



12> Людмила БОКОВА
Совет Федерации ФС РФ
Рунету — суверенитет!

14> Артём СЫЧЁВ
Банк России
2019-й — год усиления контроля



24> Лев ШУМСКИЙ
Ассоциация ФинТех
О безопасности национальной платформы Мастерчейн

26> Михаил ШАГОВ
Сбербанк
Алексей ФЁДОРОВ
Российский квантовый центр
Квантовый скачок в масштабах банка

88> Александр МЕЛЬНИКОВ
ЦРТ-Инновации
Россияне — чемпионы мира по... идентификации!

СТРОИМ БАНК БУДУЩЕГО





Ежегодные мероприятия в области информационной безопасности:

- **XI Уральский форум** (18–22 февраля 2019 года, республика Башкортостан)
Ключевое мероприятие Банка России по информационной безопасности финансовой сферы.
ural.ib-bank.ru
- **SOC-Форум Казахстан** (18 апреля 2019 года, Астана)
Ежегодная конференция по практике противодействия кибератакам и построения центров мониторинга ИБ. Проводится при поддержке ГТС Комитета национальной безопасности Республики Казахстан.
soc-forum.kz
- **XXIV Конференция «Комплексная защита информации»** (22–24 мая 2019 года, Беларусь)
Конференция Союзного государства России и Беларуси, проводится при поддержке Совета безопасности Российской Федерации.
www.kzi.su
- **VIII Симпозиум CTCrypt 2019** (4–7 июня 2019 года, г. Светлогорск)
Симпозиум «Современные тенденции в криптографии».
Организаторы: ТК 26, Академия криптографии РФ и МИАН им. В.А.Стеклова.
www.ctcrypt.ru
- **V Международная конференция «Актуальные вопросы развития наличного денежного обращения»** (июнь 2019 года, г. Тула)
Международная конференция по безопасности оборота наличных денег и ценностей.
Проводится при поддержке Банка России.
inkas.ib-bank.ru
- **XVII PKI-Форум Россия** (17–19 сентября 2019 года, г. Санкт-Петербург)
Международная научно-практическая конференция, посвященная проблематике инфраструктуры открытых ключей, электронной подписи и электронного документооборота.
Проводится при поддержке Минкомсвязи России и ФСБ России.
www.pki-forum.ru
- **SOC-Форум** (ноябрь 2019 года, г. Москва)
Ежегодная конференция по практике противодействия кибератакам и построения центров мониторинга ИБ. Организаторы: ФСБ России, ФСТЭК России.
soc-forum.ib-bank.ru



Артём ЗУБКОВ
генеральный
директор Медиа
Группы «Авангард»



Игорь НЕКРАСОВ
главный редактор
BIS Journal



Андрей МИНАКОВ
директор
по развитию
BIS Journal

Почти медицинский факт: пульс отрасли, который регулярно фиксирует BIS Journal, в этом году ровный, спокойный. Два года назад в таком же номере, посвященном Уральскому форуму, отмечалось некоторое возбуждение, часто использовались слова «революционный», «футуристический»... Много и с придыханием говорили о цифровом банке, блокчейне, искусственном интеллекте, облаках... Образ банка будущего вызывал волнение и некоторую неуверенность. А будет ли такой банк? А если будет, как его охранять?

Сегодня мы констатируем: 2018 год прошел спокойно, в рабочем порядке. Банк будущего — это уже и не будущее, а реальные контуры небоскреба, взмывающего в небо в соответствии с графиком строительных работ. Со стороны ИБ возведен стройный, крепкий законодательный каркас: работают законы 187-ФЗ, 167-ФЗ, обновлено Положение 382-П. Кредитно-финансовые организации усиленно категоризируют объекты КИИ, строят СОСы, гонят информацию в ФинЦЕРТ и ГосСОПКУ. И футуристический финтех уже — не набор дискуссионных идей, а вполне конкретные инструменты, работающие на прибыль и обсуждаемые с вполне обыденной интонацией.

Ключевое слово тут «обсуждаемые». Вы заметили, становление отрасли во многом идет через слово? Неслучайно именно в сфере ИТ и ИБ проходит так много форумов и конференций. Во многом благодаря именно им заоблачный блокчейн буквально на глазах превратился в конкретную, рабочую платформу Мастерчейн, а искусственный интеллект лишился чудесного футуристического флёра и воплотился в предельно функциональное машинное обучение.

Активный обмен информацией — как обмен веществ — насущная потребность растущего организма, то бишь отрасли. И эта потребность вместе с отраслью только растет.

BIS Journal и Медиа Группа «Авангард», как часть отрасли, прекрасно ощущают эту рвущуюся вперед потребность и откликаются на нее. Журнал увеличивает число полос, сайт журнала и портал www.ib-bank.ru по своей оперативности и информационной насыщенности не уступает ежедневным изданиям, постепенно превращаясь в отраслевое информагентство, BIS TV поражает воображение репортажами и комментариями на злобу дня. Надеемся, всем понравились новые проекты «Наша игра» и BIS Огонёк.

Безусловно, в авангарде наших забот Уральский форум, наша любовь и наша надежда. Он растет год от года вместе с отраслью и по масштабам, и по глубине содержания. По сути — это зеркальное отражение, фото отрасли на память. Десять таких фото мы уже сделали.

Надеемся, одиннадцатое получится не менее красивым.

ОБЩЕСТВЕННЫЙ РЕДАКЦИОННЫЙ СОВЕТ

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, кандидат технических наук, доцент

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. — начальник управления информационной безопасности АО КБ «Златкомбанк»

Вихорев С.В. — заместитель руководителя направления информационной безопасности НТЦ «Вулкан»

Держинский Ф.Я. — главный эксперт — координатор системной экспертизы блока «информационные технологии» ООО «ТехноСофт», CSDP

Зубков А.Н. — генеральный директор ООО «Медиа Группа „Авангард“», директор Фонда содействия развитию безопасных информационных технологий (ФСБИТ)

Курило А.П. — заместитель генерального директора компании «РНТ», кандидат технических наук

Левиев Д.О. — председатель Совета НП «Партнерство специалистов по информационной безопасности»

Мельников С.Ю. — заместитель генерального директора ООО «Лингвистические и информационные технологии», кандидат физико-математических наук

Музипов Ф.Х. — председатель правления НП «Партнерство специалистов по информационной безопасности»

Некрасов И.В. — главный редактор журнала

Окулесский В.А. — заместитель начальника службы ИБ банка «Возрождение», кандидат технических наук

Пазизин С.В. — начальник Управления по обеспечению информационной безопасности ОАО Банк ВТБ, кандидат физико-математических наук

Шумский Л.С. — CISO в Ассоциации «Финтех»

Янсон И.А. — бизнес-партнер по информационной безопасности, Департамент безопасности ПАО «Сбербанк России», кандидат физико-математических наук

ЭКСПЕРТНАЯ ГРУППА

Одувалов М.В. — эксперт BIS Journal

Филипчук А.А. — технический директор ГК ЦРТ

Калашникова Е.В. — Банк ВТБ (ПАО)

РЕДАКЦИЯ ЖУРНАЛА

Главный редактор: **Некрасов И.В.**

Шеф-редактор: **Былевский П.Г.**

Директор по развитию: **Минаков А.В.**

Арт-директор: **Мельников Н.С.**

Обозреватели, корреспонденты: **Бендин С.В.,**

Северный В.П., Хвастунова О.Н., Бродская М.А., к.т.н.

Иллюстрация на 1-й обложке: **Ларичкина О.А.**

Фото в номере: **фотобанк DepositPhotos, Салаватова Я.М., wikipedia.org, waralbum.ru**

Менеджер по распространению: **Кузнецова М.Д.**

Цветокорректор: **Науменко М.Б.**

Корректор: **Бальтерманц Л.Ф.**

УЧРЕДИТЕЛЬ-ИЗДАТЕЛЬ

ООО «Медиа Группа „Авангард“»

Адрес: 127473, Россия, Москва, 3-й Самотечный переулок, д.21 (м. «Достоевская»)

Координаты: 55.779380, 37.61150

Тел./факс: +7 499 271-70-85

Интернет-версия: journal.ib-bank.ru

E-mail: bis@ib-bank.ru

Отдел рекламы: reklama@ib-bank.ru

Отдел распространения: tirazh@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 21.01.2019. Тираж 7000 экз.

Заказ № 4421. Цена договорная.

Отпечатан в «Типографии на Угрешской»

115088 РФ, Москва, ул. Угрешская, д.2, стр.2.

Тел.+7 495 720-62-28

© BIS Journal, 2019



НОВОСТИ

- 5 **В России, законодательство, в мире, технологии, криминал**

РЕГУЛЯТОРЫ

- 12 **Совет Федерации**
Людмила Бокова (Совет Федерации)
Рунету — суверенитет!
- 14 **Банк России**
Артём Сычёв (Банк России)
Повышать ситуационную осведомлённость



БАНКИ

- 18 **Интервью**
Гарегин Тосунян (АРБ)
«Цифровая платформа — это не столько технология, сколько изменение мышления»
- 22 **ФинТех**
Татьяна Жаркова (Ассоциация ФинТех)
Что такое Open Banking?
- 24 **ФинТех**
Лев Шумский (Ассоциация ФинТех)
Защита Мастерчейна
- 26 **Криптография**
Михаил Шагов (Сбербанк), Алексей Федоров (Российский квантовый центр)
От лаборатории к бизнес-приложениям
- 30 **Облака**
Дарья Орешкина (эксперт ИБ)
Стратегический тренд... без стратегии
- 33 **Антифрод**
Александр Вильдман (АО «МТИ Банк»), Руслан Фахретдинов (ООО «Фродекс»)
Антифрод-системы: быстро и дешево
- 36 **Биометрия**
Максим Федотенко (Сбербанк)
Технология защиты от угрозы подмены биометрического сканера



УГРОЗЫ И РЕШЕНИЯ

44 **Дискуссия**

Сергей Вихорев (ООО «ИТ-экспертиза»)
**Дёрни за верёвочку, дитя моё,
дверь и откроется**

47 **ASV-сканирование**

Дмитрий Слободенюк (ARinteg)
**Соответствие стандарту безопасности
платёжных карт**

50 **Законодательство**

Владимир Шилин,
Роман Козырь (АО «РНТ»)
Закон в тренде

52 **Новые технологии**

Роман Жуков (Гарда Технологии)
Гарда Аналитика

54 **Исследования**

Денис Гойденко (Positive Technologies)
Инцидент: почему, как и что в итоге?

56 **Пентесты**

Сергей Нейгер
(Перспективный мониторинг)
Исследования защищённости по 382-П

58 **DSS**

Александра Бялькина
(АО «Кросс Технолоджис»)
Судьба офицера ИБ

62 **Биометрия**

Сергей Агафшин, Татьяна Ларина,
Станислав Смышляев
(ООО «КРИПТО-ПРО»),
Алексей Юдин (ПАО «Ростелеком»)
**ЕБС: от общих требований
к конкретным решениям**

65 **DLP**

Иван Бируля (СёрчИнформ)
«Серебряных пуль» не осталось

68 **Patch Management**

Андрей Перкунов (СТИ),
Сергей Смелов (Ivanti)
Разрывая замкнутый круг



71 **ИБ-системы**

Антон Тихонов (MONT)
**Кибер-обмен — искусство
«самопознания» ИБ-систем**

74 **Электронная подпись**

Денис Калемберг (SafeTech)
**Две стороны мобильной электронной
подписи**

76 **Управление доступом**

Дмитрий Романченко (ИБС экспертиза)
Лучшие практики

79 **IDM**

Марина Доний (Аванпост)
От заката до рассвета

82 **Облачные технологии**

Павел Коростелев (Код безопасности)
**vGate: как защитить частное облако от
рисков?**

84 **Бумажные документы**

Леонид Бондаренко (Сикрет Технолоджис)
Утечки данных

86 **Аудит**

Роман Косичкин (ЦИБИТ)
Аудит как способ повышения доверия

ИНФРАСТРУКТУРА

- 88 События**
Евгений Смирнов, Александр Мельников, Екатерина Крылова (ООО «ЦРТ-Инновации»)
Россияне победили на чемпионате мира по... идентификации!
- 96 Деловые мероприятия**
Александр Бодрик (BIS Journal)
SOC-Форум 2018
- 100 Деловые мероприятия**
Павел Никифоров (BIS Journal)
OFFZONE 2018
- 102 Деловые мероприятия**
Марк Новодачный (BIS Journal)
Кто вы: доктор Джекил или мистер Хайд?
- 103 Деловые мероприятия**
Марк Новодачный (BIS Journal)
ВБА-2018
- 104 Деловые мероприятия**
Подъём с глубины
- 106 Блокчейн**
Александр Колодзей (МГТУ им. Н.Э.Баумана)
Ключ к паутине
- 112 Блокчейн-калейдоскоп**
Анна Катанкина (BIS Journal)
Аргументы против фактов
- 114 Предиктивная аналитика**
Пётр Соломонов (BIS Journal)
Побочные «заработки» ИБ



ОБРАЗОВАНИЕ И КАРЬЕРА

- 116 Круглый стол**
Ещё один Хомо. Куда его?
- 122 Кадры**
Екатерина Зобова (ФСРБИТ)
Целевой набор
- 124 Обзор**
Марина Бродская (BIS Journal)
Обратная сторона золотой медали
- 127 Отцы и дети**
Валерия Мещерякова (BIS Journal)
«В России нет понимания профессии безопасника»

СУБЪЕКТЫ

- 130 История**
Дмитрий Ларин (историк криптографии)
Великая криптографическая битва
- 134 История**
Дмитрий Ларин (историк криптографии)
Шифры двух океанов
- 138 История**
Борис Столпаков (историк криптографии)
«Замрите со склонённой головой при звуках имени его: Макаров...»
- 143 История**
Борис Столпаков (историк криптографии)
«О сколько нам открытий чудных готовят...»
- 148 Мысли вслух**
Михаил Савельев (Информзащита)
Оглянуться вперед
- 150 Заметки безопасника**
Александр Бодрик (ISACA Moscow)
Враги и союзники... процессов ИБ
- 152 Репортаж**
Тридцать пять девушек и один мужчина

ПЕРВАЯ МАССОВАЯ АТАКА В 2019 ГОДУ

Эксперты Group-IB сообщили о масштабной волне вредоносных рассылок группы Silence в России. С начала года это самая крупная атака, насчитывающая более 80 тыс. получателей — сотрудников банков и крупных платёжных систем.

Атака началась с фишинговых рассылок 16 января. Silence замаскировала вредоносное вложение под приглашение на iFin-2019. Интересно, что XIX Международный Форум iFin-2019 «Электронные финансовые услуги и технологии» действительно пройдёт в Москве 19–20 февраля, о чём организаторы мероприятия сделали рассылку 16 января около 9 утра по Москве. Через несколько часов своё «приглашение» отправила Silence. Фальшивая рассылка велась от имени «Forum iFin-2019», но с адреса info@bankuso[.]com. Злоумышленники использовали официальный анонс-приглашение, но отредактировали его.

«Заполните анкету в приложенном архиве и перешлите нам. Вы получите два бесплатных пригластельных и название Вашего банка будет размещено на официальном портале форума», — говорится в письме Silence.

В аттаче к посланию был прикреплён ZIP-архив, внутри которого приглашение на банковский форум и вредоносное вложение Silence.Downloader aka TrueBot — инструмент, который используют только хакеры Silence.



ЕБС. НЕБОЛЬШИМ БАНКАМ ВЫШЛА ОТСРОЧКА

До 1 января 2021 года небольшие банки с базовой лицензией должны будут подключиться к единой биометрической системе для сбора биометрии клиентов.

В соответствующем законопроекте оговаривается, что банки с универсальной лицензией уже приступили к внедрению необходимых инфраструктурных решений, но «банкам с базовой лицензией в силу их меньшего размера требуется больше времени для подготовки и внедрения

механизма удалённой идентификации».

«Обеспечение сбора биометрических персональных данных требует изменения инфраструктуры банков, включая ИТ-доработки в части ИБ, что обосновано в первую очередь необходимостью обеспечить максимальную защиту персональных данных граждан», — говорится в пояснительной записке к документу.

Отмечается, что целевой функционал отдельных подразделений банков (например, операционных касс вне кассового узла) не соответствует тем клиентским операциям, для упрощения которых и вводится сбор биометрических персональных данных. В этой связи законопроектом предлагается конкретизировать виды внутренних структурных подразделений, в которых банки обязаны обеспечить сбор биометрических данных, исходя из осуществляемых ими функций.



СИСТЕМА БЫСТРЫХ ПЛАТЕЖЕЙ

До конца 2019 года система быстрых платежей станет обязательной для системно значимых банков, рассказала глава Банка России Эльвира Набиуллина.

«Очень важный проект запущен в январе — система быстрых платежей. Эта система избавит людей от заградительных комиссий при переводе средств между банками. Сейчас она работает для ограниченного круга клиентов с учётом того, что банкам необходимо адаптировать свои операционные системы, а с конца февраля будет работать для всех банков, которые к ней подключаются. Остальные банки будут присоединяться поэтапно. Мы рассчитываем, что системно значимые банки присоединятся до конца года», — сказала Эльвира Набиуллина.

Соответствующие изменения законодательства уже направлены в Государственную Думу.

ОТДЕЛИТЬ ОВЕЦ ОТ КОЗЛИЩ

Банк России начал маркировку интернет-порталов всех поднадзорных компаний (НПФ, кредитных кооперативов, брокеров, ломбардов и прочих участников финансового рынка).

Инициатива направлена на борьбу с мошенническими сайтами фиктивных финансовых организаций, ущерб населения от которых оценивается в сотни млн рублей. Законопроект, наделяющий регулятора правом на досудебную блокировку лжефинансовых сайтов, одобрен в первом чтении в Госдуме.

Инициативу уже поддержал «Яндекс», который сообщил о 2,5 тыс. промаркированных сайтов. Другие популярные в России поисковики Google и Mail.ru не предоставили комментариев. Эффективность меры будет во многом зависеть от того, как быстро население узнает о значении и важности метки «ЦБ РФ».

ИМПОРТО-ЗАМЕЩЕНИЕ В ДЕЙСТВИИ

Федеральная антимонопольная служба РФ будет бороться с доминированием Google, Apple и Microsoft на российском рынке.

По мнению ФАС, на устройствах российских пользователей должно быть установлено отечественное ПО, в том числе браузер, мессенджер, антивирусное решение, карты и навигатор. Регулятор разработал законопроект, обязывающий производителей электроники устанавливать на свои продукты российское ПО. Инициативу поддержали Mail.ru Group, «Лаборатория Касперского», МТС, «МегаФон» и «Руссофт».

Производители электроники в свою очередь не согласны с ограничениями. Ассоциация торговых компаний и производителей электробытовой и компьютерной техники, членами которой являются Apple, Samsung, Huawei, Google, Philips и пр., написала протест руководителю ФАС.

НОВЫЕ СТАНДАРТЫ НТИ

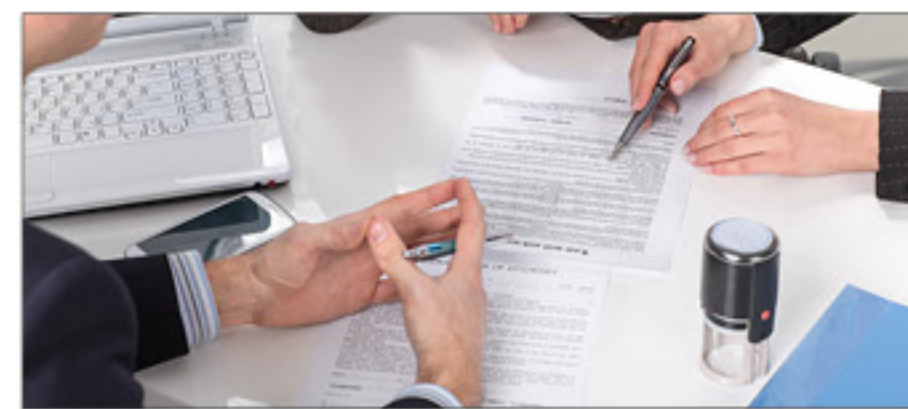
Минпромторг и Росстандарт утвердили Перспективный план стандартизации в области передовых производственных технологий на 2018–2025 гг.

План предусматривает разработку свыше 70 нормативно-технических документов, регулирующих сквозные технологии современной цифровой промышленности. Среди них — интернет вещей, промышленный интернет вещей, большие данные, искусственный интеллект, а также стандарты кибер-физических систем и умного производства. Разработка стандартов позволит снять технические барьеры при внедрении передовых производственных технологий на территории России, а также повысить конкурентоспособность российских компаний и выпускаемой продукции.

«Одним из базовых принципов НТИ является развитие рынков, которые еще не зарегулированы инструментами стандартизации. План разработан

таким образом, чтобы не допустить отставания России по критически важным технологическим направлениям и обеспечить первенство в создании инженерных «правил игры». Первые шаги в этом направлении уже сделаны. В прошлом году РВК через комитет «Кибер-физические системы» инициировала разработку более 30 национальных стандартов, один из них — стандарт интернета вещей NB-Fi — будет утвержден в ближайшее время», — отметил генеральный директор РВК Александр Повалко.

