хостинговая компания ASAC, на площадке которой размещены серверы и сайты пострадавших организаций.

Правительство Испании не раз заявляло о готовности предотвращать и выявлять атаки хакеров на государственном уровне, уверяя жителей, что их персональные данные будут в безопасности, пишет El Mundo (перевод Софьи Бубко).

В Латинской Америке лидирует Эквадор. 3 августа 2021 г. подвергся кибератаке Совет по коммуникациям Эквадора.

Злоумышленники перекрыли доступ к компьютерным системам сотрудникам Совета. Вредонос отключил устройства, в результате чего департамент приостановил работу.

В середине июля Национальная телекоммуникационная корпорация (CNT EP) подала жалобу в Генеральную прокуратуру на кибератаку, которая заставила «объявить чрезвычайное положение» на рабочих местах и привела к созданию Департамента по защите данных.

По данным разработчика антивирусного ПО и решений в области компьютерной безопасности для корпо-

ративных и домашних пользователей ESET, Эквадор входит в число стран с наибольшим количеством кибератак в Латинской Америке, пишет *Elcomercio* (перевод Валерия Круглова).

Флорида. Просто вредительство. Зимой 2021 года неизвестный хакер отравил воду системы центрального водоснабжения во Флориде. Злоумышленник захватил доступ к системе городской очистки воды и увеличил количество гидроксида натрия (известного как щёлочь) более чем в 100 раз. Это химическое вещество используется в небольших количествах для контроля кислотности воды, но в больших концентрациях может вызвать раздражения и другие осложнения.

Дежурный по станции, заметив, что показатели содержания щёлочи резко выросли, оперативно прекратил подачу воды.

Станция обеспечивает водой предприятия и около 15 тыс. домохозяйств. По данным следствия, злоумышленник смог взломать систему удалённого доступа к городскому водоснабжению, которая создавалась для упрощения работы персонала в штатном режиме и для оперативного решения проблем во время ЧС, рассказала *The Guardian* в переводе Полины Вершининой.

В своём комментарии Полина отмечает, что «хакерские атаки зачастую нацелены на мирных жителей. Хакеры используют технологии, изначально созданные для благих целей, для нанесения вреда. Более того, некоторые из них, в частности «герой» данной истории, работают на бытовом уровне, т.е. пытаются повлиять на людей через то, что те используют каждый день».

Сорвали зло. Хакеры, взломавшие базу данных компании Electronic Arts (EA) в июне 2021 г., опубликовали украденную информацию после неудачной попытки вымогательства. Сведения, изначально загруженные в даркнет в конце июля, активно распространяются на торрентах.

Согласно копии файлов, полученных специализирующимся на кибербезопасности изданием *The Record* (перевод Никиты Ляпорова), в утечку входили исходный код игры FIFA 21 и инструменты регулировки работы серверов компании.



Об утечке стало известно в июне, когда хакеры опубликовали запись на подпольном форуме, утверждая, что получили доступ к данным EA и планируют продать их за \$28 млн. Хакеры использовали аутентификационные файлы cookie, содержащие сведения аккаунтов сотрудников EA, а затем обманом вынудили техподдержку дать им доступ к внутренней сети компании, после чего украли более 780 Гб данных.

Желающих купить сведения, большая часть которых является исходным кодом игры, не нашлось. Однако ситуация показывает, что вне зависимости от масштаба компании и её систем защиты данные всегда находятся под угрозой утечки, делает вывод переводчик, отмечая также, что далеко не вся информация имеет ценность.

Новости из Японии. 1 сентября власти Токио сообщили о кибератаке на консалтинговую компанию, сотрудничающую с городскими департаментами, в результате чего возможна утечка данных. Также об атаках на свои сети и возможных утечках информации сообщили префектура Сайтама и город Итикава. Хакеры использовали вирус-вымогатель.

Все аутсорсинговые компании мэрии Токио являются собственностью Oriental Consultants (Сибуя, Токио), которая сообщала о нескольких кибератаках на свои сервера в августе-сентябре 2021 г. Инциденты выявили слабые места в системе ИБ компании. *Новости из Японии* перевела Яна Рожновская.

Без вымогательства. Японское правительство пострадало от утечки

данных после компрометации платформы ProjectWEB, разработанной корпорацией Fujitsu, продолжила японскую тему Анна Морозова.

Компания Fujitsu объявила промежуточные итоги расследования, согласно которому в мае 2021 г. произошла утечка информации 129 правительственных агентств и организаций, работавших через платформу обмена проектной информацией ProjectWEB. Воспользовавшись уязвимостью, хакеры получили идентификатор и пароль и легально вошли в систему. Они получили доступ к данным МИД Японии и Центра кибербезопасности правительства. Были похищены около 76 тыс. электронных адресов сотрудников и подрядчиков разных ведомств. От утечки данных пострадал и аэропорт Нарита.

Цели злоумышленников пока неизвестны, понятно только, что перманентная компрометация различных организаций и государственных учреждений не предполагает вымогательства. Тем не менее компания Fujitsu отключила платформу ProjectWEB и проинформировала всех клиентов.

* * *

Редакция благодарит за организацию и проведение творческого эксперимента по созданию киберобзора ИноСМИ преподавателя МГЛУ, кандидата философских наук Павла Былевского и обозревателя BIS Journal, кандидата технических наук Марину Бродскую.

ВНИМАНИЕ, «Я» — ЖЕРТВА!

ЛИНГВИСТИЧЕСКИЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ — МЕТОДЫ АНАЛИЗА ВИКТИМНОГО ПОВЕДЕНИЯ В СОЦИАЛЬНЫХ СЕТЯХ



**Сергей
РОМАНОВСКИЙ**
директор Института
информационных
наук МГЛУ

Актуальность изучения деструктивного поведения людей в киберпространстве обусловлена продолжающимся развитием инструментов цифровой коммуникации, социальных медиа, новых форматов взаимодействия, которые получили ускорение, в том числе за счёт ограничительных мер, направленных на борьбу с распространением COVID-19. Анализируя деструктивное поведение в киберпространстве, учёные связывают его с чрезмерной степенью самораскрытия в социальных сетях, публикацией провокативного контента, низким уровнем эмпатии, негативным отношением к человеческим ценностям, насилием. Инструменты виктимизации, или механизмы превращения в жертву преступного посягательства лица или группы лиц, формируются на базе психосоматического статуса жертвы, склонности к повышенной тревожности, гневу, депрессии, проблемам со сном, причинению вреда и нарушению общественных правил. В связи с деструктивностью, иногда опасностью для человеческих жизней этот феномен виктимизации в цифровой среде требует разностороннего и последовательного изучения, в том числе специалистами в области лингвистики.

ДИСКУРС

Одним из методов исследования виктимизации в среде коммуникаций является единая унифицированная система когнитивного анализа дискурса, которая реализуется в лингвистике на уровне не только текста, но и контекста,

являясь своего рода посредником в исследовании языковых структур и экстралингвистических факторов.

Дискурс — многозначный термин, означающий в общем смысле речь, процессы языковой деятельности и предполагающие их системы понятий. Дискурс относят к междисциплинарным понятиям, которые используются в различных науках и имеют различные интерпретации. Французский лингвист Элизабет Ле отмечает, что дискурс в лингвистике рассматривается в контексте трёх составляющих:

- ◆ использование языка;
- ◆ встраивание в общественное сознание определённых представлений;
- ◆ взаимодействие социальных групп и индивидов.

Тройственность структуры дискурса определяет параметры исследования, на которых основаны методы и инструменты анализа:

- ◆ дискурс есть использование языка, его изучение предполагает анализ текста в отношении синтаксиса, лексики, голоса, полифонии, функции, модальности отдельных компонентов с целью прояснить либо завуалировать детали;
- ◆ дискурс формирует представления и делает необходимым анализ продуцирования текстов и их интерпретации;
- ◆ дискурс формирует смысловое взаимодействие общественных групп и индивидов и исследуется в контексте социальных структур культуры общества.

АНАЛИЗ ДЕСТРУКТИВНОГО ДИСКУРСА

Дискурсивный анализ не ограничен языковыми рамками, поскольку дискурс — междисциплинарное понятие,

сформированное в траекториях нескольких областей исследования: семиотики, этнографии, нарративного анализа, анализа речевого общения, лингвистики текста, прагматики, социолингвистики, психологии, теории искусственного интеллекта.

Современный метод когнитивного анализа деструктивного дискурса — это особый подход к анализу дискурса, в основе которого структура текста определяется характером контекста, а дискурс рассматривается с позиций единства языковых и когнитивных структур. Метод когнитивного анализа деструктивного дискурса имеет два аспекта — текстуальный и контекстуальный. Текстуальный анализ включает рассмотрение языковых структур на всех уровнях: фонетическом, графическом, морфологическом, синтаксическом, семантическом, макроструктурном. Контекстуальный анализ включает рассмотрение всех экстралингвистических факторов: времени, места, сферы деятельности, участников дискурса, их социальных ролей, характера их взаимоотношений и когнитивных характеристик участников.

Для участников информационного обмена характерны определённые модели поведения, которые, с точки зрения когнитивного анализа деструктивного дискурса, в частности виктимного поведения, можно определить следующим образом:

- ◆ отклонение от норм безопасного поведения, реализующегося в совокупности социальных, психических и моральных проявлений;
- ◆ аутодеструктивное поведение, для которого свойственно совершение

опасных для жизни действий, не связанных с осознанными представлениями о собственной смерти;

- ♦ поведение личности, которое значительно повышает риски субъекта стать жертвой преступления;

- ♦ психологическое отклонение, закреплённое в привычных формах активности, обуславливающих предрасположенность субъекта становиться жертвой;

- ♦ вызывающее, опрометчивое, патологическое поведение;

- ♦ отклонение от норм безопасного поведения, обусловленное характерологическими особенностями и деформацией ценностно-мотивационной составляющей личности;

- ♦ сложная система взаимодействия между потенциальной жертвой и окружением.

КИБЕРБУЛЛИНГ

Виктимное поведение — отклонение от норм безопасного поведения в процессе коммуникации, реализующееся в совокупности социальных, психических, моральных проявлений. В качестве инструмента среды опосредованной коммуникации выступает полимодальная (вербальная, визуальная, кинетическая (жестовая)) смысловая составляющая взаимодействия. Среда формирования виктимного поведения формируется в общем случае за счёт низкого уровня цифровой грамотности, импульсивности и низкого уровня эмоционального контроля, заниженной самооценки, низкого уровня удовлетворённости жизнью, чрезмерного пребывания в соцсетях, высокого уровня доверия или чрезмерной открытости.

Кибербуллинг является распространённым видом межличностной коммуникации и формой виртуальной коммуникации и виртуального экстремизма. Кибербуллинг и виктимизация имеют многочисленные негативные последствия для психологического здоровья и навыков социализации, включая беспричинный гнев, тревогу, депрессию, уныние, желание остаться одному, избегать контактов, попытки причинить себе физические увечья и даже совершить попытку самоубийства. В группу риска, в частности, попадают женщины, дети, принадлежащие к национальным меньшинствам или имеющие низкий

социальноэкономический статус, люди, страдающие избыточным весом, имеющие инвалидность, плохие социальные навыки и т.д. Одним из отличительных признаков подобной формы виртуальной коммуникации является провокативная тональность текста участников информационного обмена. Этимологическая основа термина «провокация» берёт начало в латинском языке — *provocatio*, что означает «подстрекательство, побуждение к действиям, которые могут повлечь за собой тяжёлые последствия».

Участники конфликтной интеракции, социальные условия и условия языковой среды формируют когнитивную базу конфликтного дискурса. Исследование интеракции в кибербуллинге и выявление её признаков возможно через лингвистическое описание. В силу своего опыта и в соответствии с условиями речевого эпизода каждый участник коммуникации оценивает интеракцию и совершает определённые «речевые действия», которые ведут к появлению конфликтной интеракции¹. Создавая тексты конфликтного содержания, автор использует особые высказывания, чтобы спровоцировать адресанта вступить с ним в коммуникацию. Реципиент, участвующий в кибербуллинге, изначально имеющий личную интенцию, осознанно выбирает из всех доступных языковых средств «инвективы» (нападки, брань, «наезд») и «перформативы» (речевые акты, равноценные поступку) для выполнения воздействующей функции. В процессе восприятия выбранные языковые средства и обороты оказывают отрицательное влияние на психическое состояние адресата, в ходе которого изменяется его восприятие ситуации². Важным обстоятельством является тот факт, что при исследовании кибербуллинга текст получает признаки процессуальности, необходимости исследования дискурсивной и когнитивной составляющих, поскольку смысл

¹ Сусов И. П. Говорящая личность в лингво-социальном и лингвопрагматическом пространствах. — Пятигорск: Пятигорский государственный педагогический университет, 1989.

² Белоус Н. А., Ананьева А. А., Признаки конфликтной интеракции в кибербуллинге среди подростков. — «Молодой учёный». № 26 (316). Июнь 2020.

текстового целого даёт возможность свободной интерпретации, игры авторских и читательских смыслов.