РВК и ТК «Кибер-физические системы» планируют проводить корректировку и дополнение Перспективного плана на ежегодной основе.



iFin-2019

XIX МЕЖДУНАРОДНЫЙ ФОРУМ

19-20 февраля 2019, г. Москва,
«Рэдиссон Славянская»

**Электронные финансовые
услуги и технологии**

Спонсоры



Партнеры



Тематические акценты Форума:

- Современные электронные финансовые услуги для розницы, МСБ и корпораций
- Софт и оборудование для построения ИТ-инфраструктуры цифрового банка и финансовой компании
- Информационная безопасность банков и их клиентов
- Удаленная идентификация, биометрия, ЕБС: перспективы, ожидания и результаты
- От интерфейсов к UX-мышлению - создание функциональных и удобных электронных финансовых услуг
- Использование облачных технологий, Open API, Data Science, Big Data, Machine Learning, IoT для развития электронных финансов
- Маркетплейсы, финансовые экосистемы и небанковские сервисы в ДБО



АССОЦИАЦИЯ
БАНКОВ
РОССИИ

XXI ВСЕРОССИЙСКАЯ БАНКОВСКАЯ КОНФЕРЕНЦИЯ

Банковская система России-2019: пропорциональное регулирование и практика его применения

К участию в конференции приглашены руководители Банка России, федеральных министерств и ведомств, члены Совета Федерации и депутаты Государственной Думы РФ.

На конференции предлагается обсудить широкий круг проблем и задач, связанных с развитием банковского сектора России.

В ходе дискуссий участники смогут обменяться мнениями о текущей ситуации в отрасли, совершенствовании регулирования, применении наиболее эффективных стратегий и моделей банковской деятельности, развитии событий на финансовых рынках.

Подробная информация на сайте Ассоциации банков России: www.asros.ru
Оргкомитет: +7 (495) 785-29-93, +7 (495) 785-29-88,
event@asros.ru

www.asros.ru

29 марта 2019 года

Москва, Кутузовский проспект 2/1, стр.1
отель Radisson Collection Hotel Moscow

ЛИЧНЫЕ ДАННЫЕ ПРЕЗИДЕНТА

Данные личной почты президента Франции Эммануэля Макрона утекли в сеть вместе с 773 млн адресов электронной почты и более 21 млн паролей. Объём выложенных данных составляет более 87 гигабайт. Это одна из крупнейших утечек личных данных в интернет.

Личный e-mail, созданный на почтовом сервере Gmail, Эммануэль Макрон сохранил после прихода в Елисейский дворец и использовал для частной переписки, хотя обычно такое не приветствуется службами безопасности.

В то же время в Елисейском дворце утверждают, что президент регулярно меняет пароль от почты, использует двухэтапную аутентификацию, поэтому информационной безопасности главы государства ничто не угрожает.



КИБЕРАТАКА НА ТИПОГРАФИЮ

Сразу несколько крупных американских изданий не смогли напечатать субботний тираж из-за технических проблем, сообщил телеканал CNN. Среди пострадавших оказались газеты The Los Angeles Times, The New York Times и The Wall Street Journal. Причиной стала кибератака на газетную типографию в Лос-Анджелесе.

Все пострадавшие издания пользуются одинаковым программным обеспечением. Типография принадлежит газете The Los Angeles Times. Кибератака затронула компьютерные системы, отвечающие за процесс печати, пишет AP со ссылкой на источник. Пресс-секретарь The Los Angeles Times Хиллари Мэнинг заявила, что типография работает над устранением сбоя, но не исключила, что проблемы могут возникнуть и с печатью воскресного номера.

США. КУРС О РОССИЙСКОЙ УГРОЗЕ

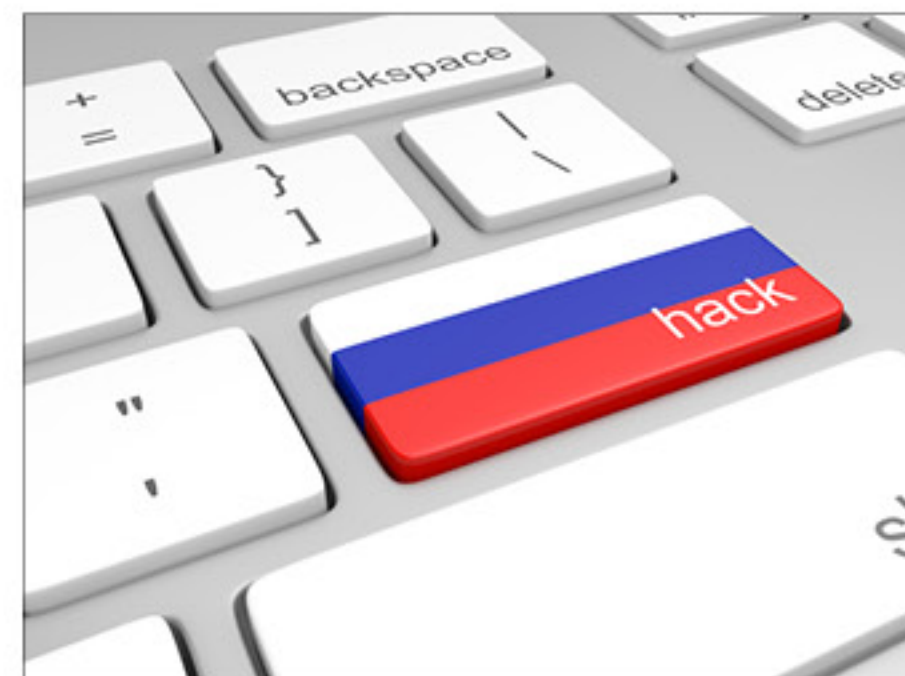
В Джорджтаунском университете в Вашингтоне решили преподавать студентам курс о российской гибридной угрозе. Информация об этом содержится на сайте-агрегаторе, где представлены курсы разных учебных заведений. Курс стартует весной 2019 года.

«Кибератака против Эстонии в 2007 году, вторжение в Грузию в 2008 году, аннексия Крыма в 2014 году. Боты, тролли и информационные операции. Манипулирование, влияние и отрицание. «Нелегалы», «патриотические хакеры» и «маленькие зелёные человечки». Олигархи, компатриоты и полезные дураки. После выборов в США в 2016 году возросла осведомлённость о новом способе ведения войны Кремлём и о том, как он нацелился на наше общество и граждан», — говорится в описании курса.

Курс будет «охватывать российскую доктрину и идеологию, которая закладывает основу для глобального импе-

риалистического бунта Кремля», сказано на сайте вуза. Во время курса планируется рассмотрение примеров, а также исследование тактик и операций, будет изучаться и история подобных тактик ведения гибридной войны. «Материалы курса будут приводиться из первых рук тех, кто находится на передовой линии выявления теневой войны Кремля и противодействия ей», — обещают авторы курса.

Вести курс будет американская журналистка-аналитик, эксперт по информационной войне Молли МакКью.



НОВЫЙ ВИРУС-ВЫМОГАТЕЛЬ

Хакеры создали Djvu, маскирующийся под «кряки» для ПО, на базе известного вируса STOP. Вирус загружает на компьютер четыре файла, которые в несколько шагов подчиняют атакованную машину.

Один из файлов генерирует поддельное сообщение об обновлениях системы Windows, что вводит пользователей ПК в заблуждение. На заражённом компьютере появляется файл с контактами вымогателей. Цену расшифровки хакеры не раскрывают, но обещают сделать скидку на выкуп,

если обратиться к ним максимально оперативно. Djvu практически останавливает работу ПК, так как у вируса есть способность шифровать новые файлы.

Способа вернуть себе данные без помощи хакеров и бесплатно пока не найдено. Аналогичный вирус привёл в конце 2018 года к проблемам на Московской канатной дороге. А ещё один «шифровальщик» WannaCry до сих пор активен в интернете. В 2018 году на его долю пришлось 28% вирусных нападений.



PHD
Positive
Hack
Days

BREAKING
THE CONSTANT*

Реклама



**БИЛЕТЫ
УЖЕ В ПРОДАЖЕ**

21–22 Мая 2019

Более 100 активностей
PHDays9 объединит идея взаимодействия социума и ИТ: доклады и дискуссии с участием признанных лидеров мнений, мастер-классы от ведущих экспертов в сфере исследования безопасности информационных систем, выставочная зона, конкурсы по анализу защищенности всевозможных систем и технологий, умных машин и устройств, музыкальный фестиваль и многое другое.

* Взлом константы

Действительно ли привычные цифровые константы на самом деле неизменны? А что, если их взломать?

На PHDays9 вы увидите в действии эффект «цифровой» бабочки в контексте:

- промышленного IoT, умного дома и видеонаблюдения;
- телекоммуникационных сетей;
- финансовых технологий и блокчейна;
- веб- и бизнес-приложений;
- машинного обучения;
- прикладной криптографии;
- безопасной разработки и автоматизации средств защиты;
- вредоносного ПО и разработки эксплойтов;
- целевых атак и аппаратных закладок.

#PHDays phdays.com

Практические соревнования

в уникальном реалистическом формате The Standoff — грандиозная битва экспертов по взлому и защите информации.

Более 5000 участников:

элита хакерского мира, первые лица, CIO и CISO российских и зарубежных компаний, представители интернет-сообщества и госструктур, регуляторы, политики, теоретики и практики в области медицины и нейротехнологий, деятели искусств и другие.

Открыта регистрация СМИ.

E-mail для заявок:

ysorokina@ptsecurity.com

КРОКУС ЭКСПО
Международный выставочный центр



twitter.com/phdays_ru



facebook.com/PHDays

POSITIVE TECHNOLOGIES

БИТКОИН ПРОВАЛИЛСЯ

Биткоин стал самым провальным инвестиционным инструментом 2018 года. К такому выводу пришли аналитики «ФинЭкспертизы», проанализировав 14 инвестиционных инструментов.

Если в январе инвесторы вложили в биткоин 300 тыс. рублей, то к декабрю они потеряли 213 тыс. или 71,1%. Что касается палладия, то владельцы металла заработали по 10,2% реального рублевого дохода или по 30,5 тыс. на каждые 300 тысяч вложений.

Также эксперты выяснили, что покупательская способность 300 тыс. рублей за год снизилась почти на 3,3%. То есть, если бы инвестор имел эту сумму дома по состоянию на январь, то в декабре на эти деньги он бы купил товаров на 9,8 тыс. рублей меньше.



В ТОМСКЕ ЧИПИРОВАЛИ ПРОРЕКТОРА

В Томском государственном университете проректор по инновационной работе Константин Беляков вживил себе под кожу унифицированный чип.

Это первый в России такой опыт. Чип изготовлен в форме цилиндра, его размеры составляют 4 миллиметра в длину и 1,5 миллиметра в диаметре. Он объединяет в себе функции банковской карты, электронного ключа к объектам Томского университета и транспортной карты «Тройка». К.Беляков считает, что вживлённые чипы безусловно удобны и полезны.

В некоторых европейских странах чипирование активно используется в компаниях, работающих в инновационных сферах. Сотрудники таких фирм относятся к нему не только как к практической необходимости, но и называют себя последователями использования современных технологий.

ГЕНОМНАЯ ИНФОРМАЦИЯ ПОД ЗАЩИТОЙ ГОСУДАРСТВА

Опубликован законопроект о защите геномной информации человека. Указанные нововведения призваны установить дополнительные меры защиты граждан от неконтролируемого распространения личных сведений о человеке, говорится в пояснительной записке.



Проект предусматривает установление в качестве объекта защиты геномную информацию о человеке, полученную из его биоматериала, уточняется на сайте Экспертного центра электронного государства. Такая информация позволяет узнать состояние здоровья, питания, образ жизни, поведенческие особенности, чувствительность к фармакологическим препаратам или аллергенам и другие сведения о человеке.

Законопроект изменит федеральный закон №152-ФЗ «О персональных данных» и статью 39.1 закона №2300-1 «О защите прав потребителей» в части установления особенностей обработки персональных данных, полученных из биологического и генетического материала человека и оказания услуг, связанных с использованием и обращением биологического и генетического материала человека.

СПЕЦФЛЕШКИ ДЛЯ МИНОБОРОНЫ

Минобороны РФ ужесточает правила передачи информации в цифровом формате. Теперь для переноса секретной документации и файлов с пометкой «для служебного пользования» с одного компьютера на другой можно будет использовать только специальные флеш-накопители.

«Секретные» usb-носители централизованно поставляются в вооружённые войска с этого года и бывают двух видов: синего цвета — предназначены для документов «служебного пользования»; красного цвета — для документов под грифом «секретно». Каждая флеш-карта имеет свой уникальный номер и выдаётся ответственному за неё военнослужащему. Для получения доступа к записанной информации необходимо знать пин-код.

Подключаются носители только к компьютерам, на которые установлено специализированное ПО. Машины тоже пронумерованы и закреплены за ответственными лицами. При

этом каждый контакт флеш-носителя с компьютером фиксируется. За потерю секретных носителей, нарушение порядка записи информации на них, а также использование для переноса секретной информации обычных флешек военнослужащему грозит дисциплинарное взыскание в соответствии с уставом в виде увольнения. Если вышеуказанные действия нанесли ущерб безопасности страны, ответственное лицо может быть привлечено к уголовной ответственности за разглашение государственной тайны.



БЭКДОР REMEXI ОТ ГРУППЫ CHAFER

Исследователи «Лаборатории Касперского» обнаружили многочисленные попытки заражения иностранных дипломатических структур в Иране шпионским вредоносным ПО, созданным непрофессионально.

Атаки проводятся с использованием обновлённого бэкдора Remexi, а также некоторых легитимных инструментов. Этот бэкдор предположительно связан с киберпреступной группой Chafer, говорящей на фарси. Ранее она была замечена в киберслежке за людьми и организациями на Ближнем Востоке.

Стоит отметить, что в развивающихся регионах злоумышленники проводят вредоносные кампании, применяя относительно простое самодельное ПО в сочетании с общедоступными инструментами. В этом случае киберпреступники использовали улучшенную версию бэкдора Remexi, предназначенного для удалённого администрирования компьютера жертвы.

Бэкдор Remexi может выполнять команды удалённо и перехватывать скриншоты, данные браузера (включая учётные данные пользователя), данные авторизации и историю, а также любой набранный текст. Украденные сведения эксфильтруются с помощью легитимного приложения Microsoft Background Intelligent Transfer Service. Объединение вредоносного ПО с легитимным кодом помогает злоумышленникам экономить время и ресурсы и усложнять атрибуцию.



АТАКА НА ПРЕЗИДЕНТА РФ

Самая мощная компьютерная атака из-за рубежа была совершена в день выборов президента РФ.

«Максимум новой волны атаки пришёлся на 18 марта 2018 года — день выборов Президента РФ. Основной целью атаки был срыв работы видеонаблюдения за ходом голосования по всей стране, что впоследствии могло развязать кампанию по дискредитации итогов выборов», — сообщил заместитель директора Национального координационного центра по компьютерным инцидентам (НКЦКИ) Николай Мурашов на XXI Национальном форуме информационной безопасности «Инфофорум-2019».

В кибератаках использовалась бот-сеть 30 тыс. компьютеров в 86 странах мира. Ежедневно каждый бот генерировал 15 млрд запросов к DNS-серверам, что создавало запредельные нагрузки.

Всего за шесть месяцев российские специалисты прекратили рабо-

ту 50 тыс. источников атак, выявили использованные злоумышленниками 30 тыс. доменных имён. При этом Мурашов отметил, что объекты критической инфраструктуры РФ подвергаются «изодрённым и целенаправленным» кибератакам из-за рубежа: «Практически все крупные компьютерные эпидемии последнего десятилетия затронули нашу страну. Кроме того, российские информационные системы, прежде всего критической инфраструктуры, подвергаются изодрённым и целенаправленным атакам из-за рубежа».



РЕКОРДНЫЕ 2,2 МЛРД

Одну из самых серьёзных ворованных баз данных, содержащую 2,2 млрд логинов и паролей, начали распространять в Сети. В нее включены данные, добытые хакерами за несколько последних лет.

Возможно, информация была получена из Yahoo, Linkedin и Dropbox при помощи взлома маленьких и не очень известных сайтов. Ранее она в сети не публиковалась. Данным уже присвоили название Collection #2–5. За несколько дней к ним обратились десятки тысяч пользователей.

Специалисты утверждают, что речь идет о самом большом объеме информации, украденном за всю историю интернета. Прошлый рекордный массив содержал 773 млн логинов и паролей и получил название Collection #1.



АТАКА НА ВАШИНГТОН

АРТ-группировка Fancy Bear атаковала Центр стратегических и международных исследований в Вашингтоне.

Суд штата Вирджиния передал специалистам Microsoft контроль над несколькими принадлежащими группировке доменами под общим названием «Strontium Domains». Сайты представляли собой поддельные страницы авторизации во внутренних системах Центра и могли использоваться преступниками для похищения учётных данных и целенаправленного фишинга.

Удалось ли злоумышленникам похитить какую-либо информацию, в материалах суда не указано. Не сообщается также, были ли атаки успешными. С Центром связано множество высокопоставленных лиц, которые могут быть интересны Fancy Bear, в том числе бывший госсекретарь США Генри Киссинджер.

**Людмила БОКОВА**

заместитель председателя Комитета
Совета Федерации ФС РФ
по конституционному законодательству
и государственному строительству,
председатель Комиссии по развитию
информационного общества

РУНЕТУ — СУВЕРЕНИТЕТ!

СОЗДАНИЕ УСЛОВИЙ АВТОНОМНОЙ РАБОТЫ РУНЕТА
ОБЕСЦЕНИТ УГРОЗЫ ЕГО ОТКЛЮЧЕНИЯ ИЗВНЕ

В последние годы Российская Федерация неоднократно оказывалась перед лицом различных внешних угроз её информационной безопасности. Связанных не только с атаками хакерских группировок, но и недружественными действиями на государственном уровне. Чтобы повлиять на наш политический курс, ряд государств предпринимал давление в виде санкций, включая область информационных технологий, в том числе в финансовой сфере.

ИНТЕРНЕТ КРИТИЧЕСКИ ВАЖЕН

Имели место угрозы отключения российских финансовых организаций от международных платёжных систем, включая SWIFT — международную межбанковскую систему передачи информации и совершения платежей. Также под вопросом могла оказаться работа в России VISA и MasterCard. Чтобы нейтрализовать ущерб от подобных возможных негативных действий извне, была создана Национальная платёжная система карт (НСПК) «Мир». Тем самым оппоненты были лишены инструмента политического шантажа, международные платёжные системы лишились части прибыли в России, а у нас заработала отечественная карточная платёжная система.

Однако интернет используется не только российскими финансовыми организациями и платёжными сервисами. Это глобальная международная сеть, многие ресурсы которой задействованы в работе российского сегмента. Доступ в интернет стал очень важной и даже обыденной частью жизни многих россиян. Думаю, сегодня в нашей стране нет людей, которые хотели бы проснуться с утра и обнаружить, что доступ в интернет не работает или работает с серьёзными пе-

ребоями. В интернете не только «живут» и работают рядовые граждане, но и функционирует бизнес, финансовые и транспортные учреждения, государственные органы.

Потенциально угроза отключения российского интернета извне пока остаётся средством политического давления. Нельзя исключать такую возможность под видом «санкций» по надуманным обвинениям. И речь сегодня идёт не о «самоизоляции», как утверждают некоторые СМИ, а о том, чтобы иметь возможность минимизировать ущерб в случае отключения нашей страны от глобальной сети извне.

УНИЧТОЖИТЬ ПОЧВУ ДЛЯ ШАНТАЖА

Создание условий для возможной автономной работы рунета обесценит такие угрозы как средство политического давления на Россию, как это уже произошло на примере карточных платёжных систем. Поэтому сейчас в нашей стране ведётся активная работа по созданию условий для противодействия таким отключениям. Рунет должен быть готов к негативному развитию событий и иметь достаточную техническую инфраструктуру для полноценной автономной работы.

Главная цель законопроекта № 608767-7 «О внесении изменений в некоторые законодательные акты Российской Федерации» — защита от внешних угроз российских пользователей, обеспечение бесперебойной, стабильной работы рунета. В информационной безопасности должны себя чувствовать все — государственные органы, банки, аэропорты, телекоммуникационные компании и другие объекты критической информационной инфраструктуры, и, конечно, граждане.

Авторы законопроекта учитывали экономические аспекты законопроекта, а именно соотношение, с одной стороны,



затрат на создание самодостаточной инфраструктуры российского сегмента интернета, с другой стороны — экономии от оптимизации (локализации) внутреннего трафика и предотвращение ущерба от внешних информационных атак.

Результатом потенциального отключения России от интернета извне могут стать не только паралич или серьёзные затруднения в работе государственных органов, транспорта, связи, энергетики, промышленности и других жизненно важных систем. Это также может создать огромный дискомфорт для большинства наших граждан, который для многих обернётся настоящим шоком. Ущерб в таком случае несопоставимо превысит затраты на создание системы, описанной в законопроекте.

ЦЕНА ВОПРОСА

Были учтены проблемы, сопутствовавшие блокировке Роскомнадзором мессенджера Telegram в 2018 году. Тогда некоторые привычные телекоммуникационные сервисы, не имевшие прямого отношения к работе мессенджера, снизили стабильность работы. Законопроект № 608767-7 будет способствовать «прицельной» блокировке запрещённого контента и сервисов, не затрагивающей «невиновных».

Законопроект предполагает установку технических средств, которые будут обладать возможностью ограничить доступ к ресурсам с запрещённой информацией не только по сетевым адресам, но и путем запрета пропуска проходящего трафика. Такая система, с одной стороны, будет способство-

вать более эффективной блокировке запрещённой информации и ресурсов, а, с другой стороны, можно будет избежать ситуации, когда будут блокироваться смежные с объектом блокировки, но не запрещённые ресурсы и сетевые адреса.

Обязанность обеспечить установку технических средств противодействия угрозам возлагается на операторов связи, оказывающих услуги по предоставлению доступа к информационно-телекоммуникационной сети интернет. В отдельных случаях операторам связи на безвозмездной основе предоставляются технические средства противодействия угрозам целостности, устойчивости и безопасности функционирования на территории Российской Федерации сети интернет и сети связи общего пользования. Эти функции возлагаются на федеральный орган исполнительной власти, осуществляющий функции контроля и надзора в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи (Роскомнадзор).

* * *

Именно Роскомнадзор будет играть ключевую регулируемую роль в реализации законопроекта, в том числе выполнять контрольно-надзорные функции. Также Правительство РФ будет наделено полномочиями по проведению специальных «информационных» учений, направленных на проверку работу системы, установленной законопроектом.



Артём СЫЧЁВ
первый заместитель
директора Департамента
информационной
безопасности
Банка России



ПОВЫШАТЬ СИТУАЦИОННУЮ ОСВЕДОМЛЁННОСТЬ

ЧТО БУДЕТ ДЕЛАТЬСЯ ДЛЯ ОБЕСПЕЧЕНИЯ
ИБ ФИНАНСОВОЙ СФЕРЫ В ЭТОМ ГОДУ



Банком России определены основные направления работы по обеспечению информационной безопасности национальной кредитно-финансовой сферы на 2019 год. По-прежнему ключевой задачей является не допускать увеличения хищений денежных средств в системах электронных платежей, препятствовать росту как количества таких инцидентов, так и похищенных сумм. Очень важно сокращать численность результативных атак на кредитно-финансовые организации и их клиентов. Чего конкретно следует ожидать, что будет делаться в этом году?

2019 год — это время усиления в отрасли контрольной деятельности в отношении того, как выполняются требования к обеспечению информационной безопасности. Важнейшая часть этой работы — ситуационная осведомлённость, оперативный обмен регулятора и всех организаций кредитно-финансовой сферы информацией об инцидентах. Это ин-

формация о том, что именно и как происходит, а также о том, как реагировать. Безусловно, ситуационная осведомлённость будет нами повышаться. Со своей стороны, Банк России будет мотивировать банки улучшать работу по этому направлению, в том числе посредством нормативных актов.

РАЗВИТИЕ ЗАКОНОДАТЕЛЬСТВА

Предстоит дальнейшее развитие федерального законодательства, регулирующего информационную безопасность финансовой сферы. Злоумышленники всё чаще создают интернет-ресурсы, которые нарушают законодательство РФ о финансовом рынке, включая «финансовые пирамиды» и сайты, распространяющие программное обеспечение для «взлома» систем электронных платежей. В Государственную Думу РФ внесён законопроект № 605945–7 о предоставлении Банку России полномочий в досудебном порядке блокировать такие ресурсы.

Также в Государственную Думу РФ внесён законопроект № 545142–7 «О внесении изменений в статью 53 Федерального закона «О связи». Суть его в том, чтобы обязать операторов мобильной связи оперативно сообщать банкам информацию, используемую в дистанционных финансовых сервисах для идентификации клиента и проверки легальности проводимого платежа. То есть информацию о замене SIM-карты, телефонных номеров, установке услуг переадресации голосовых вызовов и SMS, прекращении обслуживания абонента, расторжении с ним договора.

Позиция Банка России такова: эта услуга должна быть доступна для любой финансовой организации, независимо от оператора мобильной связи. Вне зависимости от договорённостей между ними, а по умолчанию, как требование законодательства. Понятно, что услуга эта не может быть бесплатной для заинтересованных в ней финансовых организаций, так как требует от оператора определённых затрат, которые должны компенсироваться.

НОРМАТИВНЫЕ НОВАЦИИ

В Министерство юстиции РФ Банком России были направлены на регистрацию два новых документа, регулирующие информационную безопасность. Эти акты устанавливают базовые требования как к кредитным, так и некредитным финансовым организациям. Риски, характерные для крупной финансовой организации — страховой компании, — сильно отличаются от присущих небольшой — например, ломбарду. Поэтому требования к информационной безопасности финансовых организаций разного масштаба и типа устанавливаются дифференцированные.

Большинство технических требований в этих документах сформулированы не напрямую, а представляют собой ссылки на соответствующие нормы отраслевого стандарта Банка России (действующая редакция СТО БР БФБО-1.5–2018). Таким образом, меры рекомендательного характера, содержащиеся в стандарте, становятся обязательными требованиями для подведомственных организаций. Этот переход, анонсированный три года назад на VIII Уральском форуме «Информационная безопасность финансовой сферы», сейчас совершается.

Выходит и новое положение об обеспечении безопасности платёжной системы Банка России. Вносимые новшества связаны с серьёзными переменами: запуском нового сервиса — системы быстрых межбанковских платежей. Это важная веха для российского рынка финансовых услуг, поскольку позволяет всем клиентам заметно ускорить перечисление денег любых российских банков.

Прежде межбанковские переводы осуществлялись по рабочим дням пятью «рейсами» по расписанию. Время между отправлением и получением денежных средств занимало, в лучшем случае, от нескольких часов, а в худшем, хоть и редко, — до пяти рабочих дней. Время тратилось как на обработку информации на каждом этапе перевода, так и на ожидание следующего.

Переход к быстрым межбанковским платежам требует пересмотра ряда параметров обеспечения информационной безопасности. Во-первых, изменяется конфигурация — цепочка участников перечисления средств, появляется оператор. Во-вторых, сокращается время не только проведения транзакций, но и отведённое для реагирования на возможные инциденты, для противодействия попыткам хищений. Изменения требований к безопасности были продуманы заранее и содержатся в новом нормативном документе, разработанном заблаговременно, до запуска нового удобного сервиса.

ЦЕНТРАЛИЗАЦИЯ АНТИФРОДА

Новым эффективным техническим инструментом обеспечения информационной безопасности в отрасли стала АСОИ — автоматизированная система обработки инцидентов. Это фактически централизованный механизм противодействия банкам попыткам хищений денежных средств в электронных платёжных системах. Запуск АСОИ в эксплуатацию, произведённый ФинЦЕРТ Банка России в конце лета 2018 года, стал возможен благодаря недавним изменениям в законодательстве.

Эти нормы содержатся в Федеральном законе от 27 июня 2018 года № 167-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств». После вступления закона в силу банки обязаны реализовывать меры антифрода — системы мониторинга и противодействия мошенничеству. Кроме того, создана законодательная база для обмена информацией об инцидентах. Банк России получил полномочия формировать такую базу данных и платформу для обмена ими, в том числе о счётах физических и юридических лиц, через которые осуществлялись хищения денежных средств.

АСОИ — инструмент противодействия не только попыткам мошенничества, но и другим информационным атакам чисто технического характера. Тем, что способны нарушить устойчивость функционирования электронных финансовых сервисов — операционную надёжность, непрерывность деятельности. Централизованная база данных формируется на основе информации, поступающей от подключённых финансовых организаций, которая обрабатывается и оперативно доводится до всех участников информационного обмена.

К началу 2019 года все кредитные организации, зарегистрированные на территории нашей страны, подключены к

АСОИ. Начато массовое подключение некредитных финансовых организаций, в первую очередь страховых компаний. К этому обязывает Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 года № 187-ФЗ.

Согласно этому документу, под который подпадают все финансовые организации, они обязаны информировать об инцидентах государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА). АСОИ ФинЦЕРТа Банка России является «единым окном» передачи туда данных об инцидентах информационной безопасности в финансовой сфере. Поэтому и мощность, и функционал АСОИ, и удобство использования для наших поднадзорных будут наращиваться и дальше.

ПРЕИМУЩЕСТВА АВТОМАТИЗАЦИИ

Отчёт ФинЦЕРТ в 2018 году сопровождался «юбилеем» — база данных достигла 10 000 счетов дропперов, которые мошенники используют для вывода похищенных денег.

Динамика наполнения базы данных счетов дропперов непостоянна, есть скачки, подъёмы, спады. В деятельности злоумышленников есть всплески и затухания, в том числе сезонные. Недавняя вспышка их активности отразилась и во всплеске наполнения нашей базы данных. База может сокращаться, если подозрительные счёта закрываются, а банк прекращает обслуживание их владельцев. Или если проверка покажет, что те или иные счёта по какой-то причине попали в базу ошибочно.

Принципиальный момент: это — не «чёрная база». Среди счетов могут быть счета законопослушных граждан и юридических лиц, которые используются втёмную для их владельцев. Поэтому федеральное законодательство обязывает банки принять к сведению данные, что эти счёта могут быть использованы в схемах хищений денежных средств. И более бдительно относиться к операциям, которые совершаются с этими счётами, проверять их легальность.

Банк вправе действовать так, как считает оптимальным в соответствии со своей моделью рисков. Допустим, окажется, что банк был уведомлен о дропперском счёте, но допустил совершение хищения через него. Банку придётся возмещать клиентам ущерб собственными денежными средствами. Не только физическим лицам в силу ст. 9 Федерального закона «О национальной платёжной системе» от 27 июня 2011 г. № 161-ФЗ, но и юридическим лицам.

Кроме того, у Банка России есть надзорные полномочия и возможности применять меры воздействия к банкам, которые игнорируют предупреждения о том, что счёт может быть использован злоумышленниками. Осуществляется самое плотное взаимодействие с правоохранительными органами, которые используют информацию из базы данных дропперских счетов в ходе расследования уголовных дел. Фигурантами этих дел могут оказаться и банки, по недосмотру которых произошли хищения денежных средств. Все эти риски банки должны учитывать.

АСОИ внесла ощутимый вклад в сокращение объёмов хищений в системах электронных платежей. За 8 мес. 2018 года

эта цифра составила 76,5 млн рублей. По сравнению с 1,078 млрд рублей за аналогичный период предыдущего года, это в 14 раз меньше! АСОИ — всего лишь инструмент (но очень хороший) для оперативного информирования, повышения ситуационной осведомлённости участников информационного взаимодействия. Реагирование банков на инциденты стало оперативным потому, что отработаны соответствующие алгоритмы. Банки заранее готовы к тому, что может произойти, и знают, что и как в каких случаях надо делать.

Эффективность выработанных механизмов мониторинга и реагирования показывает не только приведённая динамика многократного снижения объёмов хищений за несколько месяцев. За отчётный период удалось предотвратить попытки хищений у крупнейших российских банков очень значительных сумм. Это результат целого комплекса мер со стороны и Банка России, и кредитно-финансовых организаций, среди которых, в том числе, — запуск и работа АСОИ.

ОТ «ВЗЛОМА» К МОШЕННИЧЕСТВАМ

В связи с повышением эффективности противодействия техническим средствам хищений прогнозируется, что злоумышленники переместят «центр тяжести» своего давления на человека. Доля попыток «взлома» электронных платёжных средств станет относительно меньше, а мошенничеств, обмана, социальной инженерии — больше.

Инциденты, связанные с применением социальной инженерии, также фиксируются АСОИ и подвергаются анализу. Среди новейших тенденций — перемещение атак такого рода с граждан пенсионного возраста на экономически активных. Пенсионеры в массе своей, благодаря информированию их о правилах безопасности при использовании банковских карт и других дистанционных финансовых сервисов, стали осторожными.

Злоумышленники разработали более сложные схемы, рассчитанные на предпринимателей. Например, представляясь им сотрудниками банков, под обещания кредитов выманивают оплату «комиссии за оформление». Учитывая эту тенденцию, будут разрабатываться и применяться меры для профилактики подобных инцидентов и реагирования на них.

Финансовые услуги в электронной форме становятся всё более массовыми и доступными населению. Однако сложно говорить об их качественности без надёжного обеспечения безопасности. Инциденты, связанные с применением социальной инженерии, для клиента болезненны. Они ведут к материальным потерям и снижают доверие обманутого клиента к финансовой системе в целом.

Информационная безопасность включает не только организационно-технические средства, но и понимание сотрудниками и клиентами банков того, как противостоять мошенникам. Повышать грамотность в этой области — общая задача регулятора и финансовых организаций. Например,

АСОИ внесла ощутимый вклад в сокращение объёмов хищений в системах электронных платежей. За 8 месяцев 2018 года эта цифра составила 76,5 млн рублей. По сравнению с 1,078 млрд рублей за аналогичный период предыдущего года, это в 14 раз меньше!

банки могут напрямую обучать своих сотрудников и клиентов правилам безопасности. Это можно делать несколькими путями: тренингами, рекомендациями, специализированной рекламой, индивидуальными разъяснениями и т.п.

БЛИЖАЙШАЯ ФУТУРОЛОГИЯ

В 2019 году предстоит большая работа по внедрению биометрических систем идентификации клиентов, а также осуществление многих других масштабных начинаний, важных для обеспечения информационной безопасности финансовой сферы. Часть из них Банк России уже продвигает при своём непосредственном участии.

Особый интерес представляет переход от сбора регулярной отчётности к анализу инцидентов, первичной информации посредством технологий Big Data, больших данных. За последние годы в финансовой отрасли отмечается заметное сокращение времени, которое занимает путь от формирования идеи до её практической реализации. Банк России фиксирует проблемы на основе информации из многих источников: поступающей отчётности, собственного мониторинга, по материалам взаимодействия с другими ведомствами, жалоб клиентов финансовых организаций.

«Жизненный цикл» нововведений включает такие этапы, как формулировка проблемы, выработка технических и организационных решений, многочисленные обсуждения с отраслевыми сообществами и экспертные заключения, финансово-экономическое обоснование, нормативно-правовое регулирование, межведомственные согласования.

В настоящее время этот цикл занимает в среднем три года. Первый год дискутируем, есть ли вообще такая проблема или она надумана, насколько она серьёзна. Второй год — ищем и находим пути решения, включая нормативные. На третий уже говорим о том, как внедрять решения и внедряем их.

Лучший пример тому — главное отраслевое деловое мероприятие, Уральский форум «Информационная безопасность банков», который в этом году проводится уже в одиннадцатый раз. Можно отследить ретроспективу его программ за последние годы и увидеть, как задумывались и прорабатывались сегодняшние сервисы. И наоборот, кто хочет заглянуть в не столь отдалённое будущее отрасли, пусть ознакомится с нынешней повесткой форума.

«ЦИФРОВАЯ ПЛАТФОРМА — ЭТО НЕ СТОЛЬКО ТЕХНОЛОГИЯ, СКОЛЬКО ИЗМЕНЕНИЕ МЫШЛЕНИЯ»

НА ВОПРОСЫ BIS JOURNAL ОТВЕЧАЕТ ПРЕЗИДЕНТ АССОЦИАЦИИ РОССИЙСКИХ БАНКОВ ГАРЕГИН ТОСУНЯН

ЦИФРОВАЯ ЛИХОРАДКА

— Гарегин Ашотович, цифровая лихорадка — так можно назвать тот технологический шквал, который «накрыл» как развитые, так и развивающиеся страны, — докатилась и до России. В чём это выражается?

— Это неизбежность. Мир меняется, и мы меняемся вместе с ним. Происходящие в мире процессы прежде всего связаны с появлением всё новых и новых информационных технологий; бизнес-моделей применения ИТ, называемых цифровыми, чтобы отличить их от уже традиционных; интернет-устройств и приборов, значительно упрощающих жизнь гражданам, погруженным в «виртуальную реальность». И как главное следствие вышесказанного — появлением нового поколения квалифицированных «продвинутых» потребителей, ориентированных на получение широкого спектра качественных и своевременных услуг, доступных здесь и сейчас.

— А применительно к финансовой сфере каковы технологические тенденции в развитии банковского рынка?

— Во-первых, бизнес банков и клиентское обслуживание перемещаются из офисов и операционных касс в так называемое цифровое

пространство. При этом постоянно увеличивается потребность клиентов в цифровых финансовых сервисах, в том числе предоставляемых через интернет и мобильные приложения. Во-вторых, возрастают требования клиентов не только к перечню, но и к качеству банковских сервисов. Теперь уже банкам для поддержания конкурентоспособности нужно формировать индивидуальные предложения для клиентов. Поэтому, как следствие из первых двух, вытекает третья тенденция, а именно — осознанная банками необходимость трансформации своих бизнес-моделей и информационной архитектуры.

Трансформация бизнес-моделей — это в первую очередь предоставление финансовой услуги не в офисах банка, а там и тогда, где и когда такая услуга востребована клиентом. Это может быть как чисто финансовая услуга (например, банковский перевод), так и часть комплексной услуги (например, покупка автомобиля за счёт кредита или оплата ЖКХ).

ФРОНТ-ОФИС И БЭК-ОФИС

Если говорить о трансформации информационной архитектуры, то популярные до недавнего времени одновендорные системы, главное преимущество которых состоит в единообразии «монолитных» решений, уходят в прошлое из-за их тяжеловесности и неприспособленности к быстрым изменениям.

Сейчас передовые банки технологически разделены на фронт-офис и бэк-офис. У некоторых из них традиционные АБС превратились в отдельные приложения для сборки и консолидации бухгалтерского учёта — так называемые

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



машины проводок. Без разделения технологий банка на фронт- и бэк-офис невозможен переход к цифровому банку.

— Почему невозможен?

— Потому что требования разные. Клиенто-центричный фронт-офис должен быть быстрым, гибким и безопасным, т.е. «мгновенно» предоставлять индивидуальные сервисы под требования конкретных клиентов путём внесения конструктивных, функциональных или дизайнерских изменений, осуществлять внедрение новых услуг и компонентов без остановки действующих сервисов. Также фронт-офис должен позволять подключение к нему новых клиентов банка. Специалисты говорят, что это делается с помощью открытых API-интерфейсов — это также важная часть цифровой трансформации.

Требования к бэк-офису лежат в других плоскостях: он должен быть стабильным и безопасным, ориентированным на транзакции, а не на клиента. При этом бэк-офис должен по своей информационной архитектуре поддерживать фронт-офис и адаптироваться под все его изменения.

СМЕНА ВЕКТОРА

— В чём суть «цифровой трансформации»?

— В переходе от документо-центричности деятельности к дата-центричности.

Сейчас большинство банков ориентированы на финансовые документы (платёжные поручения, кредитные договоры, гарантии и пр.), а основной актив цифровой организации — это её данные. Дата-центричность предполагает учёт не только цифр, счетов, проводок, документов, но также их семантического смысла, т.е. должно быть единство формы и содержания.

Именно такой подход позволяет сделать клиента центром банковской деятельности, привязать к нему не только историю использования клиентом предоставляемых банком услуг, но и прогнозировать его поведение, выявлять потребности и предпочтения.

Выявление потребностей и квалифицированное согласие клиента порождают автоматические цепочки операций. Только вот автоматические цепочки операций запрограммировать легко, а гарантировать их правильное выпол-

Гарегин Тосунян,
президент Ассоциации
российских банков,
доктор юридических
наук, член-
корреспондент РАН

нение — трудно. Это и осуществляется благодаря цифровой трансформации, которая позволяет повысить эффективность банковской деятельности и в разы снизить себестоимость операций.

ЗАМЕЩАТЬ, А НЕ УЛУЧШАТЬ

— Очевидно, что цифровизация охватывает всё большее число банков. Однако, чтобы действительно стать цифровой отраслью, банкам предстоит огромная работа.

— Использование технологии Банк-Клиент и создание полнофункционального мобильного приложения — это лишь маленький шаг к массовости и цифровизации. В идеале финансовая цифровая услуга должна начинаться со стадии проектирования и оставаться цифровой от начала до конца. Она должна быть и проще, и оперативнее, чем услуга обычная — аналоговая. При этом цифровая трансформация должна именно замещать нерациональную организационную структуру, а не улучшать её.

Однако не всегда получается полная замена аналоговой услуги на цифровую. То же можно сказать и про цифровую трансформацию. В этом случае необходимо будет уже «перестраивать» аналоговую услугу в цифровую, а так называемую нерациональную организационную структуру — в цифровую. При этом, к сожалению, будет затрачиваться больше ресурсов, как человеческих, так и финансовых.

В организационной части при цифровой трансформации необходим переход от исторически сложившихся подразделений к кросс-командам, объединяющим бизнес, ИТ и маркетинг, — к так называемым «цепочкам доставки ценности». Требуется ускорение циклов производства, сокращение «time-to-market» — времени вывода финансового продукта на рынок.

Банки должны приспосабливаться к изменениям внешней среды, вливаясь в так называемые финансовые экосистемы, — динамичные и совместно развивающиеся сообщества, состоящие из разнообразных субъектов, создающих и получающих новое содержание в процессе как взаимодействия, так и конкуренции.

При этом выживает не самый сильный и не самый умный, а тот, кто лучше всех приспосабливается к изменениям.