ЛИНГВИСТИЧЕСКИЕ МЕТОДЫ

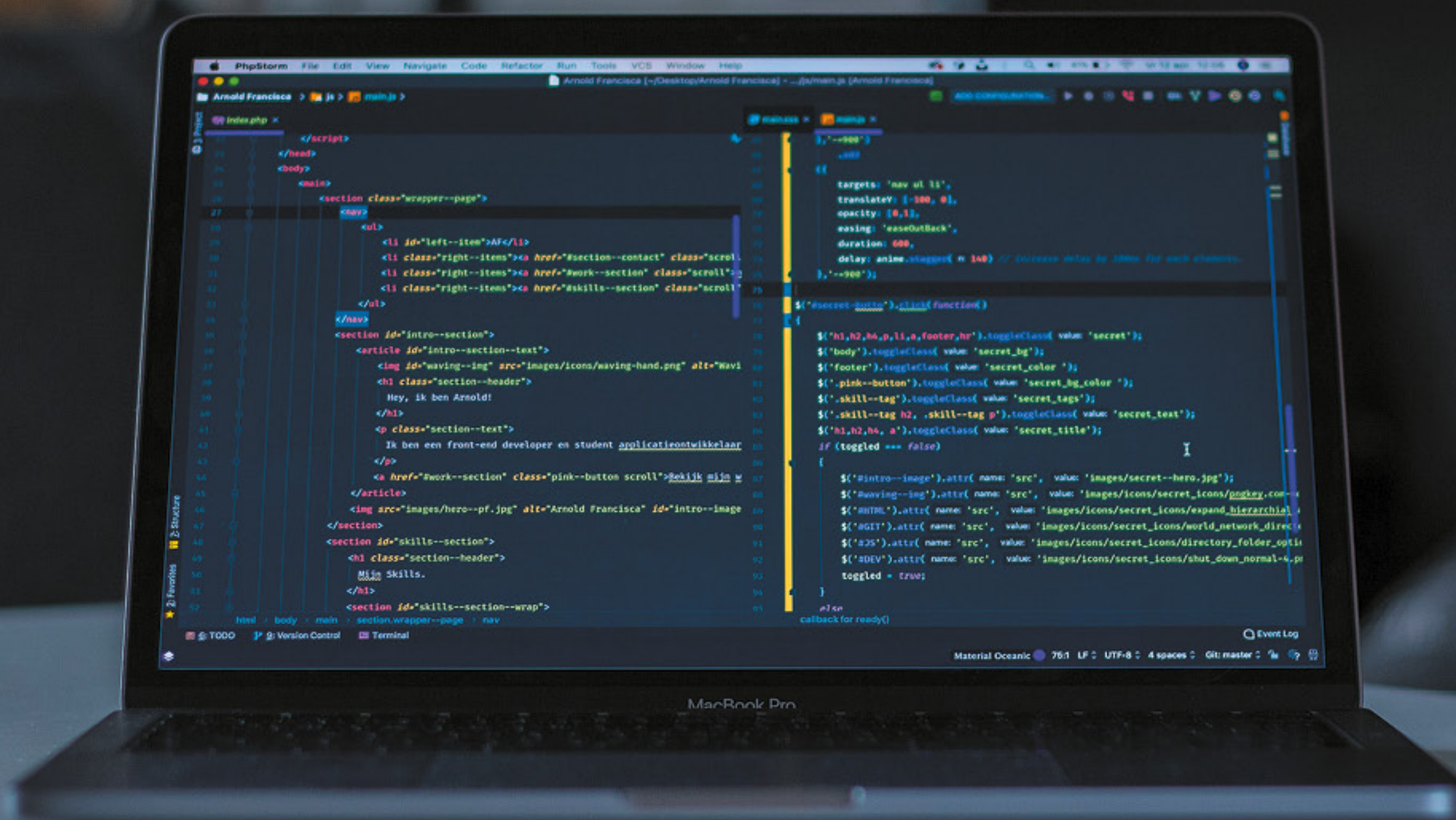
Для выявления и изучения языковых маркеров в содержании конфликтной интеракции в процессе кибербуллинга используется широкий спектр лингвистических методов, которые базируются на формировании и исследовании корпусов: анализ коммуникативного поведения с выяснением статусно-ролевых отношений между коммуникантами; пассивное наблюдение с последующей письменной фиксацией; сплошная выборка; контекстуальный анализ для учёта общих условий, оказывающих влияние на индивидуальные функциональные условия или модифицирующие взаимосвязи между индивидуальными функциональными условиями и метод описательного анализа языковых единиц. В процессе выявления признаков конфликтной интеракции решаются следующие задачи:

- ♦ описание речевых шагов в текстах конфликтной интеракции;

- ♦ выявление моделей, методов и техник диалогической интеракции;

- ♦ выявление грамматических и семантических особенностей, в том числе экспликация конфликтных маркеров и описание их принадлежности к различным видам лексики, определение грамматических особенностей выстраивания коммуникации.

В основе современного изучения деструктивного поведения людей в киберпространстве лежит корпусная лингвистика, которая обнаруживает параллели с лингвистикой дискурса. Лингвистика дискурса фокусирует интерактивность, интертекстуальную связность текстов, в свою очередь, корпусная лингвистика фокусирует репрезентативность текстовых образцов. Дискурсивно ориентированный анализ — качественно-ориентированный анализ, макросемантический, вскрывающий глубинные связи высказываний, не обязательно лежащие на поверхности. Корпусно-ориентированный анализ — количественный, создающий исследовательский фокус на том, что в языковом употреблении обеспечивает содержательное единство.



**Андрей
ЖАРКЕВИЧ**
редактор
ООО «Антифишинг»

НА ОДНОМ ЯЗЫКЕ

КАК НАЛАДИТЬ КОНТАКТ КОМАНДЫ ИБ И ПРОГРАММИСТОВ

Социальная инженерия и использование человеческого фактора в кибератаках стали основным трендом последних лет. Нападения становятся всё более сложными и задействуют все слабости корпоративных информационных систем — как психологические уязвимости людей, так и уязвимости в программах. Люди выполняют начальное действие, например открывают документ и разрешают выполнение макросов. А дальше вредоносный код использует другую разновидность уязвимостей — ошибки в программах. С их помощью на компьютере жертвы запускается «полезная нагрузка», например троян или бэкдор, шифровальщик-вымогатель или шпионский модуль...

Работу над устранением уязвимостей в программах нужно начинать не в момент, когда ими воспользовались преступники, а значительно раньше — на стадии создания приложения и даже ещё раньше, во время проектирования и формирования требований к безопасности программы (илл. 1). О том, как повысить эффективность формирования требований к безопасности разработки, поговорим в этой статье.

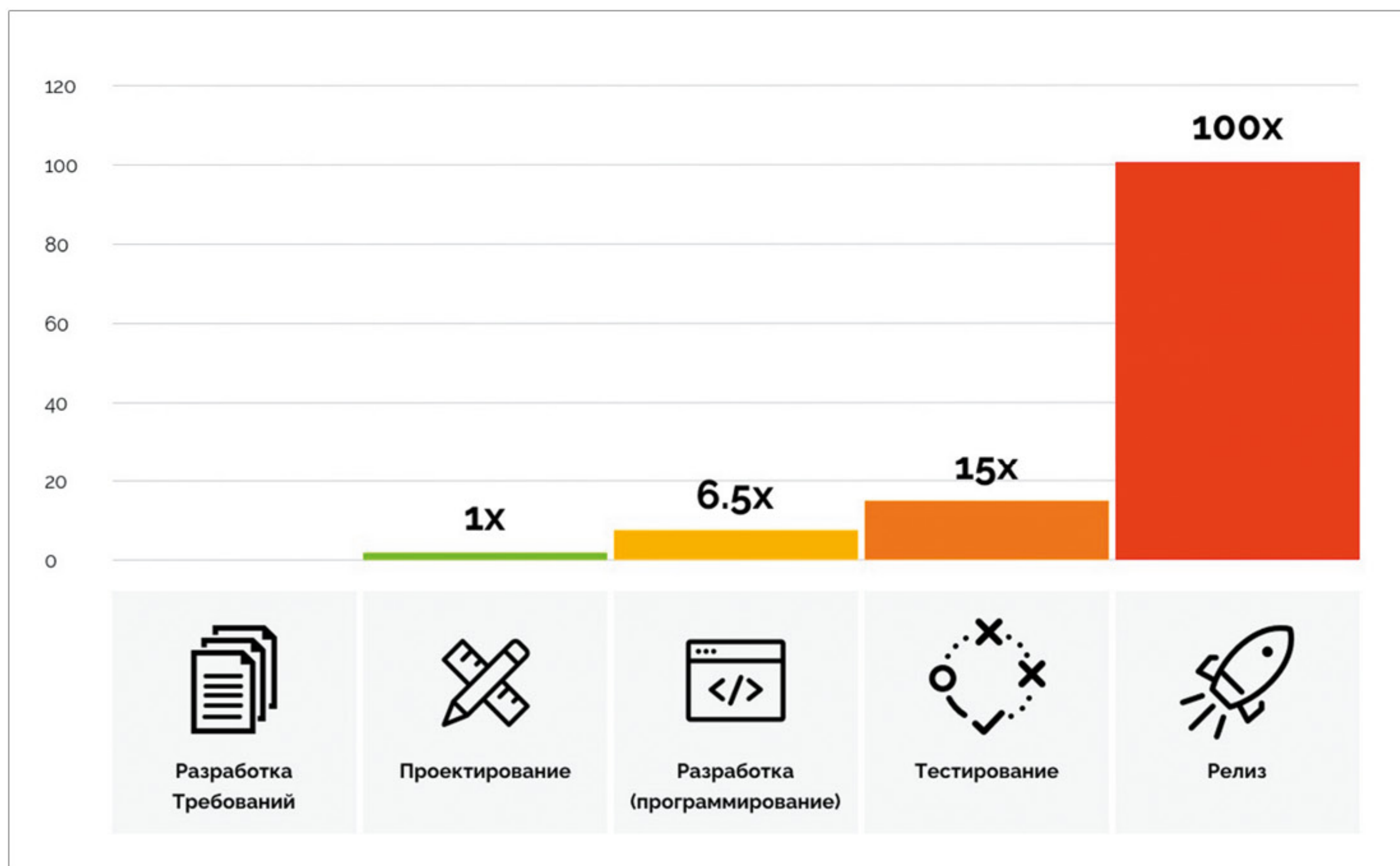
ВЫЯВЛЯЕМ НЕЭФФЕКТИВНЫЕ ПРАКТИКИ

В крупных компаниях, как правило, имеется собственный отдел или департамент разработки, программисты которого пишут код для автоматизации различных участков деятельности. Эти программы используют все сотрудники, поэтому безопасность компании зависит от того, насколько безопасно они написаны.

С первого взгляда кажется, что для разработки безопасной программы нужно не так много усилий:

- ♦ взять требования к безопасности разработки ПО, например, из ГОСТ Р 56939–2016. Защита информации. Разработка безопасного программного обеспечения. Общие требования;
- ♦ добавить отраслевые практики, например PCI DSS и/или OWASP;
- ♦ вписать всё это в таблицу Excel или Google Sheets;
- ♦ передать её программистам, которые воплотят требования и рекомендации в коде;
- ♦ проконтролировать результат на приёмодаточных испытаниях.

Однако многочисленные попытки получить таким образом действительно безопасное



приложение раз за разом оказываются неудачными. И причина не только в том, что на текущий момент только отечественные требования по безопасности с учётом нормативных актов отраслевых регуляторов и стандартов — это более 150 документов с различной степенью детализации описания этих требований. Не менее значимым фактором становится несоответствие взаимных ожиданий заинтересованных сторон.

Большинство разработчиков ожидают, что:

- ◆ сдадут продукт или проект в срок,
- ◆ качество будет наилучшим,
- ◆ все требования будут выполнены,
- ◆ всё будет работать максимально безопасно,
- ◆ они получат заслуженное вознаграждение.

Единственное препятствие на этом блестящем пути — приёмо-сдаточные испытания, в ходе которых неожиданно выясняется, что результат не соответствует требованиям. Основная причина в том, что разработчики не знают ответов на фундаментальные вопросы:

- ◆ Какие угрозы актуальны?
- ◆ В чём реальные риски?
- ◆ Что такое безопасный код и как его писать?
- ◆ Какие могут быть проблемы с окружением?

А ещё в некоторых командах существует своеобразный карго-культ — внутреннее представление о том, как должен выглядеть действительно

безопасный код, причём во многих случаях оно весьма фрагментарно и не покрывает весь спектр возможных проблем безопасности.

В результате вместо ввода программы в эксплуатацию приходится повторно уточнять требования к безопасности и заново проходить все стадии разработки и тестирования. Это приводит к срыву сроков и значительному удорожанию проекта.

Но и **со стороны ИБ-подразделений** тоже наблюдаются проблемы, поскольку их сотрудники:

- ◆ даже зная наизусть ГОСТ Р 56939–2016, Приказ ФСТЭК № 17, Положение ЦБ РФ № 719-П, не могут сформулировать их **в виде понятных разработчикам требований**;

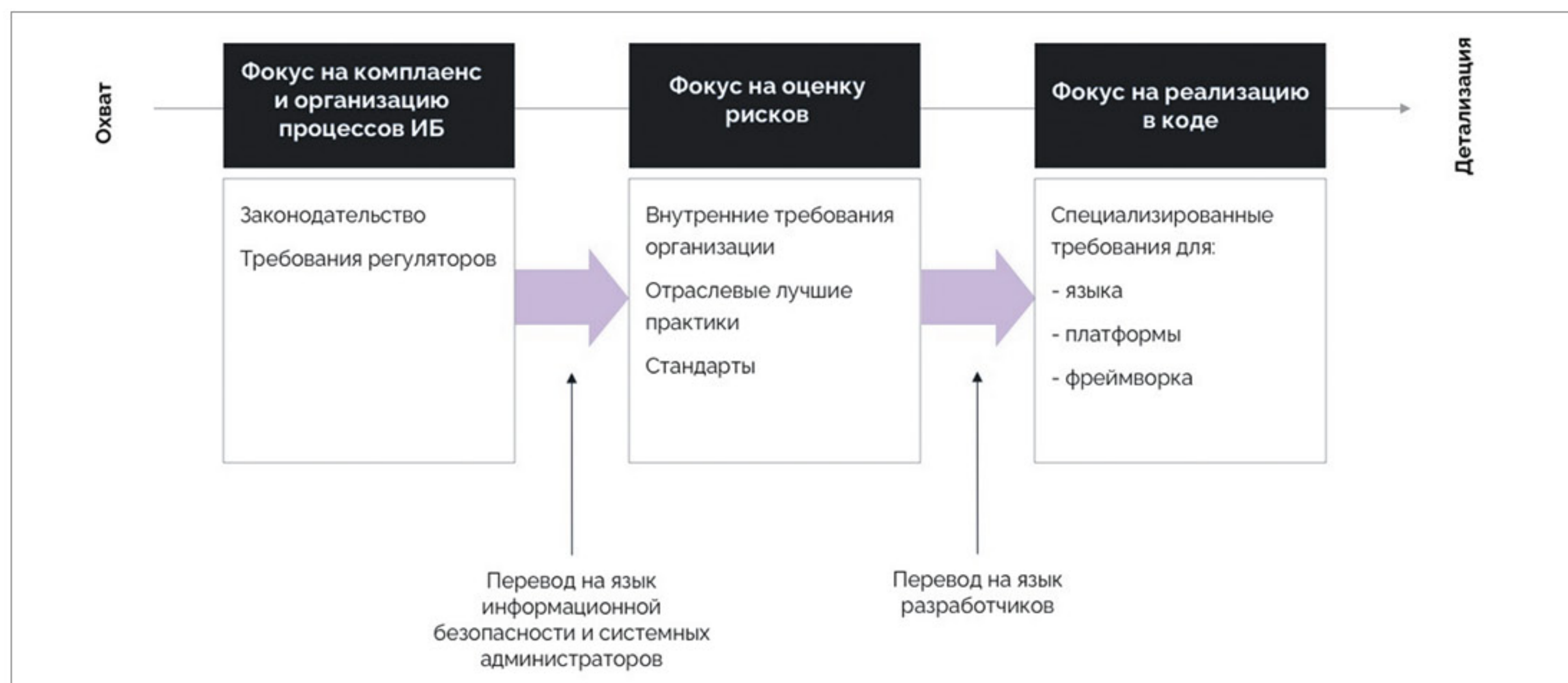
- ◆ не могут качественно сопоставить требования отечественных нормативных документов с аналогичными требованиями международных стандартов;

- ◆ не имеют представления о том, как требования к безопасности соотносятся с технологическим стеком, который использует команда разработки, а в ряде случаев не знают даже, какие фреймворки и языки программирования задействованы в проекте;

- ◆ не готовы проводить верификацию программы в части реализации сформулированных требований по безопасности просто потому, что не знают, как это сделать.