— Если конкретно, в чём заключается основная, приоритетная задача банка?

— Сделать клиентов частью своей экосистемы. Важная часть экосистемы — наличие информационного обмена, в процессе которого клиент оставляет «цифровые следы». И банки при принятии решений должны опираться на информацию, которая генерируется поведением клиента при взаимодействии с ними. Здесь включается логика «контрольно-следовой полосы». То, что мы раньше использовали для защиты — «обнаружить и пресечь», теперь используется для обслуживания, если хотите, для заманивания клиента. Логика информационной защиты теперь становится источником новой функциональности. Важна постоянная работа с клиентом, даже когда он не обращается в банк.

ЦИФРОВАЯ ФИНАНСОВАЯ ПЛАТФОРМА

Для реализации сказанного необходима цифровая финансовая платформа, предусматривающая разнообразные модели взаимодействия, в которых разрешается и поощряется участие сервисов или приложений третьих сторон в цепочке предоставления услуги. Платформа будет одна, а вот приложений может быть много.

Я соглашусь с мировыми консультантами в том, что цифровых платформ развития не может быть много.

Действительно, создание полноценной цифровой платформы не под силу каждому банку. Это дорогое удовольствие. Поэтому должна произойти серьёзная консолидация банковской системы, т.е. построение цифровой финансовой платформы силами нескольких, заинтересованных в инновациях банков. При этом важно, что сохраняется их юридическая независимость, т.е. без фактического слияния банков.

Если банк не в состоянии построить свою цифровую платформу, он может подготовить и отдать на совместную платформу своё приложение. После этого в силу вступают принципы конкуренции — у кого лучше приложение, тот и в выигрыше.

Инновации должны поддерживать процесс удовлетворения клиента. Причём необязательно банку осуществлять это собственными силами. Можно привлекать игроков с рынка. Главное — это то, что экосистема на совместной цифровой платформе должна быть открытой. Более эффективны для финансового сообщества

При цифровой трансформации необходим переход от исторически сложившихся подразделений к кросс-командам, объединяющим бизнес, ИТ и маркетинг, — к так называемым «цепочкам доставки ценности»

именно открытые экосистемы с размытыми границами, позволяющие привлекать новых участников и сокращать издержки производства за счёт привлечения ресурсов со стороны. Вспомните про API-интерфейсы, о которых мы говорили в начале беседы.

Нужно, чтобы клиент получал ответ на интересующие его вопросы не от Гугла или Яндекс, а от банка. От Своего банка. Например, на вопрос: «Могу ли я получить банковскую гарантию и за какую цену?», он должен получать ответ сразу же, а не после оформления кучи бумажных документов.

Подводя краткий итог, можно сказать, что цифровая платформа — это не столько технология, сколько изменение мышления в условиях цифровой экономики.

О БЕЗОПАСНОСТИ

— Давайте перейдём к проблемам информационной безопасности. Не является ли цифровая революция угрозой безопасности для банковской деятельности?

— Использование новых технологий всегда создаёт новые риски. Но об этом чуть позже. Сначала хотелось бы акцентировать ваше внимание на том, что с точки зрения безопасности информация характеризуется ещё и направлением. Если пользователь берёт информацию из внешней среды, то защита такой информации — это проблема самого пользователя. Но если он отдаёт информацию во внешнюю среду — в некую «центральную базу», и эта информация влияет на общество (например, расписание поездов или прогноз погоды), то задача защиты этой информации приобретает не только глобальный характер, но и большую важность.

Как было уже сказано, новые технологии создают новые риски. Традиционный подход к обеспечению информационной безопасности опирается на определённую, как правило, достаточно грубую категоризацию объектов информационной инфраструктуры, и затем, в зависимости от категории объекта, — на применение заданного перечня мер безопасности. При этом обоснование именно таких, а не иных мер в конкретной ситуации в нормативных документах, как правило, отсутствует (в какой мере и какие риски при этом снижаются — вопрос). В результате задача обеспечения безопасности на практике подменяется задачей соответствия этим требованиям, а это не одно и то же.

Представляется, что в условиях динамичной цифровой трансформации такой подход не эффективен, потому что мы всегда будем отставать

Обеспечение безопасности должно быть доказательным, а предлагаемые требования — обоснованными.

Без этого услуга не должна предлагаться клиенту банка

(в том числе и в части нормативного обеспечения) и недостаточно точно соответствовать многообразию профилей рисков, которые быстро меняются. Никакой регулятор за этим не угонится.

Нужен переход от соответствия требованиям к предоставлению безопасных услуг.

— Что такое безопасная услуга?

— Это услуга, при предоставлении которой риск инцидентов понижен до заданного минимума.

Для этого необходимо идти, отталкиваясь от нарушений, которые не должны быть допущены, к мерам доказательного их предотвращения. В этом направлении уже есть некоторые подвижки, но не более.

НА ЯЗЫКЕ БИЗНЕС-ПРОЦЕССОВ

Инциденты должны быть сформулированы на языке бизнес-процессов или предоставляемых сервисов (например, хищения, несанкционированные переводы денежных средств, нарушения прав субъектов, несоблюдение норм права). Обеспечение безопасности должно быть доказательным, а предлагаемые требования — обоснованными. Без этого услуга не должна предлагаться клиенту банка. Кроме того, должны сразу прорабатываться и меры нейтрализации последствий нарушения безопасности услуги — от страхования до юридических процедур (например, восстановление идентичности). При этом утверждения о надёжности защиты не должны являться основанием для отказа от проработки таких мер. И не нужно механически перекладывать эту работу на суды! Это им просто непосильно, к тому же судебные процессы протекают всегда очень медленно.

* * *

Роль цифрового сообщества — предложить и обсудить в профессиональной среде алгоритмы реализации этого подхода, а также критерии приемлемости риска нарушений и другие сопутствующие вопросы в тесном контакте с регуляторами, которые реализуют это уже в нормативных документах.



Татьяна ЖАРКОВА
управляющий
директор Ассоциации
ФинТех

ЧТО ТАКОЕ OPEN BANKING?

ПОЧЕМУ БОЛЬШИНСТВО ЦИВИЛИЗОВАННЫХ СТРАН ПЕРЕХОДЯТ НА НОВЫЕ СТАНДАРТЫ БАНКОВСКОГО ОБСЛУЖИВАНИЯ? ПОЧЕМУ НАЗРЕЛА НЕОБХОДИМОСТЬ В ФИНАНСОВОЙ РЕВОЛЮЦИИ, И КТО В ИТОГЕ ПОЛУЧИТ НАИБОЛЬШУЮ ВЫГОДУ ОТ ПЕРЕМЕН?

В октябре 2018 года в Сочи прошёл Форум инновационных финансовых технологий FINOPOLIS. На одной из рабочих сессий обсуждали общемировой тренд — Open Banking. Провела сессию Татьяна Жаркова — управляющий директор Ассоциации ФинТех. Её собеседниками были авторитетные российские и иностранные финансисты, которые делились опытом работы по новым стандартам.

ТРЕНД И ФЕНОМЕН

Как прозвучало на форуме, в ближайшее время почти половина стран Большой двадцатки будет вовлечена в работу над созданием стандарта открытых интерфейсов программирования (Open API). Это необходимость, продиктованная последними тенденциями мирового финансового рынка. В Европе с начала 2018 г. вступили в силу требования ко второй редакции платёжной директивы. В её рамках банки обязаны открыть посредникам доступ к информации по счётам клиентов и обеспечить им возможность осуществления платежей. Параллельно с Европой с подобными инициативами выступили Индия, Сингапур, США и Австралия.

Open Banking уже стал международным трендом. Что принципиально нового появится в финансовых секторах разных стран с внедрением открытого банкинга, и в чём будут различия? Как регулировать участников рынка, одновременно предоставляя им больше возможностей в выборе методов и технологий?

Open Banking — это, своего рода, феномен в финансовом секторе, потому что банки начали делиться информацией с третьими лицами. Безусловно, для этого нужно заручиться принципиальным согласием клиентов на использование

их персональных данных. И, если эта информация не принадлежит ещё какой-либо сторонней организации, её открытие и использование в банковском секторе даст дополнительные возможности для выработки наиболее эффективных финансовых решений.

ПЕРВЫЕ ШАГИ

Кстати, большинство крупных банков в странах, где внедряется Open Banking, были далеко не в восторге от необходимости делиться своими данными с другими участниками рынка, зачастую — своими прямыми конкурентами. Пионерами по использованию Open API стала Великобритания. Процесс запустило Агентство по конкуренции, что, в общем, вполне логично. Стандарты раскрытия информации коснулись девяти крупнейших банков. Аналогично внедрение Open Banking происходило и в Австралии. Сначала обсуждали местные платёжные системы и их трансформации. В правительстве страны высказали мнение, что закрытые системы неизбежно приводят к монополиям и блокируют возможность быстрого экономического роста других участников рынка. И тогда Комиссия по конкуренции обязала четыре крупнейших банка страны в течение года опубликовать Open API, которые раскроют информацию о счётах клиентов.

«Изначально большинству банков не слишком понравилась эта идея, — рассказала стратегический директор Australian Payments Network Limited Виктория Ричардсон. — Но сейчас появился существенный сдвиг — банки привыкли к новым условиям и уже рассматривают возможности, которые получили от этого вынужденного сотрудничества». Австралийские финансисты опирались на опыт британских коллег.

ОСОБАЯ РОЛЬ ИБ

В Open Banking доступ к клиентским данным могут иметь огромное количество компаний, поэтому банки должны чётко разграничивать и контролировать доступ к ним третьих лиц. Мировой опыт в этом уже наработан. В России Центральный Банк РФ уделяет особое внимание защите информации автоматизированных систем, внедряемых в банках. Регулятор выпустил несколько стандартов и руководящих документов в области ИБ. Требования этих документов будут учтены при разработке открытых API в России.

В ЕВРОПЕ И США

Если в Европе банки обязаны открывать свою информацию любому, кто имеет аккредитацию регулятора, то США выбрали другой путь. Заокеанские банкиры сами решают, кому предоставить данные, кому выдать аккредитацию и какие требования при этом выставить. Впрочем, в американском банковском секторе грядут большие перемены. Минфин США запускает процесс перехода к европейской модели. «Крупные банки регулируют финтех-компании и доступ к данным для своих конкурентов. Это выглядит очень странно, — заявил председатель Ассоциации финансовых данных и технологий (FDATA) Гэвин Литтлджон. — Сейчас мы пытаемся распутать «клубок спагетти» этих двусторонних договоров и создать открытую прозрачную базу».

В РОССИИ

Всемирная тенденция открывать банковскую информацию совсем скоро коснётся и России. Технологические решения для отечественных банков уже обсуждаются. По результатам пилотных проектов будет прорабатываться законодательная база.

«Стремление к строительству экосистем диктует необходимость идти в сторону открытых интерфейсов и стандартов, которые помогут общаться не только внутри банковской сферы, но и выходить за пределы банковского сообщества, распространять Open API на как можно большее число связанных и не связанных с банкингом секторов экономики», — считает заместитель президента-председателя правления Банка ВТБ Ольга Дергунова. По её словам, Россия сейчас находится в роли догоняющего, это позволит учесть ошибки первопроходцев и внедрить новые стандарты быстрее.

НЕ ВЫГОДНО ОДНОМУ СЕГОДНЯ, ВЫГОДНО ВСЕМ ЗАВТРА

Открывая API, банк впускает в систему клиентских данных и платежей посторонних участников. Если говорить о привлечении клиентов и

Всемирная тенденция открывать банковскую информацию совсем скоро коснётся и России. Технологические решения для отечественных банков уже обсуждаются

возврате инвестиций — это не выгодно. Кроме того, клиентов будет волновать безопасность их персональной информации.

«Крупным банкам, особенно на рынках с высокой концентрацией капитала, это не очень выгодно, — считает заместитель гендиректора по ИТ развитию продуктов QIWI Андрей Протопопов. — Роль регулятора здесь, конечно, критична. Без последовательного давления со стороны контролёра вряд ли финтех-компании получат доступ к банковским базам».

Сосем недавно банк QIWI открыл свою платёжную инфраструктуру для использования в финтех-проектах.

Эксперт Крис Скиннер (автор книги «Цифровой банк») однажды высказался: «Если бы PayPal и Facebook не сделали ставку на API, эти компании были бы уже мертвы». Он уверен, что совместный доступ к ресурсам у всех участников финансового сектора обеспечит им прогрессивное развитие.

По словам Ольги Дергуновой, прошло время, когда банки опасались, что финтехи поглотят банковскую индустрию. Теперь все мирно сосуществуют и зачастую вместе работают над интересными бизнес-проектами, между банками и технологическими компаниями идёт непрерывное деловое общение. В среде открытых API на равных условиях смогут конкурировать традиционные финансовые институты и финтех. Возможно, такое глобальное раскрытие информации спровоцирует появление совершенно новых видов финтех-компаний и нео-банков, предлагающих исключительные продукты. Кроме того, получают развитие «нишевые предложения», ориентированные на определённые группы населения. Клиенты получают более быстрый и доступный рынок финансовых услуг с широким ассортиментом.

* * *

Как заметила Татьяна Жаркова: «В цифровой экономике любые границы мешают развитию, будь то границы между отраслями или даже странами. Взаимодействие и создание идей глобальных стандартов, безусловно, может развивать экономику в целом».

**Лев ШУМСКИЙ**

директор
по информационной
безопасности
Ассоциации ФинТех

ЗАЩИТА МАСТЕРЧЕЙНА

О БЕЗОПАСНОСТИ ПЕРВОЙ РОССИЙСКОЙ БЛОКЧЕЙН-ПЛАТФОРМЫ

Мастерчейн — российская блокчейн-платформа, созданная Ассоциацией ФинТех совместно с Банком России и участниками финансового рынка. Платформа реализует технологические стандарты и инфраструктуру распределённых реестров для снижения издержек и повышения прозрачности операций. Как она защищена? Рассказывает директор по информационной безопасности Ассоциации ФинТех Лев Шумский.

— Насколько безопасна платформа Мастерчейн? Чем принципиально отличается её защита от Ethereum?

— Платформа Мастерчейн использует российскую криптографию. Сейчас она проходит сертификацию по требованиям ФСБ к СКЗИ. Заключение по итогам соответствующего процесса Ассоциация ФинТех планирует получить в 2019 году. Высококвалифицированные криптографы под лупой рассматривают все те доработки, которые были сделаны специалистами АФТ к Ethereum.

Помимо криптозащиты в Мастерчейне реализованы механизмы контроля доступа в сеть, которых нет у публичных блокчейн-платформ. Дополнительно к вышеперечисленным уровням защиты встроен слой конфиденциальности.

— Что собой представляют механизмы контроля доступа, зачем они нужны?

— Это так называемый «белый список» (white list), в соответствии с которым предоставляется доступ в сеть блокчейн. Работать в сети могут только те узлы, которые зарегистрированы и подтверждены администратором сети. Для повышения уровня защищённости реализует-

ся процедура KYC (know your customer, «знай своего клиента»): мы знаем, кто подключается к Мастерчейну, будь то юрлицо или конкретный администратор узла.

Процедура KYC идеологически близка к традиционной проверке банком клиента. Подключение узла в рамках бизнес-кейсов возможно только при наличии УКЭП (усиленной квалифицированной электронной подписи). Это дополнительная гарантия безопасности для платформы. Та или иная компания не сможет получить УКЭП, не пройдя полную идентификацию. К тому же администратор сети дополнительно подтверждает права владельца узла. Это эшелонированный подход к идентификации клиентов, подключаемых к платформе.

— Зачем на Мастерчейне используется цифровая подпись?

— Это придаёт юридическое значение транзакции. В соответствии с российским законодательством электронные документы с УКЭП имеют силу бумажных, подписанных собственноручно и заверенных печатью.

— Не возникнет ли сложность при подключении узлов, не станет ли это помехой нормальной работе платформы?

— Нет, для финансовых организаций высокая степень защищённости и эшелонированный подход к идентификации и верификации — привычное дело. Мы не раз обсуждали эти моменты на рабочих группах, которые проходят с участием всех заинтересованных членов АФТ. Доверие внутри сети важнее простоты подключения.

— На базе какой физической инфраструктуры строится Мастерчейн?

— Персональные данные российских граждан и содержащие банковскую тайну сведения должны храниться на серверах, физически расположенных на территории РФ. В будущем АФТ, как возможный оператор сети, планирует развернуть собственную инфраструктуру, так как использование отечественной криптографии накладывает определенные ограничения. Соответственно, к инфраструктуре с отечественными СКЗИ, предъявляются жёсткие требования по обеспечению информационной безопасности.

Подключение узла в рамках бизнес-кейсов возможно только при наличии усиленной квалифицированной электронной подписи. Это дополнительная гарантия безопасности для платформы

— Чем защита платформы Мастерчейн отличается от тех инструментов, которые используются в других национально значимых системах?

— Мастерчейн — это платформа, на которой реализуются банковские сервисы, поэтому ее защита очень близка к системам безопасности распределённых банковских систем. По сути серьёзных различий нет. Российский рынок уже накопил большой опыт в области защиты инфраструктуры, систем и сервисов, и специалисты АФТ успешно его применяют на практике.

— Разбирался ли код Ethereum на наличие уязвимостей?

— Этой части АФТ уделяет большое внимание. Так, наши специалисты постоянно детально разбирают сам код Ethereum, все выпускаемые обновления и доработки, в том числе те, которые делают разработчики АФТ и подрядчики. Это процессный подход, ведь с любыми изменениями в Мастерчейне могут появиться новые уязвимости. Поэтому проверка кода, в соответствии с требованиями Банка России, предъявляемыми к автоматизированным банковским системам, будет производиться постоянно, при выходе любого обновления.

— Возможно ли появление эффекта запаздывания — разрыва между выходом обновлений для Ethereum и их реализацией на Мастерчейне? И насколько критичным будет запаздывание?

— Это достаточно распространённая ситуация для решений, в которых применяется отечественная криптозащита. По мере доработки функционала новые версии будут проходить соответствующую процедуру оценки. То есть, параллельно будут существовать две версии платформы — сертифицированная и не сертифицированная, но это не мешает АФТ реализовывать бизнес-кейсы.

— Насколько смарт-контракты уязвимы с точки зрения информационной безопасности? Вероятно ли появление «заражённых» умных контрактов?

— Смарт-контракт — это скомпилированный код, и важно понимать, что у него внутри. Логические ошибки в этом типе ПО сложно обнаружить. Возможные недостатки программирования мы будем устранять с помощью ручного контроля на этапе анализа кода и автоматически, используя специализированные сканеры безопасности.

Кроме того, планируем создать модуль контроля кода. В итоге все смарт-контракты будут проходить проверку. Не авторизованный АФТ смарт-контракт не сможет быть опубли-

кован в Мастерчейне. Это практически сведёт к нулю вероятность попадания в систему «сырого» и вредоносного умного контракта.

Появление «заражённого» смарт-контакта в системе маловероятно хотя бы потому, что всех участников сети мы хорошо знаем, а кроме того, у владельцев узлов есть собственные службы ИБ, которые тоже контролируют процесс.

— Не отразится ли создание многоуровневой системы проверки и безопасности на цене транзакции? Не повлияет ли высокая степень защищённости на коммерческую привлекательность платформы?

— Опыта реализации российской криптографии в среде блокчейна нет. Пока Мастерчейн — уникальный проект, поэтому сравнить его не с чем. Если говорить о производительности платформы, то мы смогли добиться шести тысяч транзакций в минуту, и продолжаем работать над улучшением этого показателя за счёт оптимизации алгоритмов и исходного кода.

— Насколько велика угроза инсайда, и как с этим бороться?

— Извне проникнуть в настолько хорошо защищённую систему, как Мастерчейн, практически невозможно. Даже DDoS-атака для распределённых сетей не критична.

Основные угрозы могут исходить от злоумышленников, проникших во внутренний периметр организации. Здесь используются классические методы противодействия таким угрозам. То есть, необходимо проверять сотрудников, разграничивать доступ к документам, использовать современные средства защиты информации, осуществлять мониторинг ИБ, и т.п. Российские финансовые организации уже накопили большой опыт в организации противодействия подобным угрозам.

— Кто будет осуществлять техническую поддержку пользователей платформы Мастерчейн?

— За работоспособность платформы отвечают специалисты АФТ. В ассоциации развёрнута служба техподдержки, которая уже начала работать с запросами. Пока обращений не много, и мы отработываем методику взаимодействия АФТ как оператора с владельцами узлов.

— Нужна ли специальная подготовка для специалистов, отвечающих за ИБ блокчейн-платформ и продуктов, построенных на блокчейне?

— Конечно, необходимо понимать, как работает технология распределённых реестров и функционирует Ethereum. С точки зрения информационной безопасности защита блокчейна мало чем отличается от защиты классических сетевых банковских сервисов.

ОТ ЛАБОРАТОРИИ К БИЗНЕС-ПРИЛОЖЕНИЯМ

«КВАНТОВЫЙ СКАЧОК» В МАСШТАБАХ СБЕРБАНКА



Михаил ШАГОВ
главный инженер
Отдела средств
защиты Сбербанка



Алексей ФЁДОРОВ
руководитель
группы, Российский
квантовый центр

Криптография прочно вошла в нашу повседневную жизнь. Мы используем её практически повсеместно: при передаче данных в Интернете, в клиент-банках, при создании электронных подписей на сайте госуслуг, в мобильных приложениях и мессенджерах. Именно на использовании криптографических методов основаны популярные технологии блокчейна и биткоина.

Почему это стало возможным? Распространению криптографии поспособствовала элегантная математическая идея — использование односторонних функций. Их основное свойство состоит в лёгкости вычисления функции по известному аргументу и одновременно сложности вычисления аргумента по известному значению заданной функции. Примером односторонней задачи выступает факторизация: перемножить два простых больших числа легко, тогда как сказать, из каких простых множителей состоит заданное число, вычислительно сложно. Именно на предположении о сложности решения некоторых классов математических задач основывается современная криптографическая защита информации.

КВАНТОВЫЙ КРИПТОАНАЛИЗ

В 1994 году Питер Шор из Массачусетского технологического института (MIT) продемонстрировал, что на квантовом компьютере, который для проведения вычислений использует квантовые частицы, задачи, лежащие в основе современных алгоритмов криптографии с открытым ключом, могут решаться многократно (экспоненциально) быстрее, чем на классическом. В основе работы квантового компьютера лежат феномены квантовой физики, которые не имеют классических аналогов. Например, мы привыкли, что регистр компьютера представляет собой набор бит, каждый из которых принимает значение 0 или 1. Квантовый аналог регистра находится одновременно во всех возможных состояниях, потому что каждый квантовый бит (кубит) в силу принципа суперпозиции является одновременно и 0, и 1. Это позволяет добиваться преимуществ при решении определённого класса задач, к которым относятся криптоанализ алгоритмов с открытым ключом RSA и протокол Диффи-Хеллмана. Кроме того, Лов Гровер предложил алгоритм, пред-

назначенный для поиска по неупорядоченной базе данных. Он позволяет существенно снизить сложность задачи перебора. Это оказывает влияние на стойкость симметричных криптографических алгоритмов, таких как AES и ГОСТ, однако не столь существенную, как в случае алгоритмов RSA и Диффи-Хеллмана. Сегодня квантовый криптоанализ — активно развивающаяся научная дисциплина на стыке квантовой теории информации и классической криптографии. Её цель — использовать существующие методы и разработать новые алгоритмы для криптографического анализа с учётом возможностей «квантового противника».

Если вернуться к истокам математической теории криптографии, то можно задать вопрос: почему системы с открытым ключом стали так популярны? Со времён Шеннона мы используем криптографию, стойкость которой основывается на секретности ключей. Чем больше наша уверенность в том, что ключ неизвестен злоумышленнику и меняется достаточно часто, тем выше надёжность криптографического метода. При этом есть одна система, которая является абсолютно стойкой и не требует никаких предположений — шифр одноразовых блокнотов, или шифр Вернама. В ней кроме того, что ключ является случайным и секретным, необходимо, чтобы его размер был равен размеру сообщения и использовался только один раз. Однако практическое использование этой системы затруднено, поскольку требуется надёжный способ для распределения ключей. Криптография с открытым ключом — практический способ, но, как показывает практика, выбранные алгоритмы не всегда способны гарантировать долгосрочную безопасность. Они уязвимы с точки зрения развития алгоритмов и наращивания вычислительных мощностей злоумышленника. Интересный исторический факт состоит в том, что обоснование абсолютной стойкости одноразового блокнота независимо получил В. А. Котельников. Однако эта работа не получила широкого распространения из-за того, что была опубликована в засекреченном отчёте.

Квантовая угроза, таким образом, бросает новый вызов: как обеспечить защищённое распределение ключей с учётом возможностей квантового компьютера?

КВАНТОВАЯ КРИПТОГРАФИЯ

Вместе с орудием атаки в виде квантового компьютера технологии позволяют нам создать достаточно эффективную систему для распределения криптографических ключей, секретность которых гарантируется законами физики. Квантовые сигналы, в отличие от классических, нельзя скопировать или измерить без того, чтобы не внести возмущение — такое умение злоумышленника противоречило бы законам природы. Поэтому если мы передаём информацию с использованием одиночных квантовых объектов, то получаем систему, которая всегда позволяет обнаружить вмешательство.

На практике для этого используются так называемые протоколы квантового распределения ключа. Первый протокол был предложен больше 30 лет назад Чарльзом Беннетом и Жилем Brassardом. Он основывается на процедуре приготовления поляризационных состояний фотонов или квантов электромагнитного поля. Любая попытка атаки «человек посередине» может быть зарегистрирована именно из-за того, что злоумышленник неизбежно «портит» квантовые состояния при передаче. При этом предполагается, что злоумышленник может совершать любые действия и иметь любые ресурсы, которые не противоречат законам физики, включая квантовые компьютеры.

Технология квантового распределения ключей часто называется квантовой криптографией, хотя решается именно задача распределения ключей. Уже сейчас она активно используется на рынке. Например, компания ID Quantique из Швейцарии предоставляет уже несколько поколений устройства для квантового распределения ключей. В некоторых городах (например, Женеве, Вене, Токио, Пекине, Шанхае) созданы городские сети передачи данных, защищённые путём использования квантового распределения ключей. Линия безопасной передачи информации с помощью квантовых устройств использовалась для обеспечения связи во время федеральных выборов в Швейцарии в 2007 году. Широкую известность получило применение квантовых устройств безопасной передачи информации во время чемпионата мира по футболу в 2010 году. В 2018 году было объявлено, что доля компания ID Quantique переходит корейской телекоммуникационной компании SK Telecom.

Активную работу в направлении квантовой криптографии ведёт компания Toshiba. Её эксперименты демонстрируют рекордные скорости генерации квантовых ключей.

В мировом масштабе лидирует Китай. Построена «квантовая» сеть Пекин-Шанхай протяжённостью 2 000 км, которая включает четыре



локальных городских квантовых сети. К ней подключены 12 китайских банков и компания Alibaba. Они используют систему квантового распределения ключей для обмена регуляторной информацией и защиты пользовательских данных. К 2020 году планируется увеличить протяжённость сети до 11 000 км. Квантовая криптография реализуется как с использованием волоконных линий, так и в открытом пространстве. Например, в режиме Земля — спутник может быть реализовано глобальное распределение криптографических ключей. Китайские учёные уже провели квантово-защищённую видеоконференцсвязь через спутниковое распределение ключей между Пекином и Веней.



Рисунок 1.

Устройства квантового распределения ключей

При внедрении технологий квантового распределения ключей есть несколько принципиальных трудностей. Во-первых, проблема расстояния. Из-за оптических потерь возникает потребность в повторителях, построенных на основе доверенных узлов или полностью квантовых устройств. Типичные расстояния для передачи ключей — 80–100 км в «полевых условиях» и порядка 400 км в лаборатории. Полностью квантовые повторители на данный момент не построены, тогда как использование классических повторителей каждые 100 км достаточно затратно. Тем не менее Китай занимается развитием именно сетей с классическими повторителями.

Вторая проблема — скорость распределения ключей. Характерные скорости составляют 10–100 кбит/с, рекордные — порядка 1 Мбит/с. Их сейчас недостаточно для работы в режиме одно-разовых блокнотов. Поэтому на практике такие системы используются в гибридном режиме: для более частого обновления ключей в уже существующих системах симметричного шифрования, например, AES. В эксперименте ID Quantique ключи менялись примерно раз в минуту.

Из этих двух проблем вытекает третья — экономическая. Такие устройства целесообразно использовать для долгосрочного хранения стратегически важной информации, тогда как для широкого распространения потребуется время. По этому пути идут мировые лидеры, защищающие критически важную инфраструктуру с использованием квантовой криптографии уже сегодня.

КВАНТОВАЯ КРИПТОГРАФИЯ В БИЗНЕС-ПРИЛОЖЕНИЯХ

Несмотря на эти трудности, квантовая криптография может быть внедрена в практическое применение уже сейчас. Квантовое распределение ключа — это источник симметричных ключей. Спектр применения таких ключей достаточно широк. Например, их можно использовать для построения защищённых VPN-туннелей. Такой метод защиты очень популярен

в коммерческих приложениях, поэтому все ведущие производители шифраторов предоставляют устройства — криптошлюзы, использующие симметричные ключи. Совместная работа устройств квантового распределения ключей и устройства для построения VPN-туннелей была продемонстрирована Российским квантовым центром и Сбербанком.

В результате реализована схема по защите обмена информацией между территориально распределёнными площадками — офисами Сбербанка. Для этого задействованы два канала связи:

- ◆ первый канал предназначен исключительно для организации взаимодействия квантовых устройств QKD (quantum key distribution) — разработки Российского квантового центра и компании QRate — для передачи квантовых состояний;

- ◆ по другому каналу связи передаются пользовательские данные, криптографически защищённые VPN-туннелем между двумя программно-аппаратными комплексами.

Принцип работы заключается в следующем: одно из устройств RQC/QRate постоянно вырабатывает ключевой материал и при помощи специального API передаёт эти ключи потребителю. Второе устройство после необходимых проверок на компрометацию и исправление ошибок формирует симметричные криптографические ключи. В свою очередь VPN-построители используют эти ключи для организации криптографического туннеля. Протокол построения такого туннеля основан на использовании «двухкомпонентного» ключа, формируемого на основе собственного долговременного симметричного ключа и «квантового» ключа, полученного от квантового устройства QKD.

Режим работы VPN-туннеля может быть изменён в случае компрометации ключей и в аварийных ситуациях, когда квантовое устройство недоступно для выдачи ключа по какой-либо причине. Тогда VPN-построители задействуют только собственные ключи, а в строгом режиме



Рисунок 2. Устройства квантового распределения ключей

остановят передачу информации до восстановления обмена с устройствами квантового распределения ключей.

По своим техническим характеристикам устройства квантового распределения ключей RQC/QRate находятся на уровне мировых стандартов: скорость приготовления и измерения квантовых состояний достаточно высока. Это позволило даже на достаточно «шумной» линии, когда при потерях порядка 14 дБ использовалась уже существующая линия связи между двумя офисами Сбербанка, удалось распределять криптографические ключи со скоростью 0,1 кбит/с. Такая скорость превосходила требования к VPN-построителям по скорости запроса ключей примерно в 160 раз. При этом уровень ошибок в квантовом канале, $QBER \approx 5\%$, был примерно на 70% выше, чем $QBER \approx 3\%$, заявленный по результатам тестирования лучших зарубежных аналогов на реальных волоконных линиях связи.

Пройдя успешные испытания в «боевых» условиях и продемонстрировав совместимость с существующими технологиями защиты инфор-

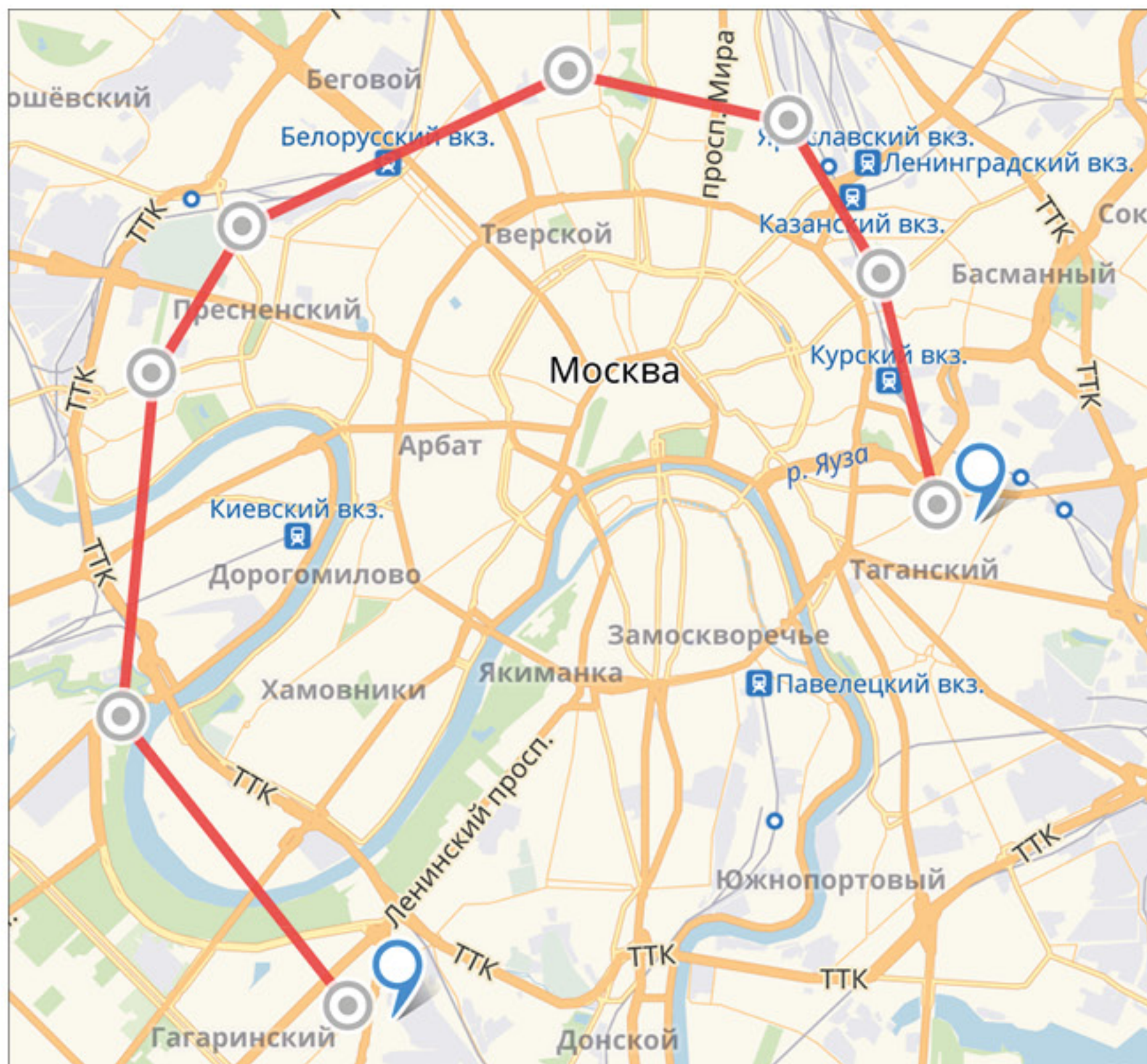


Рисунок 3. Схема оптического канала между офисами Сбербанка

мации, квантовое распределение ключа становится новым перспективным инструментом для защиты информации. С учётом активно развивающейся технологии квантового распределения ключей скорость генерации ключей, а значит, и их объём, значительно вырастут. Это даст возможность применять данную технологию во множестве других криптографических систем и получать максимальный уровень защиты с абсолютной криптографической стойкостью.

Угроза появления в ближайшем будущем квантовых компьютеров, а также возможное появление новых классических алгоритмов, например, как в случае с SHA-1, привлекает всё большее внимание к технологии квантового распределения ключей. В ближайшем будущем можно ожидать демонстрации внедрения квантовой криптографии в новые приложения, например, в технологии блокчейн и распределённых баз данных. Угроза квантовых компьютеров для этих технологий сейчас активно обсуждается сообществом. Однако для этого необходимо переходить от решений в режиме «точка-точка», как в предыдущих экспериментах, к построению многопользовательских сетей квантовых коммуникаций и демонстрации бизнес-приложений.

СТРАТЕГИЧЕСКИЙ ТРЕНД... БЕЗ СТРАТЕГИИ

ПРО ОБЛАКА НА РОССИЙСКОМ РЫНКЕ 2018



Дарья ОРЕШКИНА
эксперт
информационной
безопасности

Для бухгалтерии, отдела продаж, департаментов информационных технологий и разработки ПО провайдеры предлагают всё больше интересных облачных сервисов, повышающих эффективность бизнес-подразделений. Хотя облака по-прежнему вызывают беспокойство службы ИБ ввиду отсутствия полного контроля над инфраструктурой и чувствительными данными, облачные услуги уверенно развиваются и расширяют своё присутствие в повседневной жизни компаний. Весь 2018 год мы наблюдали подъём и оживление российских облачных провайдеров, и повышение спроса среди корпоративных заказчиков.

КЛИЕНТ ГОЛОСУЕТ

В 2018 году в СМИ в интервью экспертов аналитических агентств и поставщиков услуг, озвучивались причины повышения спроса на облачные сервисы. Среди наиболее ярких факторов отметились:

1. Возрастающий интерес бизнеса к DevOps и аналитике Big Data вызвал повышение спроса на IaaS (инфраструктура как услуга) и PaaS (платформа как услуга) (источник: руководитель исследований облачных услуг IDC Дми-

трий Гаврилов в статье на TAdviser¹). Бизнесу это оказалось нужно, например, при создании умных онлайн-сервисов для взаимодействия с клиентами компании, для реализации систем помощи принятия решений в сфере управления, продаж, маркетинга и др.

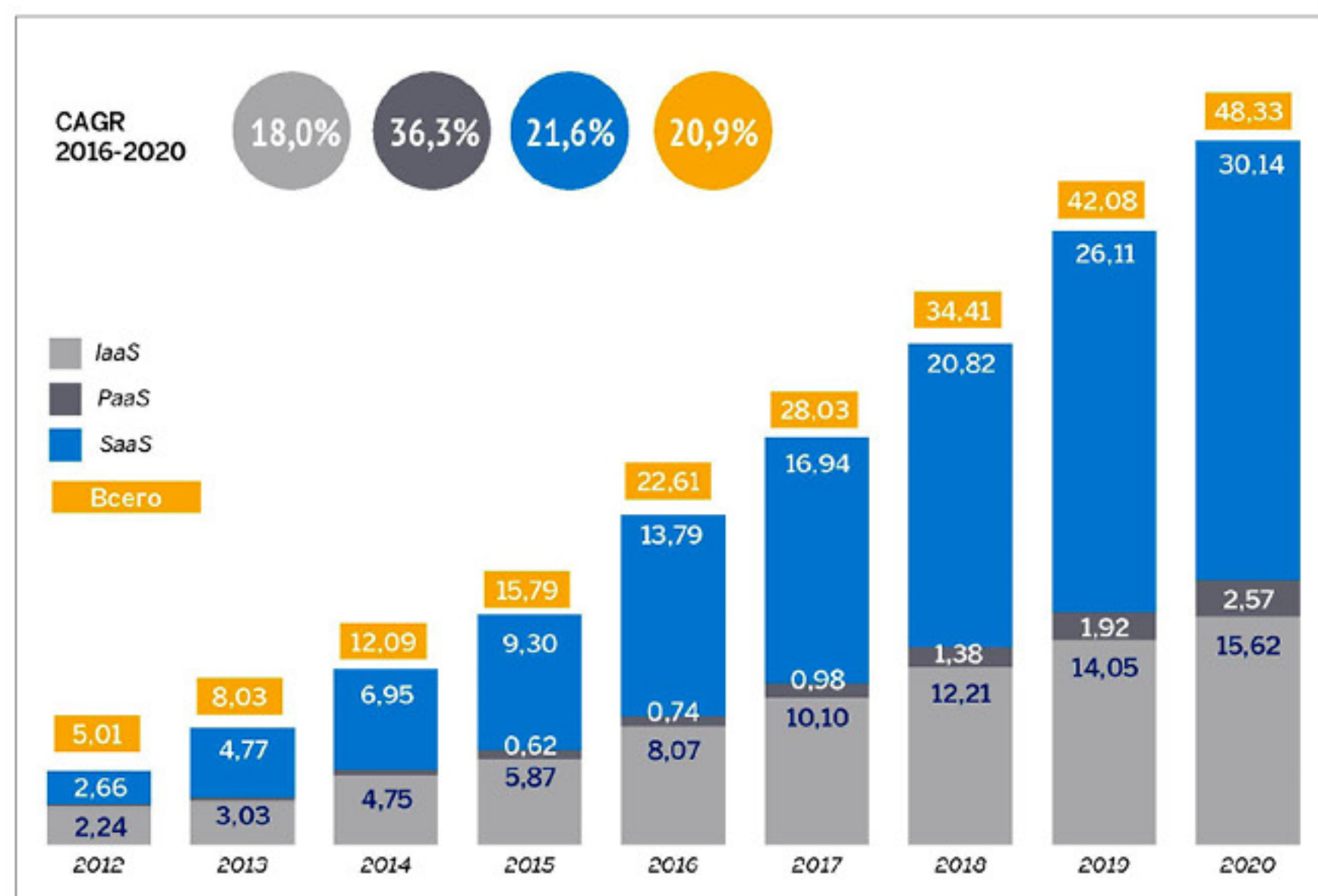
2. Массовые блокировки западных сервисов, включая Amazon дали ощутимый толчок, когда по словам облачных провайдеров, пострадавшие начали переход к мультиоблачной модели с локальными поставщиками облачных услуг в качестве резерва.

3. Локальные провайдеры смогли предложить более низкие цены на свои услуги, удобство использования и настройки решений. Последнее утверждение показалось мне спорным, и я решила провести собственный эксперимент. За один вечер в конфигураторе сервиса одного из известных российских поставщиков выбрала все необходимые опции, оформила подписку на IaaS, в тот же вечер получила сконфигурированную услугу и приступила к запуску нового проекта. Цена подписки при этом была ниже западных аналогов.