Иллюстрация 1.

Относительная стоимость устранения дефектов ПО на разных стадиях разработки

**Иллюстрация 2.**

Уровни требований по информационной безопасности

ФОРМУЛИРУЕМ ИДЕАЛЬНЫЕ ТРЕБОВАНИЯ ПО ИБ К ПО

В процессе разработки Антифишинга, программного продукта для ликвидации человеческих уязвимостей, наши разработчики и ИБ-эксперты сформулировали, как должны выглядеть идеальные требования к безопасности ПО:

Корректные требования по ИБ к ПО формируются командами разработки самостоятельно и автоматически.

Чтобы добиться этого результата, необходимо организовать процесс таким образом, чтобы учитывать все уровни требований по информационной безопасности и обеспечить «перевод» требований с формального языка на язык соответствующей целевой группы (илл. 2).

Этот процесс состоит из следующих этапов:

1. Анализ законодательства и требований регуляторов с фокусом на комплаенс и организацию процессов ИБ.

2. «Перевод» требований на язык ИБ-экспертов и системных администраторов.

3. Анализ внутренних требований организации, лучших отраслевых практик и стандартов с фокусом на оценку рисков. На этом этапе целесообразно выполнить сопоставление (маппинг) аналогичных требований из различных документов с тем, чтобы избежать дублирования одинаковых требований, сформулированных по-разному, например:

♦ **OWASP:** ошибки подсистемы аутентификации должны обрабатываться безопасно и не позволяют атакующему войти в АС.

♦ **Стандарт Банка России:** должны быть определены, выполняться, регистрироваться и контролироваться правила и процедуры —

идентификации, аутентификации, авторизации субъектов доступа, в том числе внешних субъектов доступа, которые не являются работниками организации БС РФ, и программных процессов (сервисов).

4. «Перевод» расширенной и очищенной от дублирования подборки требований на понятный разработчикам язык.

5. Дополнение и уточнение требований с учётом используемых языков программирования, платформ и фреймворков.

6. Выгрузка окончательного перечня требований в виде удобного для использования документа.

СОЕДИНЯЕМ ОЖИДАНИЯ ИБ И РАЗРАБОТЧИКОВ

Чтобы процесс формирования требований к безопасности программы не превратился в противостояние команд ИБ и разработки в виде бесконечных споров по поводу зон ответственности и трактовки различных формулировок, необходима унифицированная платформа.

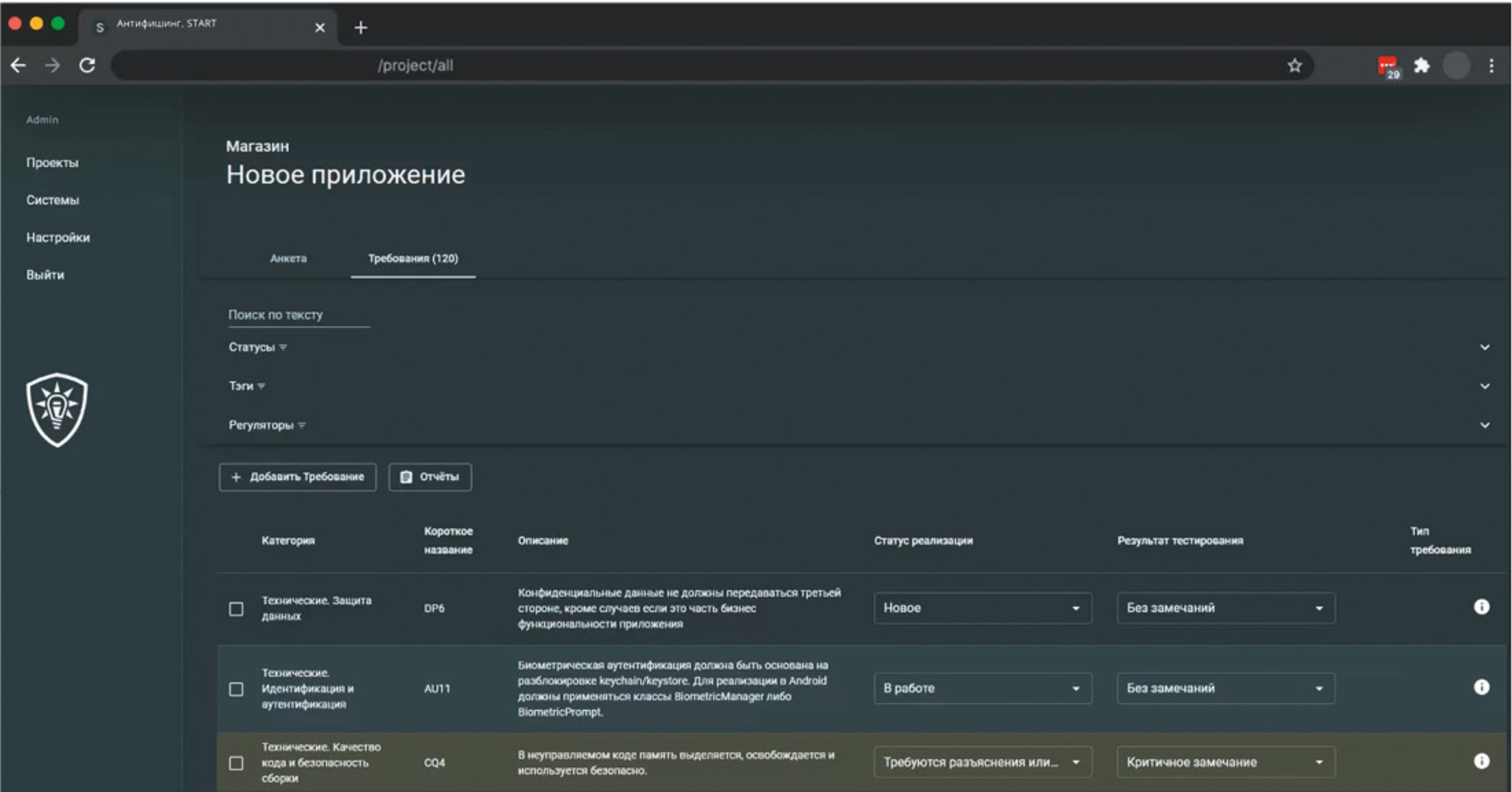
В функции такой платформы должны входить:

♦ возможность создавать и наполнять базу требований;

♦ все требования стандартов, руководств и лучших практик;

♦ автоматическое обновление требований при любом изменении конфигурации ПО, стандартов и нормативных документов, причём изменения сразу должны быть видны у инженерных команд;

♦ автоматическое сопоставление требований из разных стандартов и от разных регуляторов в единые референсные требования без противоречий и дублирования;



- ◆ конкретные примеры и практики реализации требований для разработчиков;
- Такая платформа позволила бы командам ИБ и разработки:
- ◆ поддерживать актуальность знаний о приёмках безопасной разработки;
- ◆ изменять требования при изменениях в стеке технологий;
- ◆ отслеживать обновления стандартов;
- ◆ своевременно получать информацию о новых уязвимостях;
- ◆ быть в курсе публичных инцидентов;
- ◆ получать обратную связь от процессов тестирования требований: пентест, ПСИ, SAST/DAST.

РЕАЛИЗАЦИЯ ОЖИДАНИЙ

Результатом тесного сотрудничества ИБ-команды и разработчиков Антифишинга стал новый продукт — Антифишинг.START, в котором были реализованы ожидания и пожелания всех участников процесса создания ПО (илл. 3).

Главные функции системы:

- ◆ работа начинается с составления анкеты, на основании которой формируются требования по защите информации;
- ◆ содержит предустановленные базы требований нормативных документов, регуляторов и стандартов: OWASP, 382-П и 719-П, PCI DSS;
- ◆ умеет сопоставлять требования в базе знаний с требованиями из государственных нормативных актов и стандартов, показывает, каким законом или стандартом предъявляется данное требование;

- ◆ автоматически обновляет требования по информационной безопасности при изменении архитектуры или бизнес-требований к системе;
- ◆ каждое требование привязано к одному из этапов DevSecOps;
- ◆ позволяет добавлять уникальные требования для каждой разрабатываемой системы;
- ◆ контроль выполнения требований с помощью наглядных статусов;
- ◆ интеграция с LDAP, JIRA, GRC и другими системами и средствами защиты.

Таким образом, мы создали гибкое и функциональное решение для управления требованиями к безопасности разработки ПО, которое позволяет наладить полноценный контакт ИБ, разработчиков ПО и всей инженерной команды.

Благодаря Антифишинг.START не только экономится время, но и существенно повышается качество результата:

- ◆ ИБ-команды быстро и чётко выбирают актуальные требования по безопасности;
- ◆ разработчики принимают их в работу в виде конкретных рекомендаций, повышая свой профессиональный уровень;
- ◆ менеджер проекта понимает, в каком состоянии находится реализация требований безопасности, кто, каким образом и на каких этапах реализует эти требования;
- ◆ если потребуется добавить новые функции или поменять состав технологического стека, изменения в требования по данному проекту будут скорректированы автоматически.

Иллюстрация 3.
Интерфейс системы: заполнение анкеты для формирования требований к новому приложению

ЦИФРОВАЯ ГИГИЕНА: ПРАВИЛА ИГРЫ

О БАЗОВЫХ ПРИНЦИПАХ РАБОТЫ
С КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ



**Александр
ДВОРЯНСКИЙ**
директор
по стратегическим
коммуникациям
компании
Infosecurity
(ГК Softline)

Компания Infosecurity оказывает услуги в сфере информационной безопасности, системной интеграции и консалтинга. Нам важно показать, что мы можем защитить не только данные, которые нам доверяют клиенты, но и собственные информационные активы. Даже незначительный инцидент ИБ в компании, занимающейся кибербезопасностью, может ударить по ее репутации.

Итак, на формирование цифровой гигиены в компании влияют:

- ♦ повышение осведомлённости сотрудников по вопросам ИБ;
- ♦ разграничение доступа к информации;
- ♦ применение технических средств контроля и мониторинга информации.

Остановимся подробнее на первом из этих трёх китов — повышении осведомлённости.

ЗАЧЕМ ЭТО НУЖНО?

В любой уважающей себя компании существуют внутренние регламенты, политики и методики, посвящённые правилам обработки информации

ограниченного допуска. Увы, само по себе наличие этих документов не даёт ровным счетом ничего. Реальную защиту обеспечивают сотрудники, которые точно следуют прописанным в документах требованиям. Но где найти таких идеальных сотрудников?

Хитрость в том, что их нужно не искать, а, скажем так, выращивать. Комплекс обучающих мероприятий и материалов позволяет сформировать в компании культуру работы с информацией. Если всё подобрано верно, сотрудники начинают соблюдать правила ИБ на рефлекторном уровне.

И КАК ВСЁ ПОДОБРАТЬ?

Прежде всего разделите ваших сотрудников на группы и определите темы, актуальные для каждой группы. Топ-менеджерам вряд ли будет интересно изучать актуальные уязвимости ПО, а вот разработчикам — очень даже.

Когда темы определены, подумайте о форматах обучающих материалов: их тоже нужно персонализировать. Например, у сотрудников front-офиса не так много свободного времени, а иногда нет и компьютера. Им подойдут яркие



плакаты и короткие видеоролики, которые можно размещать и демонстрировать в торговых залах. А сотрудники back-офиса могут уделить обучению больше внимания, поэтому им лучше адресовать электронные курсы и обучающие почтовые рассылки.

Ещё одна практика — перед тем как проводить обучение по ИБ, проверьте, что ваши сотрудники уже знают. Проведите тестирование и разошлите учебные фишинговые письма. Так вы поймёте, каким темам нужно уделить больше внимания. И не стоит забывать о контроле эффективности в процессе обучения.

О ФОРМАТАХ

Очное обучение. В некотором роде оно незаменимо: всем известно, что информация воспринимается лучше, когда сопровождается живым общением. Тренинг можно проводить в классической форме или по кейс-методу. Во втором случае инструктор делит учащихся на группы, описывает актуальную для компании проблему и предлагает каждой группе дать и обосновать свой вариант её решения. Можно объединить

два вида тренингов: проводить вводный для сотрудников в их первый рабочий день, а кейс-тренинг — ежемесячно или раз в квартал.

Дистанционное обучение составляет достойную конкуренцию очному. Электронные курсы, видеоролики, почтовые рассылки и онлайн-игры хороши тем, что сотрудники могут просматривать их на разных видах устройств в удобное для себя время. А ещё они дают возможность похвастаться перед конкурентами словами «геймификация» и «микрообучение».

Геймификация особенно активно используется в электронных курсах. Она предполагает добавление игровых элементов: награды и достижения, постепенное усложнение заданий, увлекательный сюжет, персонажи. Геймификация — это вообще интересная история, потому что она может быть полностью электронной, а может «перетекать» в реальную жизнь. Например, за успешное прохождение курсов по ИБ сотрудника можно наградить одним дополнительным днём отпуска. Такие вещи, конечно, согласовываются с HR. Кто из нас не мечтал на работе о компьютерных играх?