Как говорится, клиенты голосуют рублём. Отмечается, что средний чек клиентов также вырос.

ОБЛАКА ПЛЫВУТ, НЕ ТОРОПЯТСЯ

Один из критичных аспектов развития гибридных и публичных облаков — это обеспечение безопасности данных, которые хранятся у поставщика услуг. Надёжность функционирования и защищённость облачной среды — ключевые факторы для формирования доверия корпоративных заказчиков. Защита облачного сервиса начинается с построения модели угроз, далее определяется набор требований и мер безопасности. Для IaaS, PaaS, SaaS (программное обеспечение как сервис) границы ответственности провайдера и подписчика услуги различаются, при этом в SaaS получается наибольшее количество элементов, за которые отвечает провайдер. В любом случае, какую бы модель сервиса ни выбрал бизнес, необходима качественная реализация мер безопасности как со стороны провайдера, так и со стороны подписчика. Именно совместные усилия дают требуемый уровень защищённости всей системы.



«Прогноз объёма рынка облачных услуг в России в 2015–2020 гг., млрд руб.». Источник: SAP СНГ, февраль 2017 г.

¹ [www.tadviser.ru/index.php/Статья:Облачные сервисы \(рынок России\)](http://www.tadviser.ru/index.php/Статья:Облачные_сервисы_(рынок_России))

Наиболее развитые и пригодные для коммерческого использования облачные сервисы предоставляют своим клиентам широкий набор инструментов контроля и защиты корпоративных аккаунтов, например, средства централизованного управления учётными записями, выбор методов аутентификации, применяются системы выявления аномальной и вредоносной активности.

Для корпоративного сегмента — как для коммерческих компаний, так и для госструктур, важно не только наличие механизмов защиты данных, размещаемых в облаке, но соответствие их отраслевым стандартам, законодательству, внутрикорпоративным требованиям. В 2018 году российские провайдеры предлагали своим клиентам облака, сертифицированные по различным стандартам, в частности сертифицированный в соответствии с требованиями PCI DSS виртуальный дата-центр, облачные услуги для хранения персональных данных в соответствии с Федеральным Законом № 152. Таким образом, компании вольны выбирать, оставлять ли всю инфраструктуру в собственных ЦОДах или воспользоваться облачными услугами.

Примечательно, что и в России, и во всём мире банки активно применяют современные информационные технологии, но при этом неторопливо «принимают» облака и мигрируют в облачную среду. Банки видят плюсы построения ИТ-систем на облачных платформах, у них есть задачи, которые эффективнее было бы с помощью облаков решать, но в большинстве случаев отсутствует облачная стратегия, которая обеспечит переход к облаку. Облачная стратегия нужна, безусловно не только банкам, но всем другим компаниям, вовлечённым в цифровизацию и имеющим в стратегии развития планы по модернизации своей ИТ среды. В западных компаниях всё чаще встречается должность «менеджер по цифровой трансформации». Передовые компании видят необходимость выделения такой роли, даже если не определена отдельная должность. Ну а если безобразие нельзя остановить, то его надо возглавить. Почему бы CISO не взять на себя роль менеджера по цифровой трансформации, хотя бы в части обеспечения безопасности этого процесса? Ведь действительно важно, чтобы бизнес и безопасность шли нога-в-ногу, чтобы прогресс был эффективным и бизнес оставался защищённым.

КАКИЕ СРЕДСТВА ЗАЩИТЫ?

С точки зрения подписчика, при любой модели облачного сервиса неизменно остаются задачи контроля своих данных и действий своих администраторов и пользователей. Различаются лишь уровни, на которых может быть направлено вредоносное воздействие. В 2018 году множество

инцидентов, связанных с применением облачных решений, были вызваны нелегитимным использованием учётных записей, некорректными правами доступа к опубликованным ресурсам, отсутствием шифрации баз информации, к которым был получен несанкционированный доступ.

При использовании облаков, подписчику всегда нужно понимать, кто и какие данные опубликовал в облаке, кто имел к ним доступ, необходимо иметь возможность применять корпоративные политики к чувствительным данным. С этой задачей научились справляться решения класса Cloud Access Security Broker (CASB). Аналитическое агентство Gartner в октябре 2018 признало лидерами производителей: McAfee (поглотили Skyhigh Networks), Netskope (в 2018 году добавил базовую функциональность SWG в свой облачный продукт), Symantec (поглотил Blue Coat, в состав которого прежде вошли Elastica и Perspecsys), Bitglass.

Для контроля администраторов и пользователей, что особенно актуально при углублении в PaaS и IaaS, недостаточно просто назначить права доступа, требуется детальное понимание, кто какие команды вводил при настройке приложений и СУБД, появляется необходимость аккуратно управлять паролями растущих в геометрической прогрессии сущностей, автоматизировать гранулярный доступ для разных специалистов, в каких-то случаях требуется не только журналировать запросы, но и записывать экраны при подключении к системе. Эти задачи решают системы класса Privileged Identity & Access Management. Gartner в декабре 2018 лидерами производителей решений класса Privileged Access Management признал CyberArk, BeyondTrust, Centrify и CA Technologies. Примечательно, что компания Bomgar в сентябре 2018 объявила о приобретении компании BeyondTrust для расши-



Magic Quadrant for Cloud Access Security Brokers. Источник: Gartner (October 2018)

Magic Quadrant for
Privileged Access
Management.
Источник: Gartner
(December 2018)



рения возможностей решения для управления привилегированным доступом и о продолжении своей деятельности под именем BeyondTrust.

СОБЛАЗН ВЕЛИК, ПОРА ЗАДУМАТЬСЯ...

Переход из корпоративной сети в облако должен быть тщательно продуман и спланирован, потому что на карту поставлены доверие клиентов к компании, качество и гибкость услуг, фундамент для дальнейшего развития. Важно, чтобы компании и лица, принимающие решения в области ИТ, оценили свою готовность к переходу в облако. Вот список вопросов, которые необходимо задать для принятия верного решения:

1. Каковы причины для перехода в облако и какие выгоды ожидаются от миграции?

Нужно определить основные стратегические цели облачной инициативы. Таким образом, ответ должен прийти коллективно от всех ключевых заинтересованных сторон — операционного управления, ИТ, финансов, продаж, маркетинга, отдела кадров и других.

2. Выразите в цифрах и конкретных значениях ожидаемый результат, как для клиентов, так и для компании после завершения перехода в облако.

Ответы должны помочь определить параметры облачной инициативы — оцифрованные ожидания каждого участника.

3. Каковы выводы бизнес-обоснования потенциального перехода в облако, какие бизнес-процессы следует перенести в облако и почему?

Тщательная оценка потребностей необходима, прежде чем мобилизовать крупную инициативу.

4. Достаточно ли в компании человеческих ресурсов, специалистов и времени для реализации инноваций?

Нужна оценка готовности сотрудников компании к реализации инноваций.

5. Согласуются ли ресурсы корпоративной сети с новыми инициативами?

Как и предыдущие, вопрос также направлен на оценку стратегической согласованности. Перемещение в облако означает уменьшение присутствия локальной ИТ-среды, но требует дополнительной пропускной способности сети.

6. Как вы узнаете, что у вас достаточно пропускной способности для поддержки новых и/или существующих приложений?

Здесь оценивается, может ли ёмкость вашей сети идти в ногу с вашими устремлениями.

7. Каковы самые сильные и слабые стороны корпоративной сети на данный момент в части работы с клиентами и в части работы офисов?

Подумайте, как и где использовать свои сильные стороны и укрепить слабые. Что произойдёт, если сеть выйдет из строя, когда центр обработки находится в облаке.

8. Как изменятся подходы и потребности в безопасности при переходе в облако? Какие виды мер безопасности могут потребоваться, чтобы защитить пользователей, данные и ИТ активы?

Безопасность — стратегически важная облачная цифровая услуга, наравне с переносом сетевой инфраструктуры и приложений в облако. Ландшафт угроз поменяется, появятся новые киберуязвимости, в том числе DDoS-атаки, вторжения вымогателей и кража вычислительных ресурсов (в 2018 году облачные системы подвергались нападениям с целью майнинга криптовалют), несанкционированный доступ к данным и другие формы взлома.

9. Как будет выглядеть дальнейший план развития ИТ в компании?

Что даст переход в облако в дальнейшем.

10. Каково видение того, как будет развиваться процесс перехода в облако?

Это будет массовая миграция или поэтапный подход? Какой срок? Как будут разделены обязанности по управлению процессом?

Чтобы инициатива была успешна, убедитесь, что у правильных людей есть место за столом переговоров с самого начала. Переход в облако, начиная от планирования и заканчивая реализацией инициативы — непростая задача и для отдела ИТ и для команды информационной безопасности. Взвешенный подход, тщательно проработанные потребности и возможности, слаженная работа всей команды приведут к верному решению и дадут бизнесу надёжный фундамент для прогресса.

АНТИФРОД-СИСТЕМЫ: БЫСТРО И ДЁШЕВО

РЕКЛАМА ВЕНДОРА С КОММЕНТАРИЯМИ
БАНКА-ПОТРЕБИТЕЛЯ

В историю 2018-й войдёт, как год смены мотивации при внедрении антифрод-систем при оказании услуг ДБО. С вступлением в силу Федерального закона № 167-ФЗ, вдруг обнаружилось, что ЦБ исходит из постулата, что такие системы уже имеются в кредитных организациях. Опыт компании Фродекс показывает, что это не так. С момента появления компании на рынке в 2011 году ситуация, безусловно, изменилась, но тем не менее и сегодня процесс противодействия мошенничеству подкреплён соответствующей аналитической системой далеко не в каждом банке.

Почему? Прежде всего, ограниченное предложение на рынке. Раньше спрос по факту создавали только крупные кредитные организации. В силу неограниченности бюджетов они обращались к зарубежным тяжеловесным системам, обеспечивающим широкий функционал. Но такая ситуация была скорее исключением. В целом по банковской отрасли внедрялись либо только узкоспециализированные решения, ориентированные на конкретные системы ДБО, как правило, создаваемые теми же разработчиками, либо ничего не внедрялось, либо создавалось, что называется, «на коленке», собственное решение.

Однако, нынешнее законодательство не признаёт разницы ни в каналах обслуживания, ни в типе клиентов. Анализировать надо везде, всюду и все платежи клиентов.

Кредитные организации столкнулись с задачей в срочном порядке выстроить свои процессы противодействия мошенничеству. Устоявшаяся практика по созданию систем автоматизации бизнес-процессов тут не подходит, т.к. предполагает длинный многосложный цикл: анализ требований, изучение имеющихся на рынке продуктов, проектирование решения, выполнение интеграционных работ, тестирование, доработки и, наконец, запуск в промышленную эксплуатацию. В некоторых случаях такой процесс может занять до нескольких месяцев и даже лет.

В сложившейся ситуации компании Фродекс есть чем ответить на вызовы времени. Большой опыт разработки и поставки систем анализа

банковских данных и защиты информации (более 40 успешных внедрений в банках РФ) с успехом доказывает, что внедрение антифрод-системы — это быстро, просто и недорого.

Флагманским решением «Фродекс» является антифрод-система FraudWall. Базовые принципы, изначально заложенные при построении системы, такие как многоканальность анализа и независимость от источников данных (отсутствие привязки к конкретным автоматизированным системам), поставка логики обнаружения вместе с продуктом, обеспечивают любой кредитной организации возможность успешно решить поставленные задачи.

Рассмотрим, с чем сталкивается банк при внедрении антифрод-системы.

ВРЕМЯ ДОРОГО

В первую очередь, фактор успешного внедрения — это время, затрачиваемое на подготовительные работы, развёртывание системы, интеграцию с источниками данных. Вне зависимости от банка длительный процесс внедрения антифрод-решения может привести к фактическому сворачиванию проекта.

Исходя из опыта, разворачивание сервера с антифрод-системой FraudWall занимает не более одного дня. Все интеграционные работы, необходимые для подключения системы к источникам данных, не требуют больших временных и денежных затрат. Интеграция может быть выполнена не только разработчиками, но даже силами самого банка. Как правило, эта процедура занимает не более недели.

Следует отметить, что для большого числа источников (системы ДБО, АБС) есть готовые шаблоны для коннекторов, позволяющие подключить систему практически «из коробки».

Нынешнее законодательство не признаёт разницы ни в каналах обслуживания, ни в типе клиентов. Анализировать надо везде, всюду и все платежи клиентов



Александр ВИЛЬДМАН
советник
председателя
правления
АО «МТИ Банк»



Руслан ФАХРЕТДИНОВ
ведущий аналитик
Информационной
безопасности
ООО «Фродекс»

При расширении лицензии, например, подключения антифрода для физлиц дополнительно к антифроду для юрлиц, необходимо только добавить/изменить коннектор к источнику данных и выполнить настройки в интерфейсе.

Комментарий АО «МТИ Банк»

Как банк, активно использующий решения Фродекс, можем отметить, что внедрение действительно не составило труда. В подходах этой команды есть подкупающие вещи — предоставление софта на тестирование, дружелюбная и оперативная техническая поддержка, готовность к сотрудничеству и умение прислушиваться к пожеланиям заказчика, учитывать его опыт. Предложения по добавлению функционала принимаются к обсуждению и действительно внедряются. Эксплуатация системы не требует много ресурсов. Это из области «поставили и забыли»: правила настраиваются легко, дропы добавляются просто.

БЮДЖЕТ ВАЖЕН

Другой аспект: внедрение антифрод-системы может «влететь в копеечку».

Часто в качестве решения в проекте рассматриваются продукты компаний, по сути предлагающих рынку аналитическую платформу за немалые деньги. Но даже в случае приобретения такой платформы для создания функционирующей антифрод-системы потребуются проведение длительных и дорогостоящих работ по реализации логики обнаружения, написания коннекторов, а иногда и дополнительного обучения персонала по работе с системой. В бюджет проекта также нужно будет добавить расходы на серверное оборудование, лицензии на программное обеспечение (ОС, СУБД) и др.

В результате практически под каждый отдельно взятый банк необходимо создание собственного решения или, по крайней мере, выполнение множества работ по подготовке продукта, которое сильно отражается на бюджете проекта.

FraudWall, в отличие от таких решений, не требует дополнительной доработки самой системы. В данном случае банк помимо инструмента для борьбы с мошенническими платежами получает и регулярно обновляемые с учётом текущих реалий мошенничества встроенные

правила обнаружения. Это помогает банкам, эксплуатирующим систему, выстроить высокоэффективный механизм предотвращения мошенничества.

Для добавления собственных правил проверки (к поставляемой и обновляемой логике обнаружения) банк может использовать конструктор правил, встроенный в систему.

Если кредитная организация хочет контролировать специфические схемы мошенничества, мы всегда стараемся идти навстречу и готовы, по мере возможности, реализовать дополнительную логику в рамках техподдержки, т.е. без дополнительной оплаты. В отдельных случаях возможна оплачиваемая доработка.

Мы также предусмотрели, что банк может использовать несколько систем источников данных (несколько ДБО, АБС). Лицензия не привязана к числу анализируемых источников данных, и банк может обходиться без дополнительных затрат. Это актуально в случае перехода с одной системы дистанционного банковского обслуживания на другую или в случае, когда исторически в банке используется несколько систем.

Что касается необходимости докупки дополнительного ПО, система FraudWall изначально разработана с учётом возможности развёртывания совместно с программным обеспечением с открытым исходным кодом, что позволяет избежать дополнительных затрат на ОС, СУБД и т.д.

Комментарии АО «МТИ Банк»

Если рассматривать бюджет, то затраты действительно далеко не заоблачные. Часто поставщики решений умалчивают о стоимости владения, а она может оказаться весьма значительной. У Фродекса всё понятно — открытое ПО. Очень простая схема: лицензирование по количеству клиентов, вне зависимости, какие системы ДБО используются — у нас, например, настроены клиент-банки для физических и юридических лиц. Кроме того, проверяем и поступившие на бумаге документы — тут уже, конечно, не в целях антифрода как такового. Система позволяет использовать функционал и в целях ПОД/ФТ. Регулятор достаточно часто выпускает новые вводные, и Фродекс позволяет оперативно реагировать на них, даже в качестве временного решения за счёт возможности гибко настроить систему под конкретную задачу.

УДОБСТВО В РАБОТЕ И АВТОНОМНОСТЬ

Многие системы требуют постоянного мониторинга за логикой обнаружения и часто модернизации и/или создания новых правил провер-

Для добавления собственных правил проверки (к поставляемой и обновляемой логике обнаружения) банк может использовать конструктор правил, встроенный в систему

ки силами самого банка. Связано это с тем, что злоумышленники не стоят на месте и постоянно используют новые схемы.

Наш подход отличается от такой концепции модернизации логики. В системе предусмотрена встроенная и обновляемая разработчиком логика обнаружения.

Обезличенная информация по выявленным инцидентам, которой делятся с нами клиенты, позволяет совершенствовать и своевременно актуализировать встроенную логику, доступную в качестве обновления для всех банков, эксплуатирующих антифрод-систему.

Помимо регулярных обновлений, мы несколько раз существенно изменяли логику работы встроенных правил, что помогает более эффективно обнаруживать новые схемы поведения злоумышленников. Среди причин подобных изменений можно выделить следующие:

- ♦ переход с создания платежей с устройства злоумышленника на практически повсеместное использование средств удалённого управления;
- ♦ длительная подготовка к мошенничеству с изучением характера и истории работы жертвы;
- ♦ рост популярности методов социальной инженерии среди злоумышленников;
- ♦ резкое снижение характерных сумм мошеннических платежей до минимальных размеров и т.д.

Это означает, что вместо того, чтобы в одиночку бороться с новой схемой кражи средств, банк может рассчитывать на обновление логики обнаружения, основанной на нашем опыте и опыте других банков-клиентов, которые заинтересованы в своевременном выявлении новых схем.

При этом затраты, требуемые на сопровождение и администрирование системы, минимальны.

Фактически в большинстве банков, эксплуатирующих систему, её администрированием занимается всего один человек, который тратит на текущие задачи порядка 30 минут в неделю. И то, в основном, для переноса архивных логов и снятия снапшот-образов системы.

Комментарий АО «МТИ Банк»

Разработчики Фродекс действительно следят за изменениями поведенческих моделей злоумышленников, консультируются с ИБ-сообществом и учитывают рекомендации ФинЦЕРТ Банка России. Мы это можем подтвердить со всей ответственностью: наш FraudWall с начала использования прошёл уже ряд серьёзных обновлений. И что порадовало — ни в одном обновлении не было ошибок. Те, кто регулярно ставят обновления АБС, знают, что это дорогого стоит. Наш Банк пока

Обезличенная информация по выявленным инцидентам, которой делятся с нами клиенты, позволяет совершенствовать и своевременно актуализировать встроенную логику

использует АБС ЮниСАБ, и мы понимаем существование гипотетической вероятности, что из-за ошибок в обновлении, в «некоторых» случаях возможны отключения каких-либо автоматизированных функций. Конечно, остаётся возможность совершить необходимые действия вручную, особенно когда знаешь об отключении автоматической функции. Во избежание таких проблем Банк решил использовать другой, связанный с FraudWall, продукт Фродекс — FraudWall AML, и мы ни разу не пожалели об этом. Система получилась не требовательной к ресурсам, легко масштабируемой и с отличным быстродействием.

НАЦЕЛЕННОСТЬ НА РЕЗУЛЬТАТ

Постоянно меняющееся поведение злоумышленников и смещение их прицела на весь банковский сектор только подтверждает необходимость выстроенного процесса борьбы с мошенничеством в банке любого уровня. Перед банками всегда стоят задачи обеспечения сохранности денежных средств на банковских счётах и выполнения требований регулятора в части антифрода.

Эти задачи и помогает решить антифрод-система FraudWall. Система, помимо выполнения требований, касающихся выявления и блокирования банком мошеннических операций, позволяет более комплексно подойти к учёту различных схем действий злоумышленников и выявить мошеннические платежи даже в тех случаях, когда операция клиента, на первый взгляд, не вызывает сомнений.

Комментарии АО «МТИ Банк»

В заключение хотелось бы отметить, что мы действительно довольны сотрудничеством с компанией Фродекс. В Банке используется не только антифрод-система FraudWall, но и система противодействия отмыванию (легализации) доходов и финансированию терроризма FraudWall AML. Специалисты Банка очень плодотворно сотрудничают с разработчиками по оптимизации системы и расширению её функционала. Надо отметить, что изменения вносятся очень оперативно и позволяют значительно ускорить процесс автоматизации исполнения рекомендаций и требований регулятора.

ТЕХНОЛОГИЯ ЗАЩИТЫ ОТ УГРОЗЫ ПОДМЕНЫ БИОМЕТРИЧЕСКОГО СКАНЕРА

ЧАСТЬ 1. РИСКИ БИОМЕТРИЧЕСКОГО ПРОЦЕССА



Максим ФЕДОТЕНКО
руководитель
направления
Центра внутри-
корпоративного
взаимодействия
Сбербанка

В ближайшую пару лет Россию ждёт технологический прорыв: применение биометрии станет по-настоящему массовым. Российские банки уже сейчас начали предлагать клиентам использование государственной Единой биометрической системы, которая позволит получать множество услуг онлайн. Единожды зарегистрировав свой биометрический образец, можно проходить удалённую идентификацию в различных банках без личного присутствия. Сбербанк не только участвует в общенациональной биометрической системе, но и строит собственную платформу, которая охватит отделения и устройства самообслуживания банка, а также системы дистанционного банковского обслуживания (ДБО).

Мы осознаём, что использование современных биометрических технологий — это не только удобство и скорость, но и определённые риски, связанные с угрозой мошенничества. Поэтому перед внедрением нового процесса мы

разрабатываем меры для минимизации рисков. На каких принципах основана наша модель угроз биометрии, и какие риски мы оцениваем?

МОДЕЛЬ УГРОЗ БИОМЕТРИЧЕСКОЙ СИСТЕМЫ

В качестве основы мы взяли модель, приведённую в рекомендации Международного союза электросвязи (МСЭ) ITU-T X.1086 «Telebiometrics protection procedures — Part 1: A guideline to technical and managerial countermeasures for biometric data security», и документ Международной организации по стандартизации ISO/IEC 30107 «Biometric presentation attack detection». Для начала рассмотрим функциональную биометрическую модель (Рис.1).

В соответствии с ней биометрический сканер сначала собирает характеристики человека: например, отпечатки пальцев. Затем он преобразует их в биометрический образец (растровый рисунок) и отправляет в модуль обработки. Из биометрического образца выделяются определённые

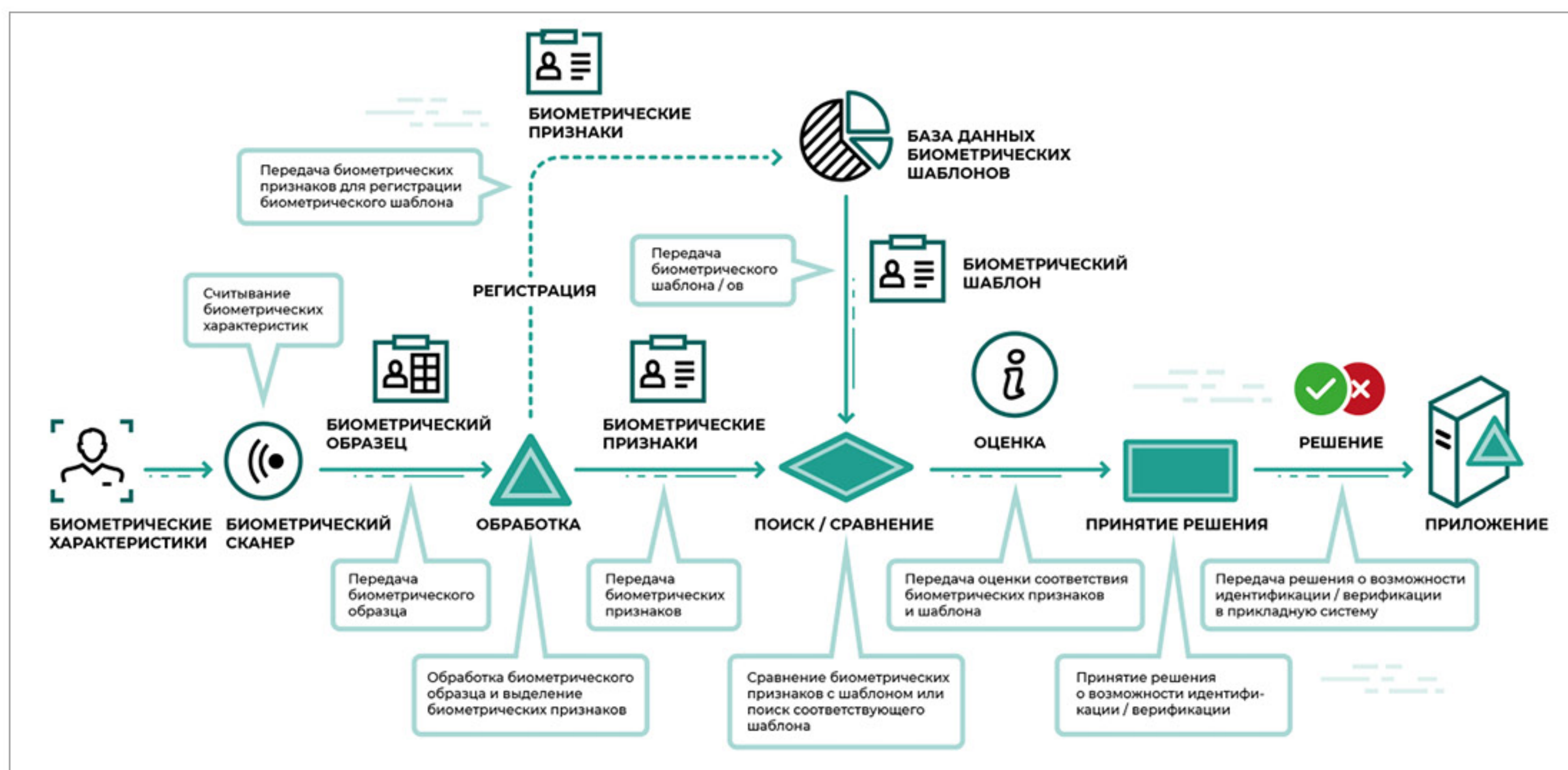
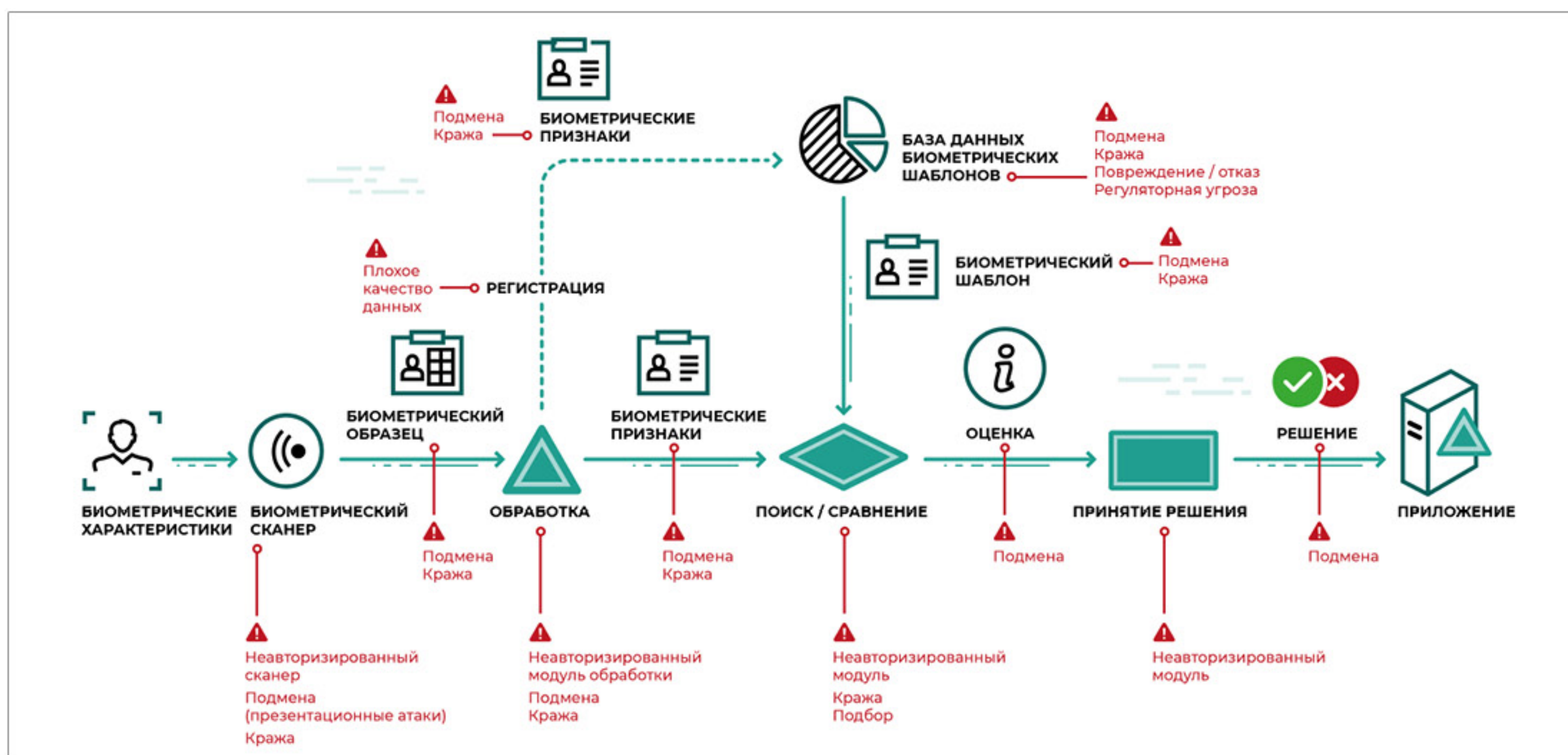


Рисунок 1. Функциональная биометрическая модель



ные признаки. Если человек только регистрирует свою биометрию, биометрические признаки записываются в базу данных (далее они называются биометрическим шаблоном). В дальнейшем признаки направляются на сравнение с биометрическим шаблоном (в случае верификации) или для поиска наиболее подходящего шаблона (в случае идентификации). При этом модуль поиска и сравнения выдаёт оценку соответствия (скор-балл), на основании которой модуль принятия решения информирует систему об успешной или неудачной попытке идентификации/верификации.

Практически при каждом действии функциональной биометрической модели возникают угрозы безопасности (Рис. 2).

Рассмотрим эти угрозы по порядку. Место снятия биометрических характеристик — одно из самых проблемных во всей биометрической технологии. Здесь возникает большое количество возможностей для атак, и методы защиты не всегда за ними успевают. Эти угрозы можно разделить на три основных класса:

♦ **Неавторизованный сканер.** Биометрический сканер может быть подменён или просто отсутствовать. Действительно, зачем злоумышленнику сканер, если можно просто отправить фотографию жертвы в модуль обработки? Другим примером подобной атаки может стать отключение функции liveness detection сканера. В этом случае любое изображение на экране смартфона или силиконовый отпечаток пальца могут сойти за действительные биометрические характеристики.

♦ **Кража.** Биометрический образец, создаваемый сканером, может быть украден и использован в дальнейшем для подмены.

♦ **Атаки подмены или презентационные атаки.** Описанию этого класса атак и его типов посвящён стандарт ISO/IEC 30107-1. Если коротко, то их можно разделить на синтетические и естественные. К синтетическим атакам можно отнести, например, видеоизображения человека, искусственный отпечаток пальца из желатина или просто очки от солнца. Естественные атаки — это, например, отрезанный палец, принуждение, методы социальной инженерии и т.п.

Теперь рассмотрим угрозы модуля обработки биометрического образца. На входе в него подаётся образец (например, фотография), а на выходе он генерирует математическую модель, называемую биометрическими признаками. Именно эта модель и хранится в базе данных под названием биометрического шаблона. Здесь так же, как и в биометрическом сканере, характерны угрозы неавторизованного модуля, который, например, вне зависимости от предъявляемого образца будет выдавать всегда одни и те же биометрические признаки, а также угрозы подмены и кражи этих признаков.

В случае первичной регистрации биометрического шаблона нужно отметить такой риск, как плохое качество биометрических данных. В этом случае в дальнейшем при идентификации или верификации пользователя заметно увеличиваются ошибки как первого (отказать своему), так и второго рода (принять чужого за своего).

Собранные биометрические шаблоны, а зачастую и биометрические образцы пользователей, хранятся в базе данных, которая также является

Рисунок 2. Угрозы в функциональной биометрической модели

одним из самых проблемных мест с точки зрения рисков безопасности. Здесь можно выделить следующие угрозы:

- ◆ Подмена биометрических шаблонов, кража биометрических образцов и шаблонов.
- ◆ Повреждение или полный отказ базы данных, что может привести к невозможности идентификации/верификации пользователей, а также утере всех или части биометрических шаблонов.
- ◆ Регуляторная угроза. Необходимо не забывать о законодательстве: например, хранение биометрического шаблона без письменного согласия клиента на обработку его биометрических персональных данных (ПДн), после окончания срока действия или отзыва пользователем согласия может привести к административной ответственности (штрафам).

Как уже было сказано, биометрические шаблоны, хранящиеся в базе данных, используются для идентификации или верификации пользователя. Эту функциональность реализует модуль поиска и сравнения. Он выдаёт оценку доверия (скор-балл), говорящую о точности биометрической процедуры. Здесь возможна та же угроза подмены модуля, в том числе изменения его настроек для неправильного вычисления скор-балла, а также кражи передаваемых в модуль биометрических признаков и шаблонов.

Отдельным пунктом нужно отметить новый тип угрозы — подбор биометрических признаков. Он может осуществляться как на основе имеющихся данных (например, базы данных фотографий), так и синтетическими методами: с помощью так называемой атаки Hill-Climbing. Этот термин был введён в статье C. Soutar, R. Gil-

roy, and A. Stoianov. Biometric system performance and security. In Proc. IEEE Automatic Identification Advanced technologies (AIAT), 1999.

Алгоритм такой атаки для процедуры верификации описан, например, для отпечатка пальца в статье Umut Uludag, Anil K. Jain «Attacks on Biometric Systems: A Case Study in Fingerprints» (Рис. 3).

Результат биометрической идентификации/верификации может быть подменён на уровне модуля принятия решения. В данном случае актуальна угроза подмены самого модуля на неавторизованный или изменение его настроек, например, пороговых значений (threshold) для «смягчения» решения.

Также необходимо отметить, что везде, где биометрические образцы, признаки или шаблоны передаются из модуля в модуль, возможна реализация угроз, связанных с подменой биометрических данных или их перехватом.

МОДЕЛИ БИОМЕТРИЧЕСКОГО ПРОЦЕССА

В рекомендациях ITU-T X.1084 выделяется четыре модели биометрического процесса (Таблица 1), которые классифицируются на основе следующих признаков:

- ◆ места хранения биометрических шаблонов (базы данных);
- ◆ места расположения модуля сравнения биометрических признаков и биометрических шаблонов.

Суть этих моделей легко показать графически (Рис. 4).

При использовании локальной модели сбор биометрических характеристик, их обработка и

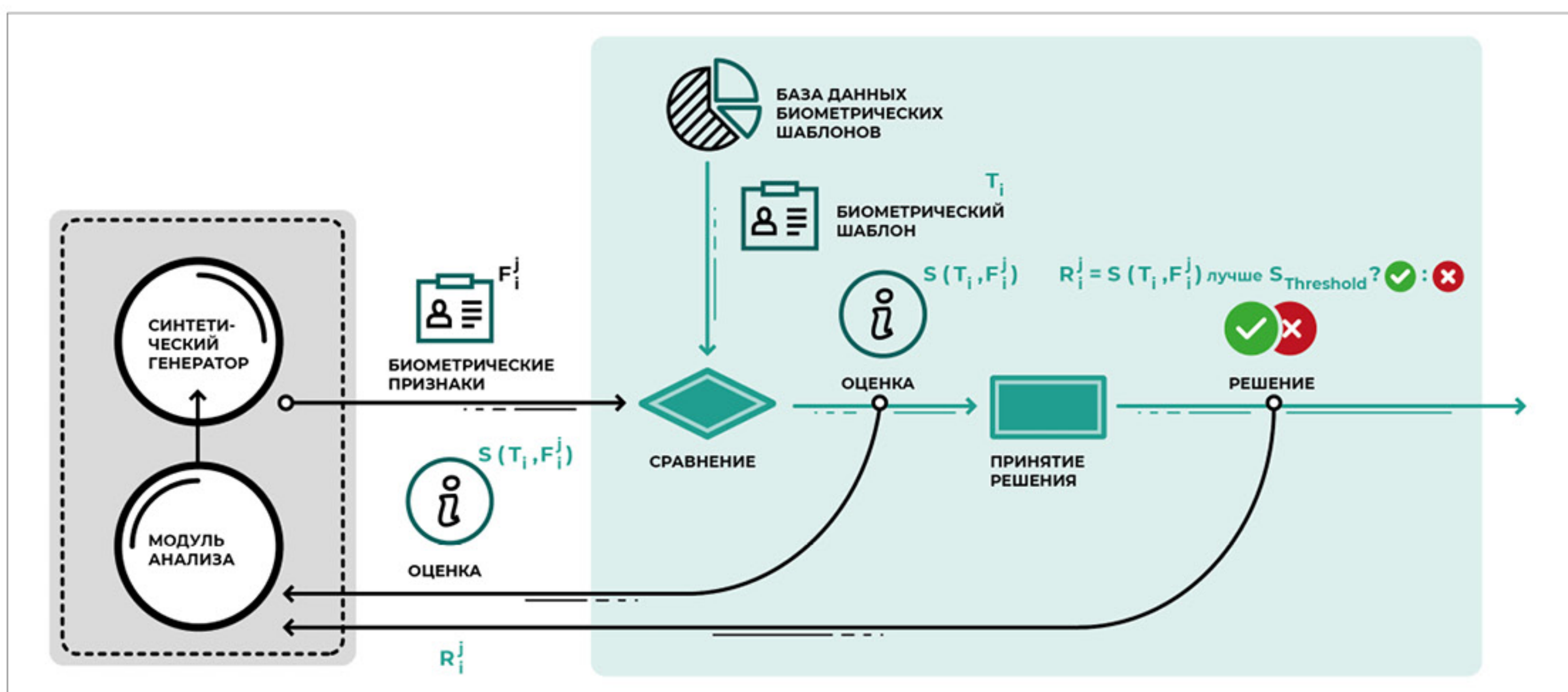


Рисунок 3. Схема атаки Hill-Climbing

Сравнение	Хранение	
	Клиент	Сервер
Клиент	Локальная	С загрузкой шаблона
Сервер	С присоединением данных	Централизованная

Таблица 1. Модели биометрического процесса

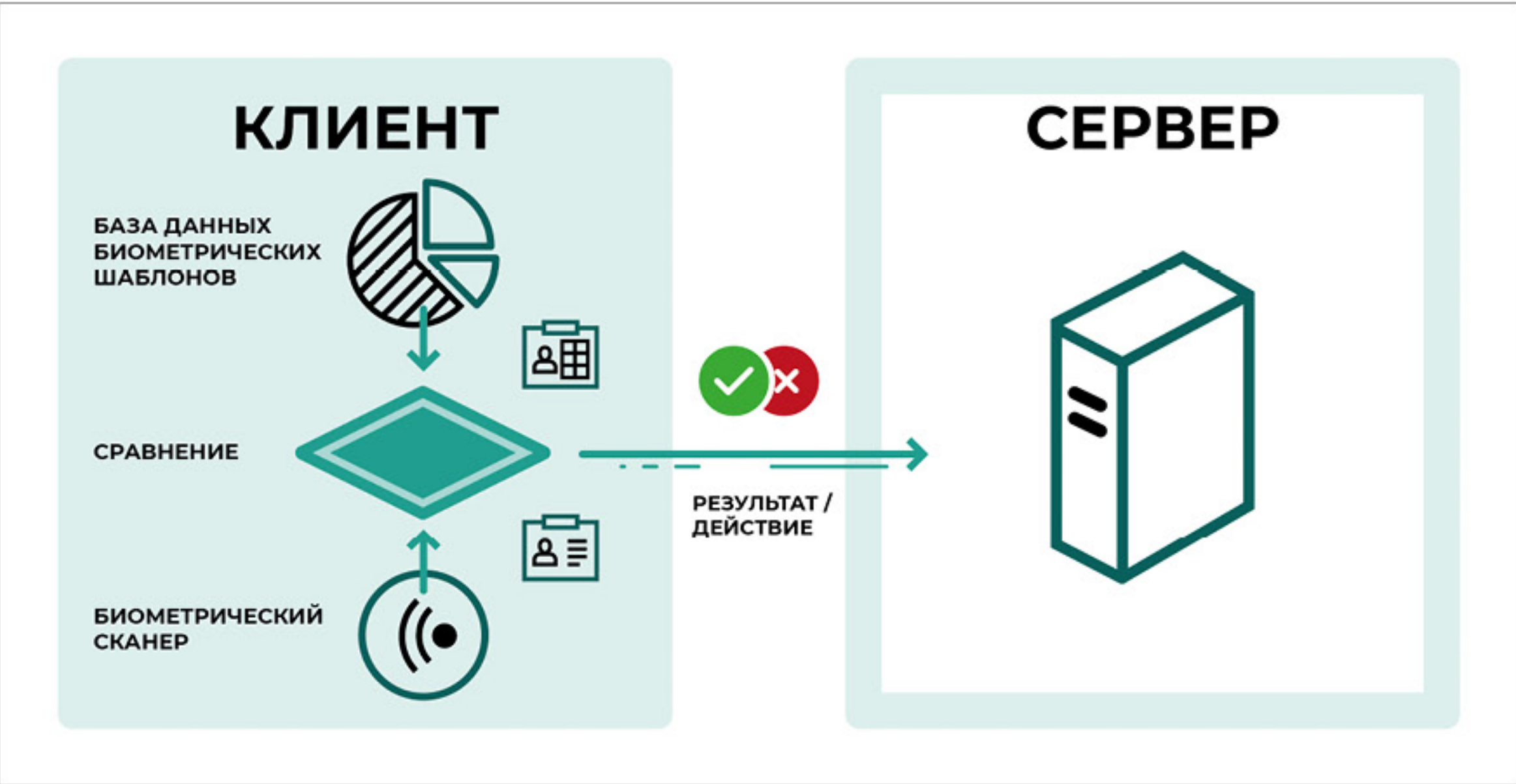


Рисунок 4. Локальная модель



Рисунок 5. Использование биометрической аутентификации в Apple iOS

преобразование в признаки, а также сравнение и получение решения по идентификации/верификации производится на клиентской стороне. Решение о биометрической аутентификации принимает или сервер (в случае если он получает оценку соответствия), или клиент, который устанавливает с сервером авторизованную сессию. Локальная модель на данный момент — наиболее распространённая схема аутентификации при помощи биометрии. Такая модель используется, например, в мобильных устройствах Apple iOS (Рис. 5) и на базе операционной системы Android.