Микрообучение предполагает подачу материала небольшими блоками и закрепление каждого блока практическими заданиями. Например, посмотрел 5 слайдов курса — ответ на тестовый вопрос или выполни маленькое упражнение. Если речь идёт о видеороликах, то они должны быть длиной не более полутора минут. Лучше сделать серию коротких роликов (кстати, их можно объединить одним забавным сюжетом), чем заставлять сотрудника смотреть тяготную семиминутную проповедь. Но и дробить обучение до бесконечности не стоит: так можно потерять логику повествования.

Кроме очного и дистанционного обучения, очень полезны дополнительные обучающие материалы. Памятки, плакаты, стикеры и скринсейверы отлично справляются с задачей сделать обучение разнообразным и запоминающимся. Не бойтесь привлекать к их оформлению профессиональных дизайнеров и иллюстраторов: материалы от этого только выиграют.

ВСЁ ДЕЛО В РАЗНООБРАЗИИ!

Заставить человека учить то, что ему неинтересно, и соблюдать то, что ему непонятно, — невозможно. Создавая для сотрудников комплексные программы обучения, излагая материал простым и доступным языком и облачая его в игровую форму, вы, по сути, делаете вклад в безопасность — вашу, вашей компании и ваших клиентов. И если всё сделано «по науке», ваши вложения непременно окупятся.



Борис СТОЛПАКОВ
историк криптографии,
кандидат физико-
математических наук

«Я ВОЕННЫЙ СВЯЗИСТ, Я ТЯНУ ПРОВОДА...»

КАК СОЗДАВАЛАСЬ НЕЙРОННАЯ СЕТЬ ПОБЕДЫ

Для многих граждан России, относящих себя к поколениям старших возрастов, каждый юбилей начала ВОВ ощущается и переживается до сих пор как нечто глубоко личное. Здесь и чувство тяжёлых потерь, и радостное осознание больших достижений, прежде всего общей Победы и послевоенного возрождения.

СТАЛИ БРАТЬЯМИ И СЁСТРАМИ...

Не вдруг, а через неимоверные страдания и самоотверженный труд была достигнута желанная Победа, осенью 1941-го чужим глазам казавшаяся сомнительной мечтой. Но пришёл её срок, и она наступила, вопреки тяжёлым поражениям советских войск в первые месяцы противостояния и вопреки вражеским ожиданиям распада страны с погружением в новую гражданскую войну.

Как мы знаем, единство народа и его вождей, ярко проявленное в обращении «Братья и сестры!», сохранило управляемость огромной страной и обеспечило Победу в 1945-м. Кажется, сама жизнь выдвинула тогда руководителей, благодаря своим талантам, энергии и самоотверженности ставших подлинными организаторами успехов на фронте и в тылу. Многие из них ныне почти забыты.

АХИЛЛЕСОВА ПЯТА

Напомним одного из этих богатырей — Ивана Терентьевича Пересыпкина (1904–1978). Поприще ему выпало

самое незавидное: он в военные годы возглавлял всю связь в СССР, военную и гражданскую. Как известно, многие беды Советской армии в первоначальный период боёв были связаны именно со слабостью организации военной связи и, как следствие, потерей управления войсками. К сожалению, осознание подобной уязвимости вооружённых сил в довоенный период сильно запоздало. Так, в выступлении на расширенном заседании Политбюро ЦК ВКП (б) в мае 1941 года Сталин сказал: «...О средствах связи. Это действительно наша ахиллесова пята. Но думаю, что здесь едва ли можно быстро сделать что-нибудь серьёзное, сейчас же устранить имеющиеся в этой области недостатки. Придётся какое-то время исходить из того, что есть».

ПАРЕНЁК СО РТУТНОГО РУДНИКА

Достоинство нашего внимания то, как произошло выдвижение И. Т. Пересыпкина, да и само становление его как специалиста. Родился он близ Горловки, рано лишился отца. Его подростковые годы пришлись на время Гражданской войны. Чтобы выжить, Иван стал работать на соседнем ртутном руднике, а с приходом Красной армии в 1919 г. прибавил себе два года и записался добровольцем. Почти всё недолгое время службы проболел, в 1920 г. был уволен по несовершеннолетию. Помыкавшись в поисках заработка, в 1921 г. вернулся

на ртутное производство. Его энергичная натура проявила себя, и в мае 1923 г. Иван Пересыпкин поступил по комсомольской путёвке в военно-политическую школу Украинского военного округа в Киеве. После её окончания в следующем году он стал политбойцом в кавалерии, в 1-й Запорожской дивизии Червоного казачества, дислоцированной тогда в г. Проскурове (ныне г. Хмельницкий). Пришлось ему послужить в сапёрном и связном эскадронах, пока в 1932 г. его не назначили сначала комиссаром, а затем и командиром эскадрона связи.

«НЕУД» ПО МАТЕМАТИКЕ

Много позже Иван Терентьевич с благодарностью вспоминал, что, выдвигая его, комдив П. К. Потапенко советовал: «Учиться тебе надо, хлопец... Через пять, десять лет все мы такие вот, как я, или честно должны уйти, или тормозом станем. Я ведь и матерюсь иной раз почему? Слов не хватает. А должно хватать...» И помогал как мог. Уже осенью Пересыпкин сдал экстерном экзамены за курс кавалерийской школы. Ещё раньше он начал основательно готовиться к поступлению в Высшую военную электротехническую школу комсостава РККА (будущую академию связи), имея лишь начальное образование в рудничной школе. Всё же к осени 1932 г. позади остались и предварительные испытания, и учёба на подготовительных курсах. Той осенью его



Иллюстрация 1. Иван Терентьевич Пересыпкин (1904–1978)

вызвали в Ленинград для сдачи вступительных экзаменов, и на испытании по математике он получил «неуд». К счастью, командование академии получило из Москвы разрешение в связи с недобором слушателей принять условно всех имевших командный стаж и получивших на экзаменах по одной двойке.

Наконец в июне 1937 г. Пересыпкин после окончания академии вместе с очередным воинским званием капитана получил направление в Москву на должность военного комиссара НИИС КА.

НЕУЁМНЫЙ ВОЕНКОМ

Военком быстро нашёл общий язык с главным инженером института, будущим академиком АН СССР, бригадным инженером М. В. Шулейкиным, с чьим именем связано развитие средств военной радиосвязи. Хотя в институте был создан мощный задел конструкторских разработок, из-за слабой технической базы промышленности новая аппаратура воплощалась лишь в опытных образцах. В то время как армия и флот испытывали острый недостаток в

средствах связи, малочисленные предприятия электропромышленности обеспечивали крайне незначительный объём их производства.

Спустя всего полгода И. Т. Пересыпкин был назначен военным комиссаром Управления связи Красной армии (УСКА) и стал полковником. Уже летом 1938 г. ему пришлось включиться в боевую работу Управления в ходе подготовки и ведения военных действий у озера Хасан на Дальнем Востоке (29 июля — 11 августа). Ещё до этих событий медленное строительство линий связи, нехватка самих средств связи и низкая укомплектованность личным составом потребовали оперативного разрешения. Поэтому энергичный и ответственный военком, заручившись поддержкой начальника УСКА, решил обратиться за помощью к наркому обороны К. Е. Ворошилову.

Пересыпкин подготовил ему в июле 1938 г. доклад «О состоянии вопросов связи в РККА и подготовки страны в отношении связи». В сопроводительной записке он просил принять его для личного доклада по существу затронутых вопросов. В январе 1939 г. Пересыпкин направил наркому обороны очередной доклад — «Готовность средств связи НКО к войне по состоянию на 25 января 1939 года». В нём он сделал вывод: «Создалось исключительно тяжёлое положение со строительством связи, и в этом вопросе мы сильно отстаём от наших вероятных противников». Его предложение: «Заслушать на заседании Главного военного совета начальника УСКА о состоянии оборонного строительства».

ОБСТОЯТЕЛЬНЫЙ АНАЛИЗ НАКАНУНЕ ВОЙНЫ

Известно, что после хасанских боёв войска связи были подвергнуты серьёзной критике на заседании Политбюро ЦК ВКП(б). Причём много претензий в первую очередь предъявлялось УСКА и радиоцентру Узла связи Наркомата обороны (НКО). Разбор с поиском виновных и спешная разработка мер по улучшению работы радиостанций военных округов затронули и Пересыпкина. Ему, как военкому, пришлось писать в феврале 1939 г. докладную записку в ЦК с обстоятельным описанием всех

недостатков в работе радицентра Узла связи НКО, их причинах, а также о принятых и намечаемых мерах по радикальному улучшению радиосвязей НКО.

Тогда же, в феврале 1939 г., К. Е. Ворошилов предложил И. Т. Пересыпкину занять должность начальника УСКА. Иван Терентьевич отказался, сославшись на отсутствие достаточного опыта и необходимой подготовки. В конце концов решили по предложению Пересыпкина назначить его заместителем начальника УСКА.

Ещё оставаясь военкомом, в марте он направил доклад начальнику Политуправления РККА З. Л. Мехлису, в котором, опираясь на мнение специалистов НИИС КА, тщательно проанализировал обеспеченность РККА средствами связи в мирное и военное время, а также обосновал вывод об угрожающем положении со средствами связи в армии и флоте.

«МЫ РЕШИЛИ ВАС НАЗНАЧИТЬ...»

Вероятно, государственный масштаб мышления автора доклада впечатлил его читателей, и вскоре И. Т. Пересыпкина вызвали в ЦК ВКП(б), где с ним беседовали о состоянии войск связи и посоветовали пока не уезжать в отпуск. Дальнейшие события, со слов Пересыпкина, развивались так.

«9 мая 1939 г. в 10 часов вечера, когда я ещё находился на работе, раздался звонок правительственного телефона. Человек, не назвавший себя, но спросивший меня, кто у телефона, сказал: «Вам, товарищ Пересыпкин, нужно сейчас же приехать в Кремль к товарищу Сталину».

Поздоровавшись и внимательно посмотрев мне в лицо, Сталин неожиданно для меня сказал: «Мы решили назначить вас народным комиссаром связи. Как вы к этому относитесь?» Трудно передать состояние, в котором я находился в тот момент. Всё что угодно я ожидал от этой встречи, но только не этого. Волнуясь, я ответил примерно следующее: я не так давно окончил академию и работаю менее двух лет. До поступления в академию командовал всего лишь эскадром связи дивизии.

Я совершенно незнаком с предлагаемой мне работой и не в силах справиться с таким огромным масштабом. «Не справлюсь с этой должностью, товарищ Сталин, — сказал я, — и потому прошу не назначать меня на этот ответственный пост». «Что касается масштаба работы, который вас пугает, то это ничего. Мы вам поможем». Я пытался что-то сказать, шёл за ним следом, но Сталин снял трубку телефона и, набрав номер, сказал кому-то: «Наркомом связи назначаем И. Т. Пересыпкина. Завтра опубликовать в печати». Он повернулся ко мне: «Поезжайте сейчас же в ЦК, там подготовьте предложения о составе коллегии Наркомата связи. Если хотите взять с собой кого-либо из военных, хорошо знающих связь, включайте и их в проект решения».

В ЦК, прощаясь со мной, в шутку сказали: «В наркомат в форме не ходите. Там привыкли иметь дело с военными более высоких званий». А ведь я никогда не носил гражданской одежды, и у меня ее попросту не было. Когда после ночной работы в ЦК где-то около 6 часов утра я вернулся домой, жена моя не спала. Она спорила с гимнастерки петлицы, загладила их следы утюгом. Получилась распространенная в то время «наркомовка». Мы с ней выпили по бокалу шампанского из бутылки, оставшейся после первомайских праздников... Утром поехал в Наркомат связи».

До Пересыпкина в 1936–1938 годах в Наркомате связи (НКС) сменились четыре руководителя. Это были крупные политические фигуры, но в ведомстве связи заметного следа они не оставили. Поэтому будни нового наркома начались с разработки «Устава о дисциплине работников связи СССР» и положений: о НКС СССР; об областных управлениях НКС; о районных конторах связи. Впервые руководящие органы связи стали выстраиваться как органы управления отраслью народного хозяйства со своей технической политикой. Уже к 1 сентября 1939 г. был разработан и сводный материал о готовности формирований НКС по семи военным округам. В дальнейшем в новых пограничных регионах ускоренными темпами реконструировали системы связи, настроив их на взаимодействие с

действовавшей в СССР системой, что обеспечило Москве надёжную связь с этими территориями.

ПРЕДВОЕННЫЕ ЗАБОТЫ

Да и по стране у связистов был непопулярный край работы. К сожалению, в СССР исторически сложилось так, что проводная связь имела радиальное построение. Линии связи расходились от Москвы к республиканским и областным центрам, от них — к районным центрам, от райцентров — к сельсоветам, колхозам и совхозам. Поэтому в предвоенные годы начали усиленно строить соединительные линии между районами разных соседних областей, между сельсоветами, колхозами. И, как показал военный опыт, сделанное принесло пользу.

Эти каждодневные хлопоты плавно перетекли в военные заботы, когда настал их срок. И. Т. Пересыпкин вспоминал: «Также имевшийся накануне войны существенный недостаток — это полное отсутствие междугородних кабельных линий и запасных узлов связи. Когда я начал работать в Наркомате связи, специальным постановлением правительства нам разрешили построить в Москве запасной узел связи. К началу войны он закончен не был. Но мы всё же туда аппаратуру внесли, так как если бы, не дай бог, упала бы какая-нибудь крупная бомба на Центральный телеграф, то Москва сразу же лишилась бы всех связей (и телеграфных, и телефонных) со всей страной, по всем направлениям. Мы построили здание в глубине на 35 м, недостижимое для вражеских бомб. К этому узлу были проведены линии связи по линиям метро. Там мы установили несколько передатчиков с антеннами. Но это был единственный узел, который гарантировал нам, что воздушное нападение противника на средства связи нашей столицы не повлияет на их нормальную работу.

Мы хорошо чувствовали неумолимое приближение войны: за несколько дней до 22 июня 1941 г. дипломаты, находившиеся в Москве, никак не могли попасть по телефонным связям в свои страны. Берлин всё время тормозил эти связи. Это было примерно в середине июня, и мы вынуждены были доложить в правительство относительно того, что берлинская

станция саботирует транзитные связи из Москвы с другими государствами.

С первых дней войны все средства и, прежде всего, резервные и запасные узлы были приведены в полную боевую готовность.

Кроме того, в первый же месяц войны своим приказом мы перевели весь руководящий состав наркомата, предприятий связи Москвы, Ленинграда, областных центров, республиканские и областные управления на казарменное положение. Люди постоянно находились на рабочих местах, обеспечивая устойчивую связь.

По плану мы должны были сформировать большое количество частей связи и вместе с телеграфными, телефонными каналами и мощными радиостанциями передать их военному командованию.

Затем мы должны были развернуть огромную сеть учреждений военно-полевой почты».

ВСЯ СВЯЗЬ СТРАНЫ, ИЛИ НАСТОЯЩИЙ ПОЛКОВНИК

22 июля 1941 г. И. Т. Пересыпкина назначили заместителем наркома обороны И. В. Сталина и начальником Управления связи Красной армии с сохранением поста наркома связи. Сразу же повысился статус Управления связи, оно стало Главным управлением (ГУСКА). При этом неизменным осталось звание Пересыпкина — полковник. Правда, в декабре 1941 г. он стал генерал-лейтенантом, а 21 февраля 1944 г. — первым маршалом войск связи.

Войска связи и созданы были под его руководством, на завершающем этапе войны они включали в себя до 10% численного состава всей действующей армии.

В ведении И. Т. Пересыпкина находилось также снабжение войск радиоразведки и правительственной связи, хотя они входили в состав НКВД.

Особенно тяжёлое положение в снабжении действующей армии средствами связи сложилось осенью-зимой 1941 г. Тогда демонтированные заводы электропрома находились в пути на восток или осваивались на новых местах, а поставки по ленд-лизу только начинались. Фронт вплотную подошёл к Москве, где

В конце января 1942 г. ГУСКА сумело организовать воздушный мост Москва — Ленинград. Из блокадного города вывезли часть специалистов завода «Красная заря» вместе с семьями и даже станки. Ленинградцев подлечили, и они смогли приступить к работе

всё возможное тоже было демонтировано, снято и вывезено. С огромным трудом удавалось хоть как-то снабдить связистов вновь формируемых частей.

В такой ситуации решено было воссоздать в Москве два завода в опустевших корпусах на остатках оборудования. В конце января 1942 г. ГУСКА сумело организовать воздушный мост Москва — Ленинград. Из блокадного города вывезли часть специалистов завода «Красная заря» вместе с семьями и даже станки. Ленинградцев подлечили, и они смогли приступить к работе.

Вскоре был пущен и второй завод, производивший радиоаппаратуру из деталей радиоприёмников, сданных населением на склады контор связи в первые дни войны. На радиозаводах в основном работали подростки. «Оба завода вполне оправдали надежды. Они начали выпускать продукцию раньше эвакуированных предприятий. Первый завод за 1942 год выпустил 130 тысяч телефонных аппаратов, более 200 коммутаторов и 20 весьма сложных в изготовлении аппаратов Бодо, второй — более 20 тысяч переносных радиостанций».

ПОД ЛИЧНЫМ КОНТРОЛЕМ

Начиная с московской битвы, И. Т. Пересыпкин неизменно лично на месте контролировал подготовку связи к крупным операциям войск и участие в них связистов. Его сталинградская командировка длилась три месяца.

«В начале ноября 1942 г. Ставка Верховного Главнокомандования командировала меня в район Сталинграда... В предстоящей операции «Уран», имевшей целью окружение группировки фашистских войск, в районе Калача должны были соединиться войска Юго-Западного и Сталинградского фронтов,

которые должны были встретиться на поле боя, действуя навстречу друг другу. Мы отлично понимали, что в случае отказа связи в момент встречи могла возникнуть опасность их взаимного поражения. В штабы участвовавших в этой операции фронтов были высланы все отправные данные, необходимые для организации радиосвязи встречного взаимодействия, как мы ее тогда называли».

Вот отзыв командующего Донским фронтом К. К. Рокоссовского о переменах в состоянии связи под Сталинградом.

В период обороны: «Трудности в поддержании устойчивой связи испытывались не только внутри фронта и армий, но и в общении со Ставкой Верховного Главнокомандования... Самолеты противника непрерывно разрушали проводную связь со штабами соединений, а радиосредствами штабы пользовались неумело... Нередко командиры и штабы не использовали радиосредства, боясь засечки их врагом, что в ходе боя наносило ущерб управлению войсками».

В ходе операции «Уран»: «Основными средствами связи с войсками в ходе операции должны были стать радио и подвижные средства связи. Кроме того, штабы фронтов имели устойчивую проводную связь с армиями и через них со стрелковыми соединениями. На период наступательной операции по ликвидации окруженных вражеских войск заблаговременно была создана сеть командных и наблюдательных пунктов. Основной командный пункт Донского фронта находился в Заворыкине (18 км севернее Фастова) и со всеми армиями имел связь: телеграфную, телефонную, по радио, офицерами связи. Кроме того с армиями имела связь по телефону ВЧ».

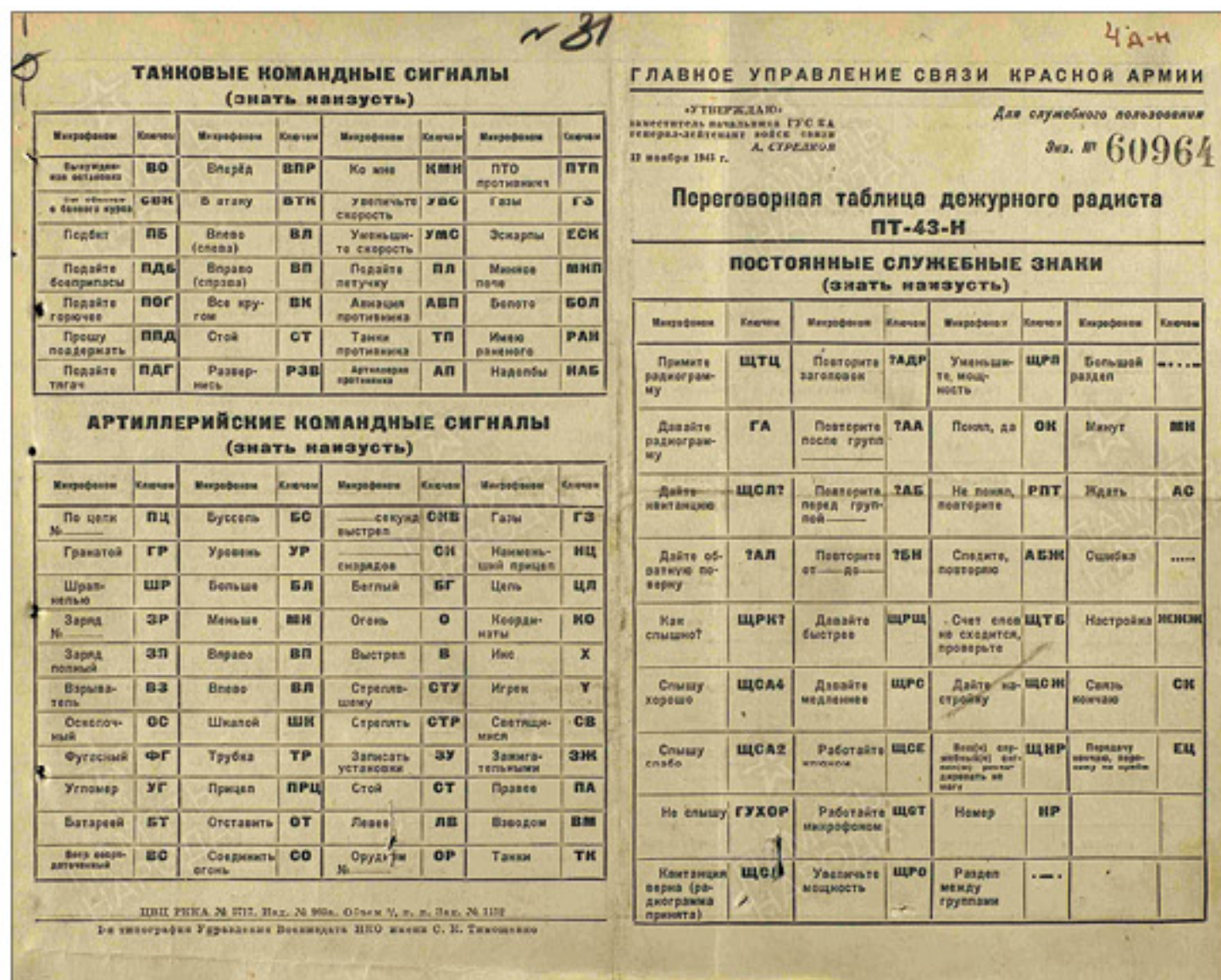


Иллюстрация 2. Переговорная таблица дежурного радиста (лицевая сторона)

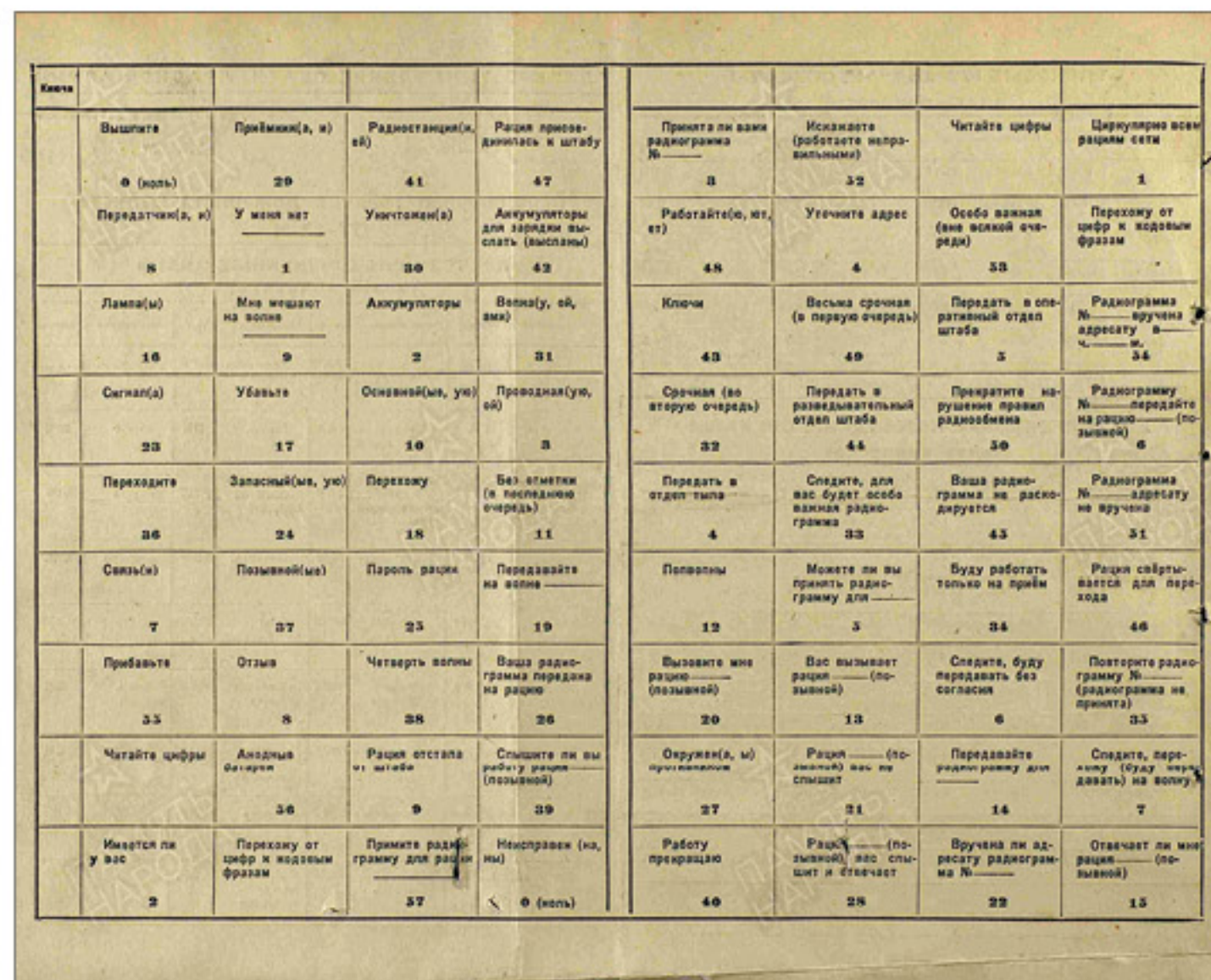


Иллюстрация 3. Переговорная таблица дежурного радиста (оборотная сторона)

ПОБЕДА НАД НЕДООЦЕНКОЙ

Ныне кажется удивительным, как могли советские бронетанковые части и авиация воевать без радиосвязи. На какие ухищрения приходилось идти, какие замысловатые системы «покачиваний» крыльями использовать в воздушных боях. Результатом стали массовые потери вовсе неотсталых боевых машин, а главное, их экипажей. Как известно, эффективное использование танков и самолётов началось в 1943 г., в значительной степени благодаря широкому внедрению радиосвязи в войсках. И роль И. Т. Пересыпкина в этом успехе трудно переоценить. Для этого пришлось победить недооценку радиосвязи. Вот содержание одного из документов начального периода войны, опубликованного на интернет-портале «Память народа»:

«Получена директива Начальника
Связи Красной Армии генерал-лейте-
нанта Пересыпкина 14.2.42 г.

«Отмечаются случаи прекращения работы радиостанций из-за отсутствия на них бензина. Нередко по этой причине не работают и двигатели для зарядки аккумуляторов. Отсутствие запасов горючего на радиостанциях создаёт угрозу потери управления войсками. Продолжают иметь место случаи отставания автомобильных радиостанций штабов из-за плохой проходимости дорог, а выделение тракторов для помощи в движении радиостанциям не организуется. Приказываю:

1. Создать неснижаемый запас бензина для радиостанций и зарядных агрегатов из расчёта пятидневной работы.

2. Все случаи прекращения работы радиостанций из-за отсутствия горючего рассматривать как чрезвычайные происшествия, производить по ним расследование и виновных привлекать к ответственности.

3. При перемещениях штабов выделять в распоряжение начальника связи необходимое количество тягачей для буксировки радиостанций.

О принятых Вами мерах донесите по телеграфу к 15.2.42 г.»»

РАДИОСВЯЗЬ СТАНОВИТСЯ НОРМОЙ

Пришлось ГУСКА преодолеть и радиобоязнь, прежде всего командования.

Некоторые основания «боязни» радиосвязи, конечно, были. Штабы противника в течение всей войны вели активную радиоразведку. Поэтому подавление вражеской радиоразведки являлось важной задачей войск связи, оно во многом способствовало и преодолению радиобоязни. Но гораздо эффективнее подействовало предложенное Пересыпкиным введение штатных, или, как их потом стали называть, личных, радиостанций командующих войсками фронтов и армий. Пересыпкин подчёркивал: «Правило должно быть железным без каких-либо исключений: где бы ни был командующий — радиостанция должна быть с ним. Это подтянет

и нижестоящие штабы: им тоже придётся держать радиостанции рядом». Положение о штатных радиостанциях было подкреплено приказом Ставки Верховного Главнокомандования и явилось первым шагом в осуществлении всестороннего внедрения радиосвязи в войсках. Велика здесь роль и квалифицированных кадров связистов.

В системе Наркомата связи СССР их готовили пять институтов, большое количество техникумов. По данным Пересыпкина, военные связисты обучались в Академии связи, на курсах совершенствования командного состава связистов и в 10 военных училищах связи. Все они в начале войны перешли на сокращённый курс обучения. Например, в Академии связи подготовка инженеров продолжалась только 2 года. А в училищах обучение велось всего лишь 3 месяца. Кроме того, была создана широкая сеть курсов младших лейтенантов связи. На передовой они находились недолго. В среднем через один-два месяца каждый из них или погибал, или получал ранение. Действовали также 10 курсов по подготовке радистов, где их обучали в течение трёх месяцев. В Горьком имелась школа старшин-радистов, которых готовили для работы на мощных телеграфных станциях.

СЕКРЕТНАЯ ИНФОРМАЦИЯ

Всех связистов обучали применению средств засекречивания сообщений. Самыми распространёнными из них

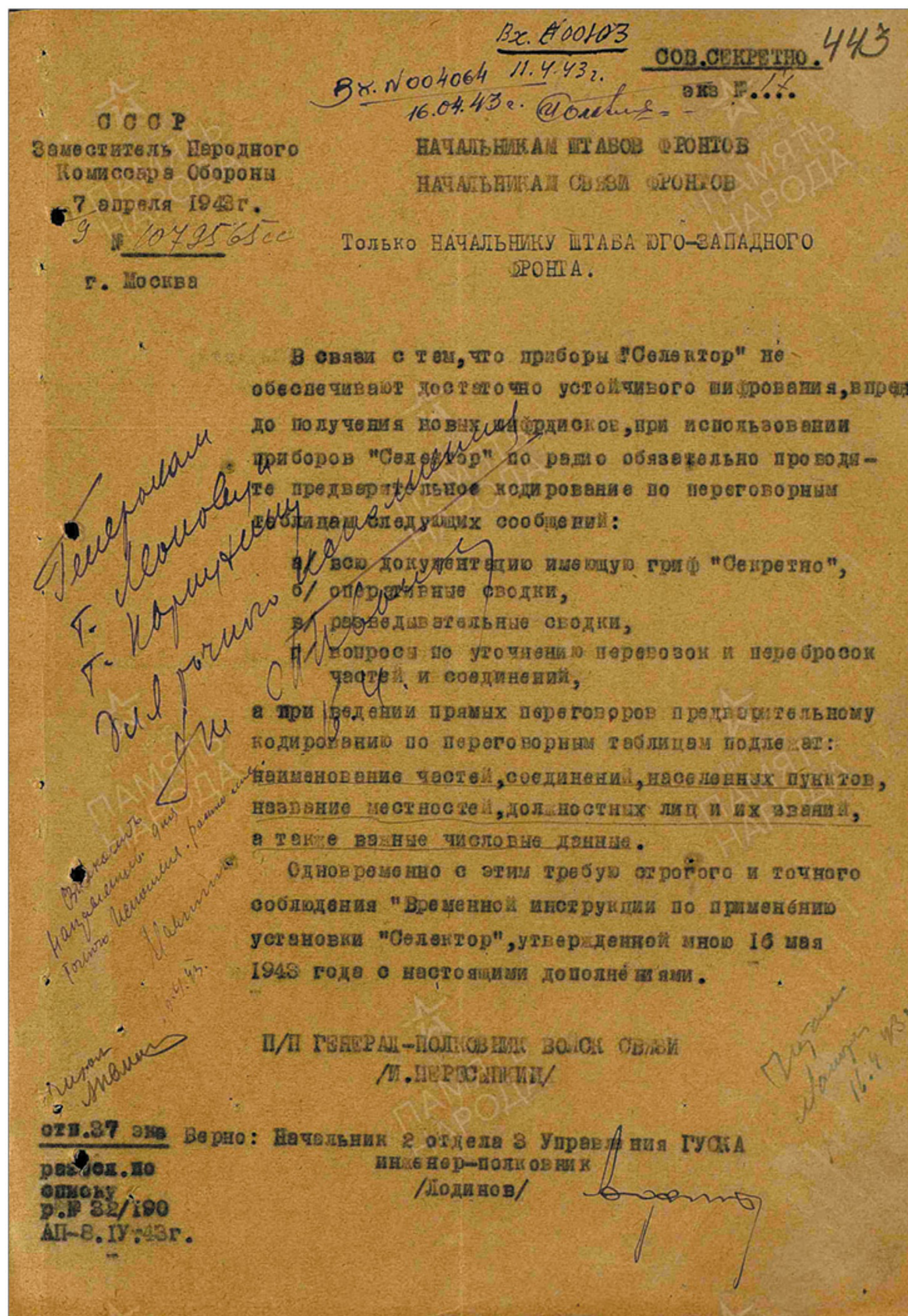


Иллюстрация 4. Распоряжение о применении аппаратов «Селектор»

были разнообразные переговорные и сигнальные таблицы (на иллюстрациях 2, 3), кодированные карты, условные наименования соединений и фамилий командиров. В переговорных таблицах было предусмотрено место для вписывания числового переменного ключа (иллюстрация 3).

Конечно, при необходимости шифровальщики обеспечивали более сложное засекречивание. Документ, приведённый на иллюстрации 4, свидетельствует о постоянном внима-

нии И. Т. Пересыпкина к надёжности шифрованной связи. Вот его содержание: «В связи с тем, что приборы «Селектор» не обеспечивают достаточную устойчивость шифрования, впредь до получения новых шифр-дисков, при использовании приборов «Селектор» по радио обязательно проводите предварительное кодирование по переговорным таблицам следующих сообщений

а) всю документацию, имеющую гриф «Секретно»,



Иллюстрация 5. И. Т. Пересыпкин

б) оперативные сводки,
в) разведывательные сводки,
г) вопросы по уточнению перевозок и перебросок частей и соединений, а при ведении прямых переговоров предварительному кодированию по переговорным таблицам подлежат:

наименования частей, соединений, населённых пунктов, название местностей, должностных лиц и их званий, а также важные числовые данные.

Одновременно с этим требую строгого и точного соблюдения временной инструкции по применению установки «Селектор», утверждённой мною 16 мая 1943 г. с настоящими дополнениями. Генерал-полковник войск связи И. Пересыпкин».

Иван Терентьевич Пересыпкин руководил и военными, и гражданскими связистами СССР до 22 июля 1944 г., с этого времени он сосредоточился на задачах войск связи, а НКС возглавил его заместитель. В послевоенные годы ещё 10 лет, пока позволяло здоровье, он продолжал служить, организуя связь Сухопутных войск. За этим последовала активная общественная деятельность на многих поприщах, в том числе и на посту председателя Федерации радиоспорта СССР.



Дмитрий ЛАРИН
историк криптографии

«ТОРА! ТОРА! ТОРА!»

КРИПТОГРАФИЯ ПРОТИВ БЮРОКРАТИИ, ИЛИ УРОКИ ТРАГЕДИИ ПЁРЛ-ХАРБОРА

80 лет назад, 7 декабря 1941 года, Япония вступила во Вторую мировую войну. Японцы нанесли неожиданный удар по кораблям ВМС США, стоявшим в гавани Пёрл-Харбор на Гавайских островах. Американский флот понёс тяжёлые потери. Было потоплено 5 линейных кораблей, 3 эсминца и несколько вспомогательных судов. Повреждения получили 3 линкора, 3 лёгких крейсера, эсминец, множество лёгких судов. Также было уничтожено 272 самолёта. Людские потери составили почти 3 тыс. человек, включая гражданских. Японские потери составили 29 самолётов и 3 (по другим данным, 5) сверхмалые подводные лодки.

ПРИБЛИЖАЛИСЬ В ТИШИНЕ

При подготовке налёта японцы приняли меры по предотвращению утечки информации через эфир. При движении к Гавайям их корабли и самолёты соблюдали полное радиомолчание. Зато активно работала ложная радиосеть, имитирующая движение японских кораблей на юг в сторону Гонконга и Сингапура. Среди кораблей-имитаторов не было авианосцев. Японцы сняли с них штатных радистов, почерк которых был известен американцам, и перевели на береговые радиостанции, также работавшие в ложной радиосети. Американцы решили, что авианосцы остались на своих стоянках, а часть флота Японии ушла на юг.

Стоит отметить, что ударное соединение шло в режиме радиомолчания.

Единственной радиограммой, переданной в эфир, была «Тора! Тора! Тора!», что по-японски означает «Тигр». Так полковник Мицуо Футида, командир первой волны торпедоносцев, дал приказ о начале атаки. Такое название получил и художественный фильм, посвящённый событиям в Пёрл-Харборе [3]. При этом береговые радиостанции постоянно информировали его командира адмирала Нагумо о перемещениях американских кораблей в гавани Пёрл-Харбора. Таким образом, японские пилоты точно знали, какие цели надо атаковать.

ИЗ ИСТОРИИ ШПИОНАЖА

Впоследствии американцы расследовали причины внезапности и эффективности японской атаки. В первую очередь расследовалась деятельность японской разведки. Интересно, что ещё до нападения американцы развили активную деятельность по пресечению работы японской агентуры. Для этого использовались самые разные, в том числе и запрещённые законодательством США, методы: наружное наблюдение, прослушивание телефонных разговоров и получение копий шифрованных и открытых японских дипломатических телеграмм.

Последнее оказалось нелёгким делом — американские телеграфные компании строго охраняли тайну переписки. Только после личной беседы сотрудников спецслужб с президентом компании RCA 5 декабря удалось получить копии телеграмм, отправленных

японским консулом 3 и 4 декабря. Криптоаналитики на Гавайях немедленно приступили к их дешифровке, но информация в них оказалась малозначительной. Более содержательными были телеграммы от 5 и 6 декабря, но до нападения их дешифровать не успели.

Одним из подозреваемых был генеральный консул Японии на Гавайях Нагао Кита. Приведём выдержку из изложения этой истории советским автором Н. Н. Яковлевым: «Нагао Кито. Это имя нужно поместить в истории шпионажа. Если кто и помог удару по Пёрл-Харбору, то им был Кита. Под прикрытием дипломатической неприкосновенности он передавал в Токио о движении кораблей в Пёрл-Харборе. А теперь, когда удар был нанесён, он стремился уничтожить свидетельства этого. Но стопы бумаг горят медленно. Он (*сотрудник американской контрразведки — авт.*) ворвался в консульство и выхватил у протестовавших японцев шифрованную книгу и кипу донесений. Всё это было передано ФБР США, которое переслало их органам флота для дешифровки» [4].

В результате дешифрования была доказана шпионская деятельность Нагао Кито, а также сам факт подготовки внезапного нападения на Пёрл-Харбор.

БЫЛО И СМЕШНОЕ

В США развернулась активная антияпонская кампания. В агентурной деятельности японцев на Гавайях

подозревали даже собак, принадлежащих японцам. Так, в одном из донесений офицера спецслужбы США на Гавайях сообщалось: «Некоторый бдительный обыватель доложил нашим властям, что на пляже Эва собака лает шифром (!) в направлении подводной лодки японцев у побережья» [4]. Офицер отметил, что заявитель был абсолютно серьёзен и верил в то, что говорил.

Другой «бдительный обыватель» сообщил, что кто-то сигналил закодированным синим светом из района расположения американской базы. Проверка показала, что два фермера доили корову в условиях затемнения, обернув старую лампу синим целлофаном. Мелькание теней рук на её фоне и было «сигналом» [4].

САМЫЙ СЕКРЕТНЫЙ УЛЬТИМАТУМ

Секретность операции достигала такой степени, что даже японский посол в Вашингтоне Номура был не в курсе предстоящих событий. Телеграмма с ультиматумом (из-за её большого объёма она была разделена на 14 частей) была направлена в США буквально в последний момент. В Токио рассчитывали, что Номура передаст этот ультиматум государственному секретарю США К. Хэллу буквально за 20–30 минут до налёта. Принять меры будет уже невозможно, но формальности будут соблюдены. Однако...

Войны, как правило, начинаются рано утром в воскресенье, так было и в этот раз. Но посла об этом не предупредили! Номура спокойно отпустил своих шифровальщиков на выходные. Дежурному шифровальщику справиться с расшифровкой длинной телеграммы быстро не удалось, и ультиматум был вручён примерно через час после окончания налёта. Вот как об этом вспоминает американский госсекретарь:

«Японский посол прибыл в госдепартамент в 2:05 (по вашингтонскому времени — *авт.*) и прошёл в комнату ожидания для дипломатов. Почти в это же время из Белого дома мне позвонил президент. Его голос был спокойным и ровным.

Он сказал: «Пришло сообщение, что японцы атакуют ПёрлХарбор».

Я спросил: «Подтверждено ли это сообщение?». Он ответил: «Нет».

Я проявил желание получить подтверждение, имея в виду предстоящую встречу с японскими послами.

Номура явился ко мне в 2:20. Я принял его холодно и не пригласил сесть.

Номура робко заявил, что он получил инструкции от своего правительства вручить мне в час дня документ, но трудности, встретившиеся при его расшифровании, задержали это вручение. Затем он передал мне ноту своего правительства.

Я спросил его, почему в своём первом обращении ко мне он попросил принять его в час дня.

Он ответил, что не знает, но так-то были его инструкции. Я сделал вид, что просматриваю ноту. Я уже знал её содержание (*откуда Хэлл получил эту информацию, мы расскажем ниже — авт.*), но, естественно, не должен был раскрывать этого. Прочитав две или три страницы, я спросил Номуру, вручил ли он документ в соответствии с инструкциями своего правительства.

Он ответил утвердительно.

Когда я закончил просмотр страниц документа, я повернулся к Номуре и, глядя на него, сказал: «Я должен заявить, что во время моих переговоров с вами в течение последних 9 месяцев я не произнёс ни одного слова неправды. Это абсолютно точно подтверждается протоколами. За все 50 лет моей государственной службы я никогда не видел документа в такой степени насыщенного позорными инсинуациями и ложными утверждениями, настолько чудовищными, что до сегодняшнего дня я не мог и представить себе, что какое-либо правительство на этой планете в состоянии измыслить их».

Номура, казалось, хотел что-то ответить. Лицо его было бесстрастным. Но я чувствовал, что он испытывал огромное эмоциональное напряжение. Я остановил его знаком руки и указал ему на дверь. Посол повернулся и, не говоря ни слова, вышел, понутив голову» [1].

Надежды японских военных сократить время предупреждения американского правительства до минимума не оправдались, таким образом, Япония начала войну без предупреждения. Впоследствии на Токийском процессе

(1946–1948 гг.) нападение без объявления войны стало одним из обвинений, предъявленных японским военным преступникам. Они были осуждены на большие сроки заключения, а некоторые (в том числе два бывших премьер-министра) приговорены к смертной казни через повешение.

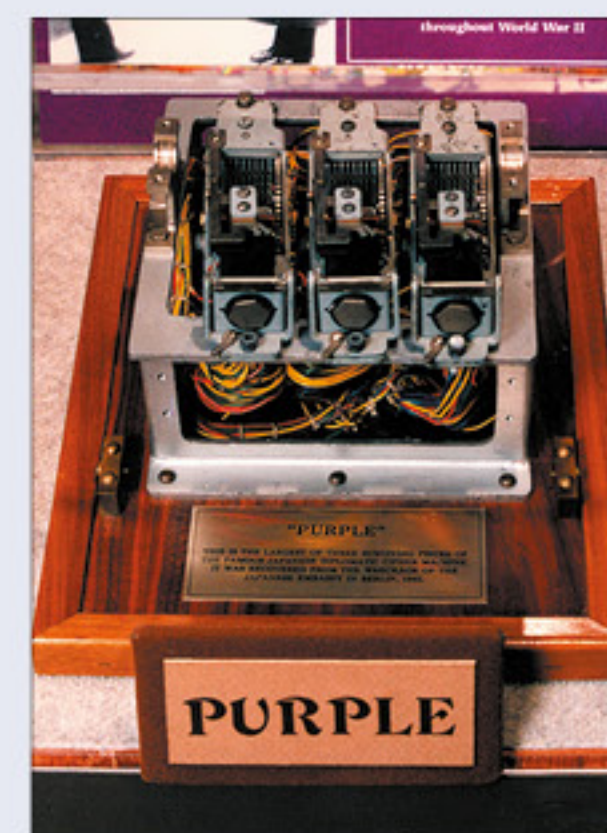
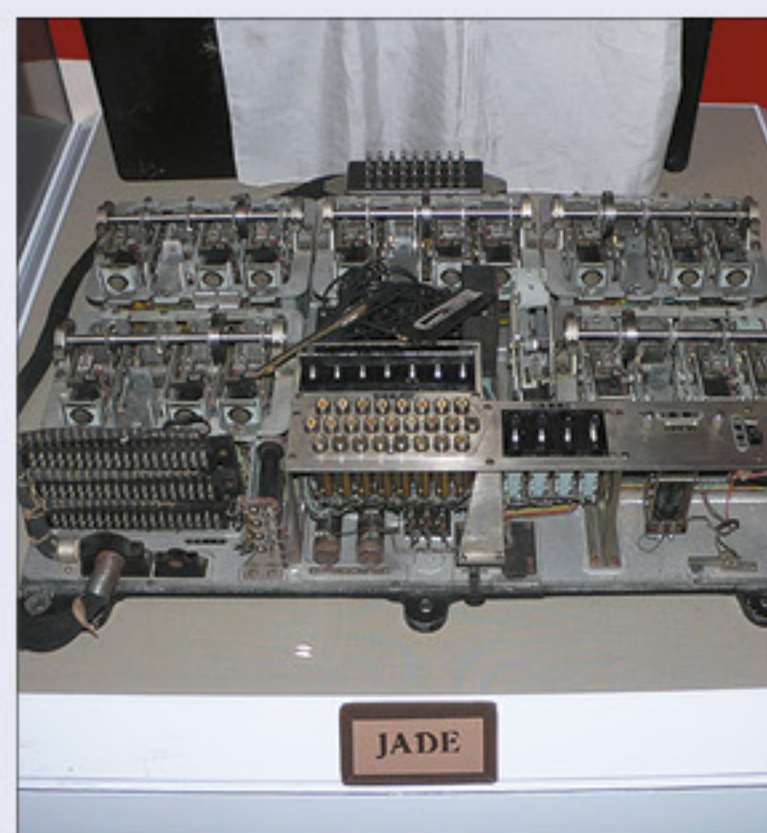
СПЕЦОТДЕЛ РАЗВЕДКИ ВМС США

Но для американцев ситуация сложилась ещё хуже. К тому времени они уже читали японскую дипломатическую и частично военную шифропереписку. Добычей шифров противника (а Япония считалась основным оппонентом США на Тихом океане) занимался созданный в 1916 г. спецотдел разведки ВМС США. Так, в 1921 г. сотрудники спецотдела тайно проникли в нью-йоркское представительство генерального консула и военно-морского атташе Японии и сфотографировали секретный код Императорского флота Японии (по другим данным, американцы проникли в японское консульство в Сан-Франциско).

В 1926 и 1927 гг. спецотдел провёл ещё две удачные операции по добыче новых кодовых книг японского флота. Интересно, что перевод этих материалов длился около пяти лет. Такая неспешность объясняется отсутствием в те годы у ВМС США возможности перехвата радиogramм японского флота. И лишь после получения японских кодов началось формирование в структуре разведки ВМС подразделений радиоразведки и криптоанализа. С этой целью на острове Гуам в Тихом океане был создан Центр электронного шпионажа. На военных кораблях были установлены станции радиоперехвата, подобное оборудование появилось и на некоторых гражданских судах. Были созданы наземные американские базы радиоперехвата: две на Филиппинах и одна в Шанхае.

ЯПОНЦЫ ТОЖЕ НЕ ДРЕМАЛИ

Имелись успехи и у японцев. После того, как в конце 1920-х гг. американский госсекретарь Стимсон (сказав знаменитую фразу «Джентльмены чужих писем не читают!») ликвидировал дешифровальную службу в Госдепартаменте,



Японские шифрмашин: Green, Red, Jade и Purple

«отец американского криптоанализа» Герберт Ярдли остался без работы. Он обратился в японское посольство и предложил продать информацию о методах работы американской дешифровальной службы, в частности, о способах дешифрования японских ручных шифров. Японцы купили эти сведения за 7 тыс. (по другим данным, 10 тыс.) долларов. Эта информация послужила стимулом для начала разработки в Японии электромеханических шифрмашин.

На создание таких машин повлияло и сотрудничество с Францией. Специалист японской разведки по шифрованию Шин Сакума в 1931 г. сотрудничал с французским генералом Анри Картье, считавшимся одним из лучших криптографов своего времени. Во время Первой мировой войны Картье регулярно дешифровывал телеграммы немецкого генштаба, способствуя победе союзников. Он поделился с японцем своими идеями, которые и были использованы при создании первых японских шифрмашин.

Вообще, история появления японских шифрмашин весьма поучительна. Японцы старались получить информацию по криптографии из всех возможных источников. В частности, читать лекции по криптографии они пригласили специалиста по кодам капитана польской армии Яна Ковалевского. Позже к нему в Польшу была направлена группа японских студентов, среди которых был Ризобар Ито (впоследствии крупный японский криптограф), занимавшийся разработкой шифров и

шифрмашин, а также криптоанализом (в частности, он вскрыл шифрсистему типа Playfair, которая применялась в 1930-е гг. на английских линиях связи). Уделяли японцы внимание и организации радиоперехвата. Так, в японских ВМС эта служба начала функционировать в 1929 году [1], [4], [5], [7].

В Японии был разработан вариант «Энигмы» с горизонтальным расположением роторов (кодовое имя, присвоенное американскими криптографами, — GREEN), но он, по-видимому, не был принят на вооружение и мало использовался.

В 1931 г. была создана экспериментальная шифрмашинка Type No.91, но и она не была принята японским флотом. Там предпочитали пользоваться кодовыми книгами. Модифицированная версия Type 91-A была принята японским МИДом для использования полами. К концу 1930-х гг. американские криптографы взломали шифр этой машины, дав ей кодовое название RED.

Хотя Япония и закупала модели «Энигмы», но предпочтение отдавала другой технологии. В 1937 г. был разработан новый шифратор 97-shiki O-bun Injiki (телетайп 97 года для европейских символов; 97 год по японскому календарю соответствует 1937 году) с электрифицированной буквенной клавиатурой. Вместо роторов для шифрования секретных сообщений использовались 4 электрических шаговых искателя, применявшиеся в телефонных и телеграфных станциях. В классе шифрмашин Type-97 капитан ВМС Ризабар Ито, главный проектировщик

Казуо Танаби и его инженеры Масаджи Ямамото и Эйкиши Сузуки разработали несколько моделей, для которых американские криптоаналитики использовали кодовые имена RED, JADE, PURPLE и CORAL. Именно Эйкиши Сузуки предложил использовать шаговые переключатели вместо проблемных «классических» роторных.

Модель Angooki Tairu-B или PURPLE обладала большей стойкостью к дешифрованию, чем первоначальная модель Type 97 print machine или RED. Тем не менее флот Японии долго не знал, что сообщения, шифрованные RED, читаются американцами. А в 1944 г. во время операции на Сайпане была захвачена и машина JADE, похожая на PURPLE.

Шифрмашинки с криптографическим механизмом Type 97 стали использоваться японскими послами и консулами с конца 1938 г. на линиях радиосвязи Токио — Берлин, а также с Вашингтоном, Лондоном, Москвой и нейтральными странами. Шифровальщик сообщений для установления суточных ключей использовал кодовую книгу YO GO, чтобы выполнить 26 проводных соединений и поставить 4 диска в заданное начальное положение, а затем печатал текст. Клавиатура шифрмашинки была латинской, а не катакана, что позволяло также успешно шифровать информацию и на английском языке. Однако для шифрования цифр и знаков пунктуации шифровальщик должен был их конвертировать в трёхбуквенные кодовые слова.

НОЗДРЯ В НОЗДРЮ

В августе 1940 г. крупнейший американский криптограф Уильям Фридман после 20 месяцев упорной работы добился успеха. Его задача состояла в реконструкции сложных внутренних проводных соединений и движений четырёх переключателей, чтобы определить стартовые позиции и ежедневные установки. Фридман и его группа построили логический эквивалент японской криптомашины с использованием шаговых переключателей известной телефонной фирмы «Строуджер» и назвали его PURPLE (пурпурная). С помощью флота США было построено пять аналогов PURPLE.

В конце войны, после захвата японских машин 97-B, выяснилось, что они отличаются от американского аналога всего лишь в двух проводных соединениях.

ПРОСТО КИНО

Японские шифрмашин были введены в эксплуатацию в начале 1930-х гг. Американцы, естественно, постарались получить о них информацию. Для проникновения в японские диппредставительства использовались различные трюки. Так, в кабинете военного атташе Японии в Вашингтоне стала выходить из строя электросеть. Устраняющие неисправность американские электрики всё время норовили оказаться поближе к странной клавишной машине. И хотя официальные американские источники утверждают, что японские «Красная» и «Пурпурная» машины были дешифрованы исключительно аналитическим путём, с большой долей уверенности

можно утверждать, что информация об их устройстве была получена из оперативных источников.

Другая история. Разведслужбы США узнали, что новая шифровальная машина будет доставлена из Токио в японское посольство двумя курьерами по морю. Для ознакомления с ней провели сложнейшую операцию. Сначала американцам удалось на час задержать отправление океанского лайнера, следующего из Токио в США. За это время был найден такой же чемодан, как тот, в котором перевозилась шифрмашинка. Далее был подкуплен профсоюз стюардов, чтобы он бойкотировал рейс. Таким образом, на корабле не хватало стюардов, и некому было доставлять завтраки, обеды и ужины в каюты. Это обстоятельство позволило разлучать курьеров на время приёмов пищи. Кроме того, в пищу курьерам периодически подмешивалось слабительное...

И это только начало. Американцы сделали так, что стала отказывать энергетическая установка: свет то мигал, то светил тускло, а иногда просто гас на время. На злополучный корабль посылались фиктивные предупреждения о циклонах, следуя которым лайнер петлял в океане и опоздал в порт назначения на несколько дней. В операции участвовали люди самых разных профессий: психологи, взломщики, фармацевты, гравёры, электрики, официанты, фотографы... В результате японский шифратор был разобран, досконально изучен и документально зафиксирован до последнего винтика [1].

ПРОКЛЯТОЕ ВОСКРЕСЕНЬЕ

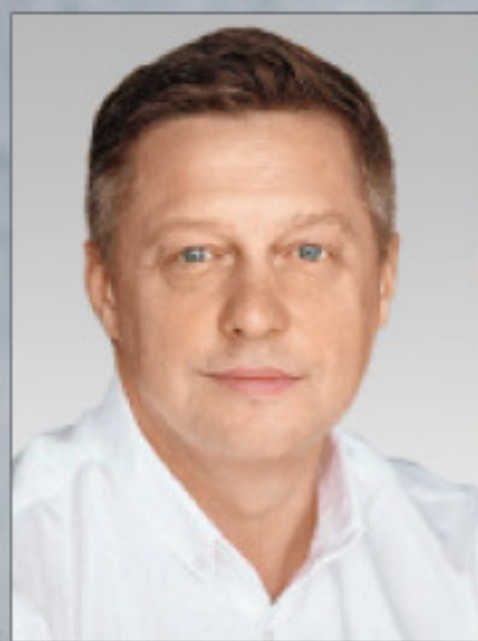
Ирония судьбы: чтение дипломатической переписки Японии позволяло американцам получать массу ценной информации, но самая важная телеграмма — об объявлении войны — хоть и была дешифрована, но не была доложена американскому руководству вовремя. Сыграл именно фактор воскресенья. Все военные руководители США, имевшие полномочия объявить боевую тревогу, отсутствовали: кто был на верховой прогулке, кто на светском рауте, кто на своём ранчо и т.п. Дежурные, а это были младшие офицеры, не входившие в узкий круг получателей информации, добытой дешифровальщиками, не зная её сути, не решались побеспокоить высокое начальство. Начался «перевод стрелок», в результате важнейшая информация была доложена президенту, госсекретарю и военному командованию слишком поздно. До Гавайских островов она дошла уже после налёта [1], [3], [4], [5].

Расследование показало, что криптоаналитики отработали на «отлично», а военная бюрократическая машинка свела их результаты на нет.

Интересный факт. Весной 1941 года японцы через своих агентов получили сведения о том, что их дипломатическая переписка читается американцами. Соответствующие донесения в Токио отправили и японский посол в Берлине Осима, и посол в Вашингтоне Номура. Однако в Токио не поверили этим сообщениям. Там были уверены в надёжности своих шифров. В результате шифраппаратуру заменять не стали, и американцы продолжали контролировать переписку.

ЛИТЕРАТУРА

- [1] Кан Д. Взломщики кодов. М.: ЦЕНТРПОЛИГРАФ, 2000.
- [2] Соболева Т. А. История шифровального дела в России. М.: ОЛМА-ПРЕСС-Образование, 2002.
- [3] «Тора! Тора! Тора!» Художественный фильм совместного производства США и Японии, 1970 г. Известен как наиболее достоверное киноизображение атаки японского флота на Пёрл-Харбор и предшествовавших этому событий. Одна из сюжетных линий фильма рассказывает о работе американских дешифровальщиков <http://ru.wikipedia.org>.
- [4] Яковлев Н. Н. Пёрл-Харбор, 7 декабря 1941 года. Быль и небыль. — М.: Политиздат, 1988. // http://militera.lib.ru/research/yakovlev_nn/index.html
- [5] Kahn D. The codebreakers. N- Y: Macmillan Publ. Co., 1967.
- [6] The New York Times, December 16, 1942.
- [7] Yardley H. O. The american black chamber. Indianapolis, Bobbs Merrill, 1931.



Александр АГАКОВ
коммерческий директор
группы QIWI



QIWI ДЛЯ БИЗНЕСА

ЗАЧЕМ БИЗНЕСУ WHITE LABEL В 2021-М

QIWI сейчас — это группа компаний, в рамках которой мы представляем «КИВИ банк», систему денежных переводов CONTACT, решение для структурированного кредитования МСБ, экосистему для автоматизации маркетинга. Мы появились на рынке как провайдер решений под узкие потребности нишевых сегментов и продолжаем следовать этой модели. Этим объясняется наш профиль работы на стыке B2B- и B2C-рынков: мы развиваем электронные кошельки и денежные переводы, а

также интернет-эквайринг, ДБО, массовые выплаты, факторинговое направление.

Как гибкая и адаптивная финтех-компания, QIWI предлагает сервисы не только для крупного бизнеса, но и для нишевых игроков, чьи потребности не покрыты со стороны финансовых учреждений. В этом помогает широкий продуктовый портфель, развитая омниканальная платёжная инфраструктура, банковская лицензия. Эти же преимущества стали основой для нашей B2B2C-платформы для решений white label.

ЗАЧЕМ ПРЕДПРИНИМАТЕЛЮ «БЕЛАЯ ЭТИКЕТКА»

Платёжная инфраструктура — «кровеносная» система любого бизнеса, поэтому любой предприниматель стремится замкнуть на себе финансовые потоки. Сложнее дело обстоит, когда компании нужна не просто платёжная функция, а инструмент для поиска добавленной ценности к уже существующим продуктам. В таких случаях помогают решения white label.

К white label обращаются игроки разных видов и размеров, у которых нет ресурсов, опыта разработки финансовых приложений и, самое главное, соб-



Получение банковской лицензии, налаживание и поддержание процессинга — долгий и сложный процесс, к тому же регулятором предъявляются жёсткие требования, поэтому купить white label проще и легче

надёжная банковская лицензия, стабильная платёжная инфраструктура и гибкий, современный API. Последний позволяет партнёрам подключаться к платформе и реализовать разные сценарии.

♦ **Коммерциализировать свои core-продукты:** выпускать под своим брендом электронные кошельки и банковские карты, которые можно привязать к системам Apple Pay, Google Pay, Samsung Pay. В результате конечные пользователи нишевых бизнесов, в том числе нефинансовых, получают удобный метод оплаты покупок и совершения платежей.

♦ **Использовать для корпоративных целей.** Здесь в первую очередь речь идёт об оптимизации внутренних процессов, например, более эффективном управлении затратами. Выпущенные кошельки и карты компании могут использовать среди сотрудников, чтобы перечислять средства на питание или суточные в командировках. Для этого можно заранее определить цели, на которые сотрудник может использовать средства.

♦ **Тестирование гипотез и экспериментальные проекты.** Актуально, когда бизнес задумывается о развитии собственного банкинга отдельно или в дополнение к своим небанковским услугам. Хотя мы видим, как бигтехи активно идут в финансовую сферу, результаты их пилотных проектов могут не оправдать вложенные силы и средства. К тому же единичные организации обладают ресурсами, инфраструктурой и банковской лицензией, чтобы позволить себе масштабные разработки. Остальным игрокам, не имеющим возможности купить банк или создать собственный, удобнее и дешевле использовать white label для пилотных проектов.

Флагманский проект в нашем портфолио — платёжная инфраструктура для NUUM. Это приложение для геймеров от МТС, в котором объединены необанк и маркетплейс игровых раз-

влечений. NUUM использует платёжный процессинг QIWI, чтобы выпускать для пользователей виртуальные карты. Их можно использовать для оплаты повседневных покупок и получения бонусов, а также для приобретения предметов в играх, в том числе за счёт накопленных бонусов.

Во всех сценариях, используя white label, бизнес не отвлекается от своей основной деятельности, применяет собственный дизайн и брендинг, а инфраструктурная основа, невидимая для конечного клиента, поддерживается QIWI. Использование white label не должно быть самоцелью — оно помогает создать добавленную ценность к уже имеющимся сервисам, например, повышать лояльность конечных пользователей.

Для подключения white label мы выясняем детали о продукте клиента, цель внедрения, оцениваем, требуются ли доработки. Если потребности типовые и полностью покрываются возможностями решения, то внедрение займёт несколько недель. В случае когда требуется кастомизация функциональности, срок обсуждается индивидуально.

КУДА ИДЁМ

В ближайшем будущем ценность будут иметь сервисы, которые можно легко «упаковать» в гибкий и удобный API. К таковым относится и white label. С его помощью компании могут экономить время и средства, делегируя непрофильную деятельность технологическим провайдерам, обладающим нужным экспертным опытом. В результате выигрывают не только предприниматели, которые усиливают бизнес-ценность своих продуктов, но и рынок в целом. Имея доступ к готовому технологическому бэку, компании делают жизнь клиента проще и могут сосредоточиться на создании принципиально новых сервисов.

ственного процессинга и банковской лицензии. Это могут быть как небольшие компании, например финтех-стартапы, так и устоявшиеся крупные игроки, чья деятельность не связана с банковским рынком. Получение банковской лицензии, налаживание и поддержание процессинга — долгий и сложный процесс, к тому же регулятором предъявляются жёсткие требования, поэтому купить white label проще и легче.

WHITE LABEL В QIWI

QIWI развивает B2B 2C-платформу, в основе которой лежат «три кита»:



Александр БОДРИК
эксперт BIS Journal



КАК СТАТЬ СИЛЬНЕЕ БЛАГОДАРЯ АТАКЕ

ЗАМЕТКИ БЕЗОПАСНИКА

Представим, компания А стала жертвой атаки шифровальщика. Как и у многих, у А бекапы неполны и не протестированы, и восстановление бизнес-процессов является проблемой. Более того, менеджмент понял, что мы интересны атакующим, и требует чёткого плана действий. Как извлечь максимум для укрепления функции ИБ в такой ситуации?

ОПЕРАЦИОННЫЙ УРОВЕНЬ (РЕАГИРОВАНИЕ)

На операционном и самом срочном уровне нам нужно понять, в какую часть сети проникли атакующие, и вернуть себе контроль над сетью. На практике это означает массовые сбросы паролей по всем учётным записям, перезаливы рабочих станций и ревью конфигурации межсетевого экрана. Довольно часто нам придётся де-факто перестроить сеть практически с нуля, так как в силу нулевых стандартов логирования качественно понять, что произошло, невозможно.

В идеале нам нужно понять:

- ◆ кто нас атаковал и почему;
- ◆ каков был вектор атаки и цепь атаки;
- ◆ какая часть сети поражена;

◆ как мы будем реагировать и у кого авторизовать реагирование.

Организации покрупнее готовят-ся реагировать (и находить угрозы в сети) заранее — разрабатывая плейбуки и ранбуки. Остальные могут воспользоваться классической шпаргалкой от команды быстрого реагирования глобального банка с французскими корнями Societe Generale, благо она есть и на русском <https://github.com/certsocietegenerale/IRM>

Кстати, важной предпосылкой для успешного реагирования будет эффективная организация, в частности, устав команды реагирования, где указаны полномочия команды реагирования. Обычно это право получать информацию, право предпринимать определённые действия или право отдавать ИТ-команды на реагирование. Устав может быть и на 1–2 страницы, но его отсутствие в критический момент плачевно скажется на эффективности команды реагирования.

ТАКТИЧЕСКИЙ УРОВЕНЬ

На тактическом уровне наша задача — не допустить повторения инцидента по уже понятному нам вектору атаки. Если в процессе реагирования стало понятно, что не внедрены базовые встроенные

контроли безопасности — нет харденинга, то нужно харденинг реализовать. Как минимум разделение на уровне сети, парольные политики, политики безопасности используемых сервисов — Windows, email и др.

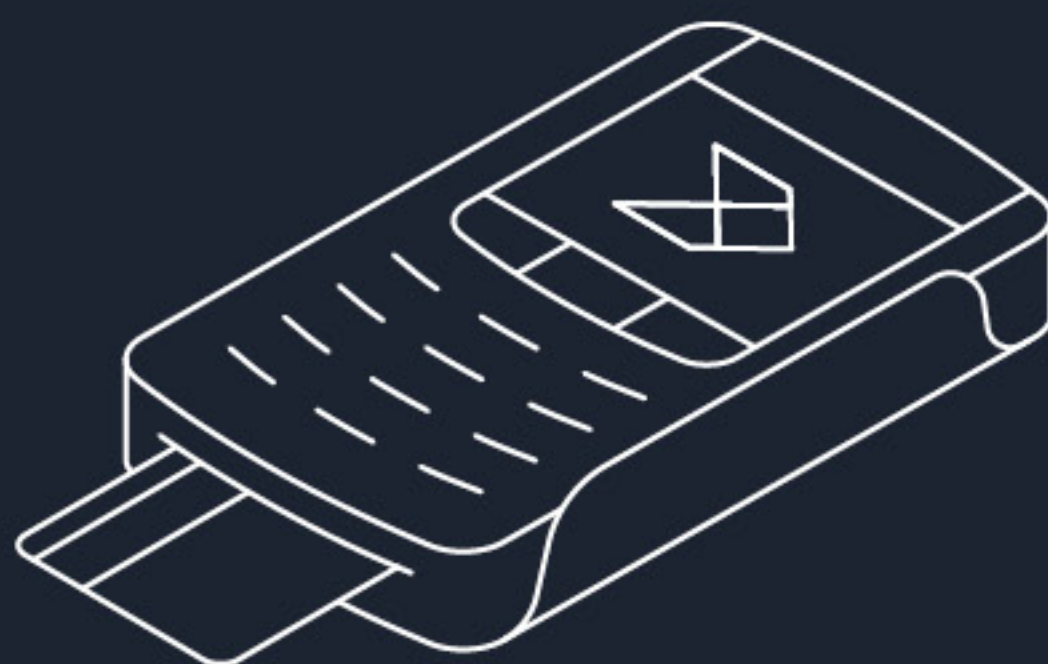
СТРАТЕГИЧЕСКИЙ УРОВЕНЬ

На стратегическом уровне мы используем ситуацию, чтобы выявить бизнес-процессы организации, найти их владельцев, провести с ними интервью, дабы понять цепочку создания ценности организации и требования владельцев процессов к информационной безопасности (например, в разрезе конфиденциальности, целостности и доступности). Конечным результатом может стать security blueprint вместе с приоритизированным набором проектов со сроками и оценками стоимости реализации.

СЕ ЛЯ ВИ

Инциденты случаются, но наша задача — не только отразить атаку, но и воспользоваться ситуацией для того, чтобы наладить диалог по информационной безопасности в организации и трансформировать информационную безопасность в более гибкую, интегрированную и устойчивую функцию.

Платежные решения для бизнеса



> 13 000

бизнес-партнеров

> 106 000

терминалов и точек
приема платежей

128 млрд

платежей в месяц
и переводов
наличными
и электронной
форме

22 года

на рынке
и представлены
в 6 странах

> 28 млн

объединенных клиентов,
которые пользуются
услугами

16,6 млн

виртуальных
кошельков

Гибкая система управления учетными записями

AK | Ankey IDM

- контроль избыточных прав доступа сотрудников
- интеграция с бизнес-приложениями
- совместимость с российским ПО
- экономия до 40 % времени IT-службы
- единый удобный интерфейс
- техническая поддержка 24/7

Кадры

1С

Бухгалтерия

ОС

ERP

СУБ

18+

Реклама

8 (800) 101-71-00

www.gaz-is.ru

GIS

ГАЗИНФОРМ
СЕРВИС