Верхнеуровнево обычный процесс аутентификации пользователя на сервере при помощи биометрии для некоторого приложения Apple iOS выглядит следующим образом. Сканер отпечатков пальцев мобильного устройства (TouchID) снимает образ отпечатка и отправляет его в Secure Enclave. Secure Enclave¹ — это защищённый сопроцессор, который использует шифрованную память, включает в себя аппаратный генератор случайных чисел, который используется для генерации ключей. Ключи используются для шифрования и дешифрования данных, хранящихся в памяти. Ключи также используются для шифрования и дешифрования данных, передаваемых по сети. Ключи также используются для шифрования и дешифрования данных, хранящихся на сервере. Ключи также используются для шифрования и дешифрования данных, передаваемых по сети. Ключи также используются для шифрования и дешифрования данных, хранящихся на сервере. Ключи также используются для шифрования и дешифрования данных, передаваемых по сети.

¹ Безопасность iOS. iOS 10. Март 2017 г. Раздел «Безопасность системы», пункт Secure Enclave (https://images.apple.com/ru/business/docs/iOS_Security_Guide.pdf)

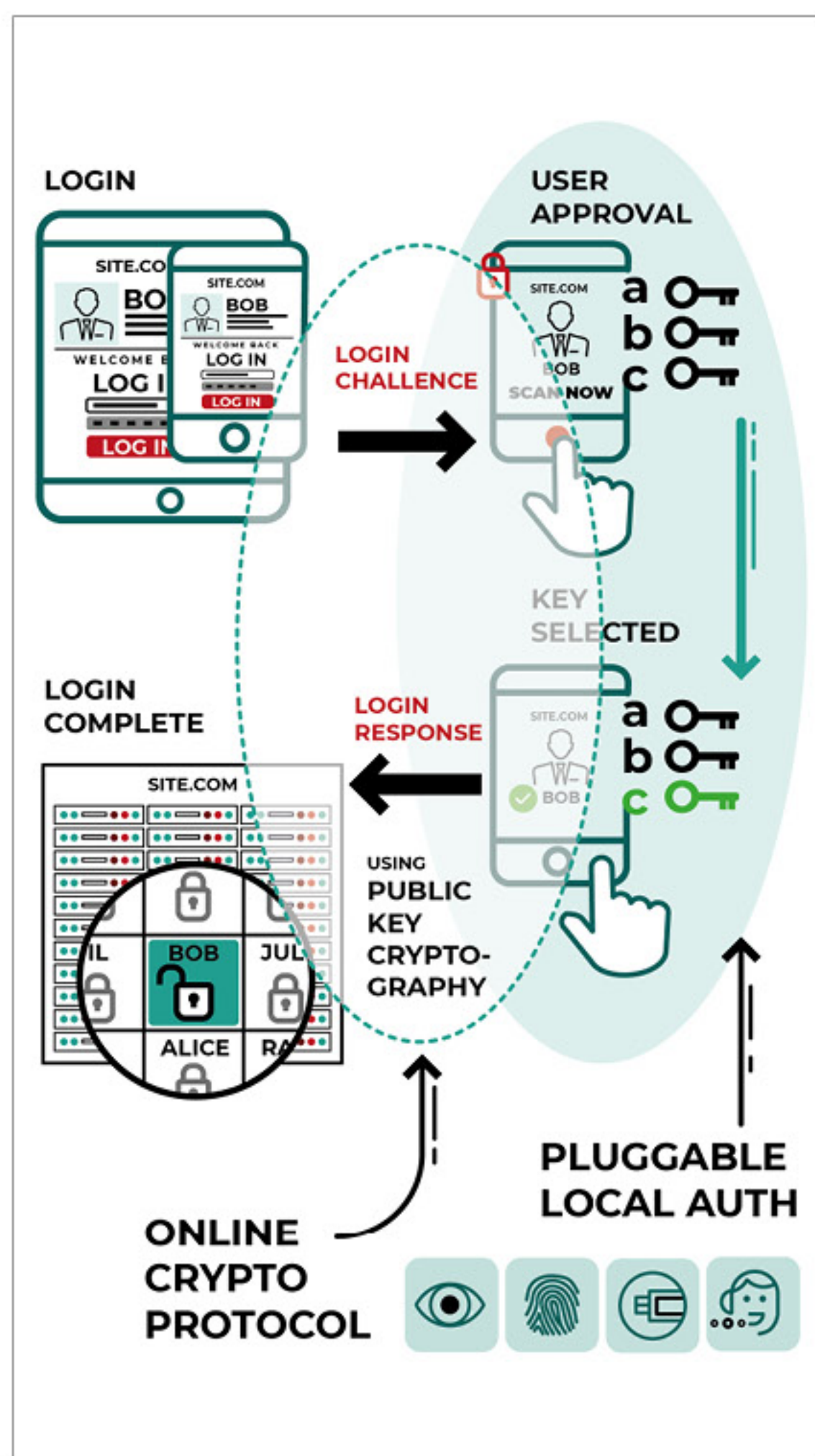


Рисунок 6. Процесс аутентификации в соответствии со спецификацией FIDO UAF

ратор случайных чисел и обеспечивает выполнение всех криптографических операций для управления ключами защиты данных. Secure Enclave, используя пароль пользователя, ключ устройства, ключи классов и т.п., предоставляет доступ к связке ключей или защищённому файлу². В них хранится тот самый аутентификатор, при помощи которого приложение может аутентифицироваться на сервере. Например, в случае мобильного приложения дистанционного банковского обслуживания Сбербанка — это PIN-код, а протокол аутентификации — Secure Remote Protocol (SRP)³. Этот протокол был выбран, так как он не предусматривает ни в каком виде передачу от приложения на сервер самого секрета (PIN-кода) при аутентификации. Аутентификация производится двухэтапным прото-

² Процесс предоставления доступа достаточно сложный и многоуровневый. Его описание — не цель данной статьи. Подробнее можно посмотреть в «Безопасность iOS. iOS 10. Март 2017 г. Раздел «Шифрование и защита данных» (https://images.apple.com/ru/business/docs/iOS_Security_Guide.pdf)

³ RFC: <https://tools.ietf.org/html/rfc2945>

ЛОКАЛЬНАЯ АУТЕНТИФИКАЦИЯ



Рисунок 7. Процесс локальной аутентификации FIDO UAF

колом, основанном на применении технологии криптографии с открытым ключом.

Такой же принцип аутентификации по биометрии предлагается использовать организацией FIDO Alliance⁴ в спецификации Universal Authentication Framework (UAF)⁵ (Рис. 6).

Аутентификатором могут служить различные устройства или программы, прошедшие аттестацию в альянсе. Основным принципом в данном случае является начальное распределение закрытых и открытых ключей между аутентификатором и сервером (см. рисунок 6). Ключи генерируются в аутентификаторе, закрытый сохраняется в нём, а открытый передаётся на сервер для проведения аутентификации в дальнейшем. Доступ к закрытому ключу, находящемуся в аутентификаторе, пользователь может получить после прохождения локальной аутентификации при помощи различных технологий, которые поддерживает производитель аутентификатора, в том числе биометрических признаков (Рис. 7).

Уже большое количество производителей провели аттестацию своих технологий в альянсе. В случае биометрической аутентификации можно привести пример российской компании VisionLabs для технологии распознавания лиц в мобильном телефоне на базе Android.

Локальная модель биометрического процесса обладает очень высокой степенью защищённости, и уже существуют качественные стандарты на разработку средств, которые используют данную концепцию.

⁴ <https://fidoalliance.org/>

⁵ <https://fidoalliance.org/download/>

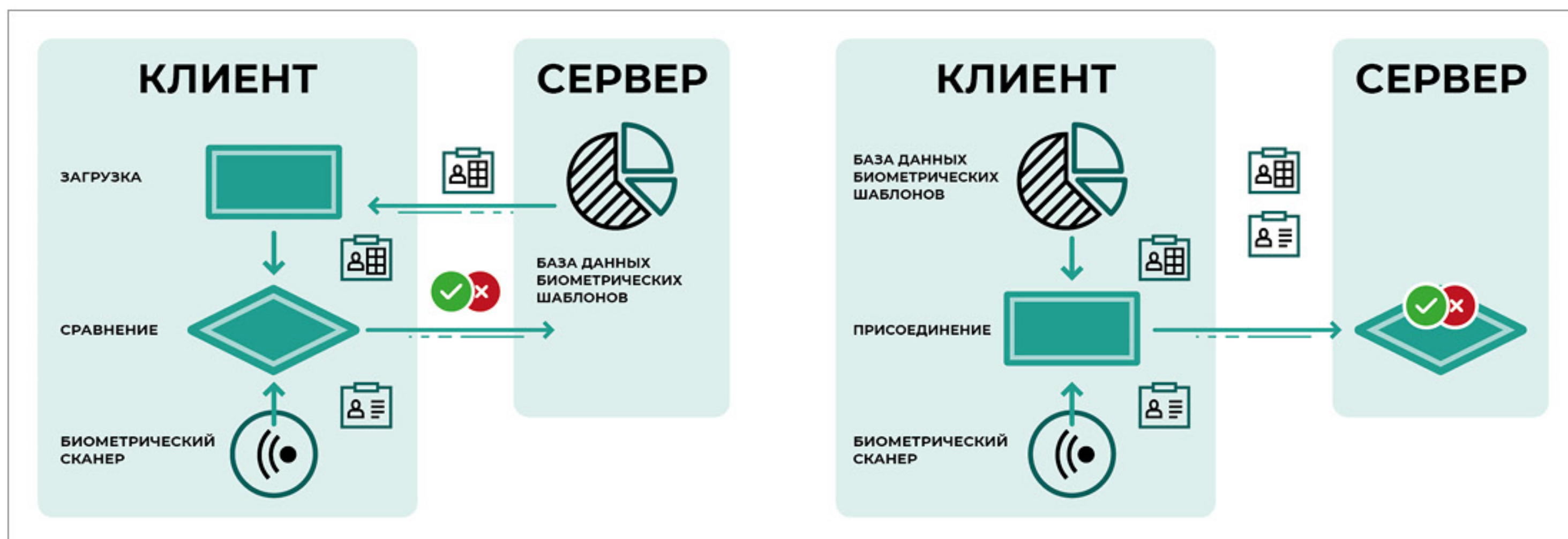


Рисунок 8. Промежуточные модели

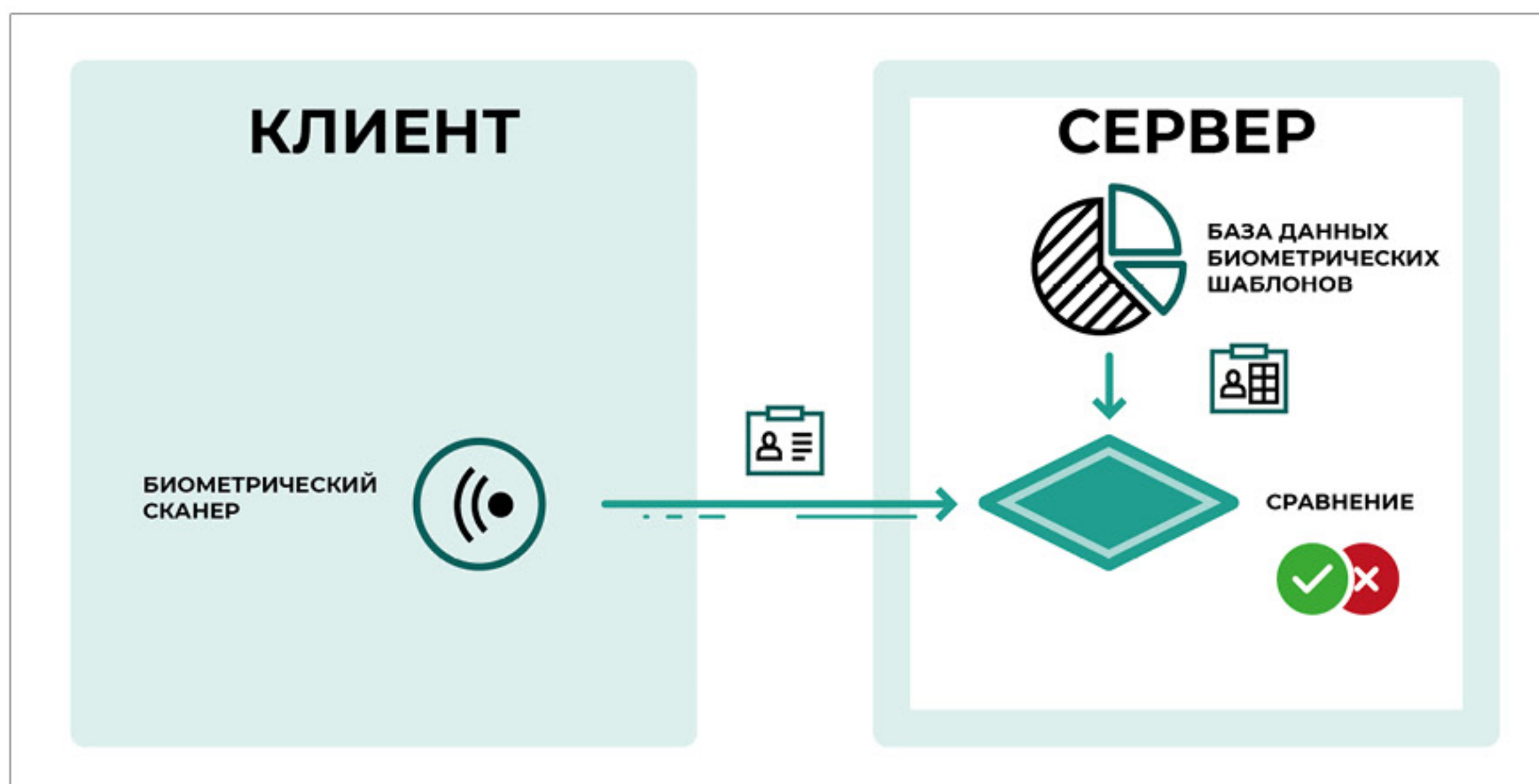


Рисунок 9. Централизованная модель

Промежуточные модели биометрического процесса — модель с загрузкой шаблона и модель с присоединением данных — являются переходными между локальной и централизованной моделями. Они не очень распространены и используются в специфических приложениях (Рис. 8).

И, наконец, мы подошли к самой интересной для нас модели биометрического процесса — централизованной (Рис. 9).

В этой парадигме биометрический сканер снимает биометрические признаки пользователя, возможно, предобрабатывает их, а затем отправляет на серверную часть, где и происходит сравнение с биометрическим шаблоном для вынесения резолюции. Централизованная модель удобна тем, что, однажды предоставив на сервер свои биометрические признаки определенной модальности, пользователь может в дальнейшем выбирать практически любой ка-

нал доступа к серверу при аутентификации. Такой подход называется омниканальностью. Он очень удобен и для клиентов, и для организации.

Локальная модель успешно применяется на собственных устройствах пользователя (например, на мобильном устройстве), однако в случае экстраполяции на многопользовательские устройства такой подход не работает — ведь локально на биометрическом сканере хранить отпечатки миллионов клиентов, мягко говоря, затруднительно.

Именно поэтому как Единая биометрическая система (ЕБС), так и собственная биометрическая платформа Сбербанка используют централизованную модель биометрического процесса. ЕБС предполагает, что регистрировать биометрические признаки, а это пока что лицевая и голосовая биометрия, клиенту нужно в отделениях банка, а использовать биометрию при идентификации и верификации можно будет уже в разных

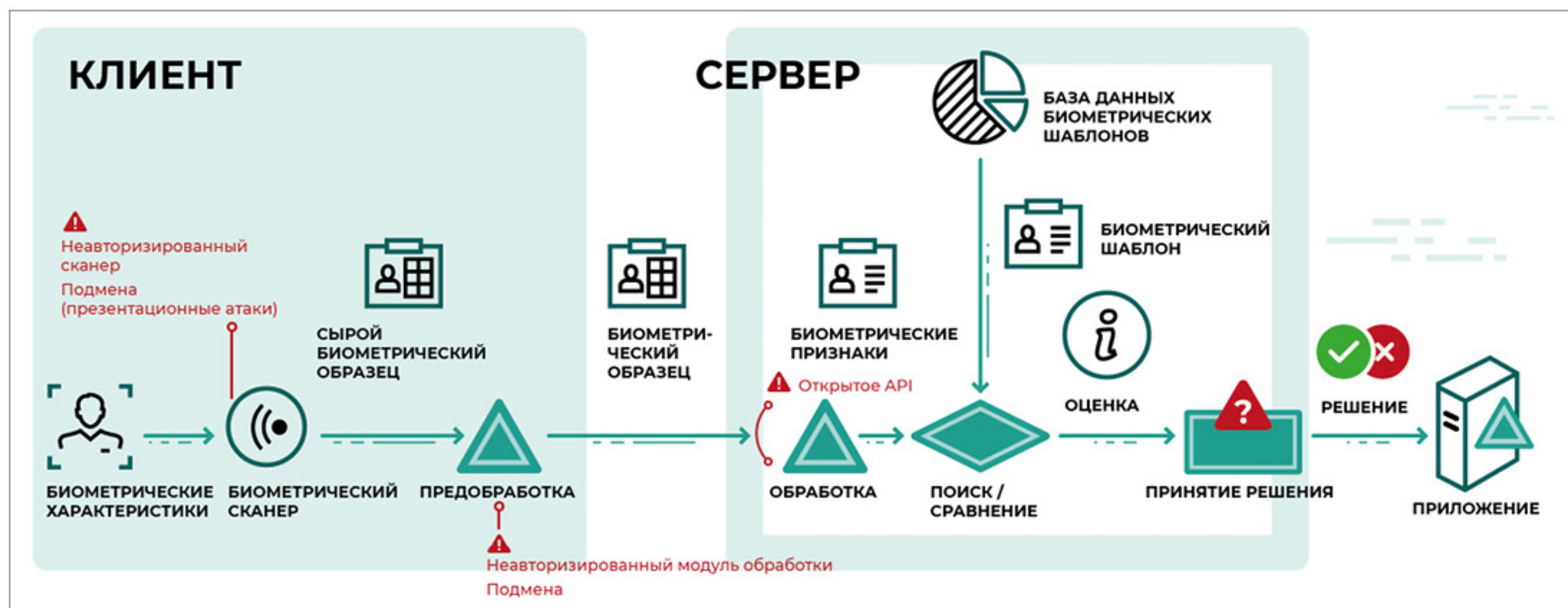


Рисунок 10. Выделяемые риски централизованной модели

каналах обслуживания. Сбербанк же планирует открыть для своих клиентов возможность регистрации биометрических признаков в том числе и удалённо: с помощью мобильного приложения или устройства самообслуживания. Наш банк использует для биометрической регистрации и аутентификации риск-ориентированный подход.

РИСКИ БИОМЕТРИЧЕСКОГО РАСПОЗНОВАНИЯ В ЦЕНТРАЛИЗОВАННОЙ МОДЕЛИ

Централизованная модель несёт больше киберрисков, нежели локальная. Основной её риск — подмена данных, которые направляются клиентской компонентой на серверную часть (Рис. 10). Действительно, сервер «не знает», откуда пришли данные. А для получения такого знания ему необходимо каким-то образом аутентифицировать клиентскую компоненту, передающую биометрический образец, которая может находиться и на другой стороне земного шара.

При использовании биометрических процессов во внутренней сети особенных рисков при использовании централизованной модели не возникает. Однако при предоставлении биометрии во вне, как услуги, — всё меняется.

ЕБС предоставляет банкам открытое API и, по сути, уходит от решения проблемы, перекладывая её на плечи самих банков. Биометрический образец нужного формата должен попасть в ЕБС от имени банка, а перед этим сам банк должен удостовериться, что это не «липа».

Когда-то серверное API было закрытым, и передать через него подложный биометрический образец было практически невозможно. Однако сегодня провести реверс-инжиниринг не составляет каких-либо проблем, поэтому сохранение в тайне протокола взаимодействия своего API

нельзя считать мерой защиты. Кроме того, в самых разных индустриях, включая финансы, побеждает концепция открытого API. Например, Сбербанк стремится превратиться в финансовую экосистему и начал предоставлять финтеху открытое API⁶. Поэтому необходимо говорить о полноценном встраивании в открытое API функций по идентификации и аутентификации клиентских компонент. Это может быть как некоторый API-ключ, так и использование криптографической подсистемы, например, на базе PKI.

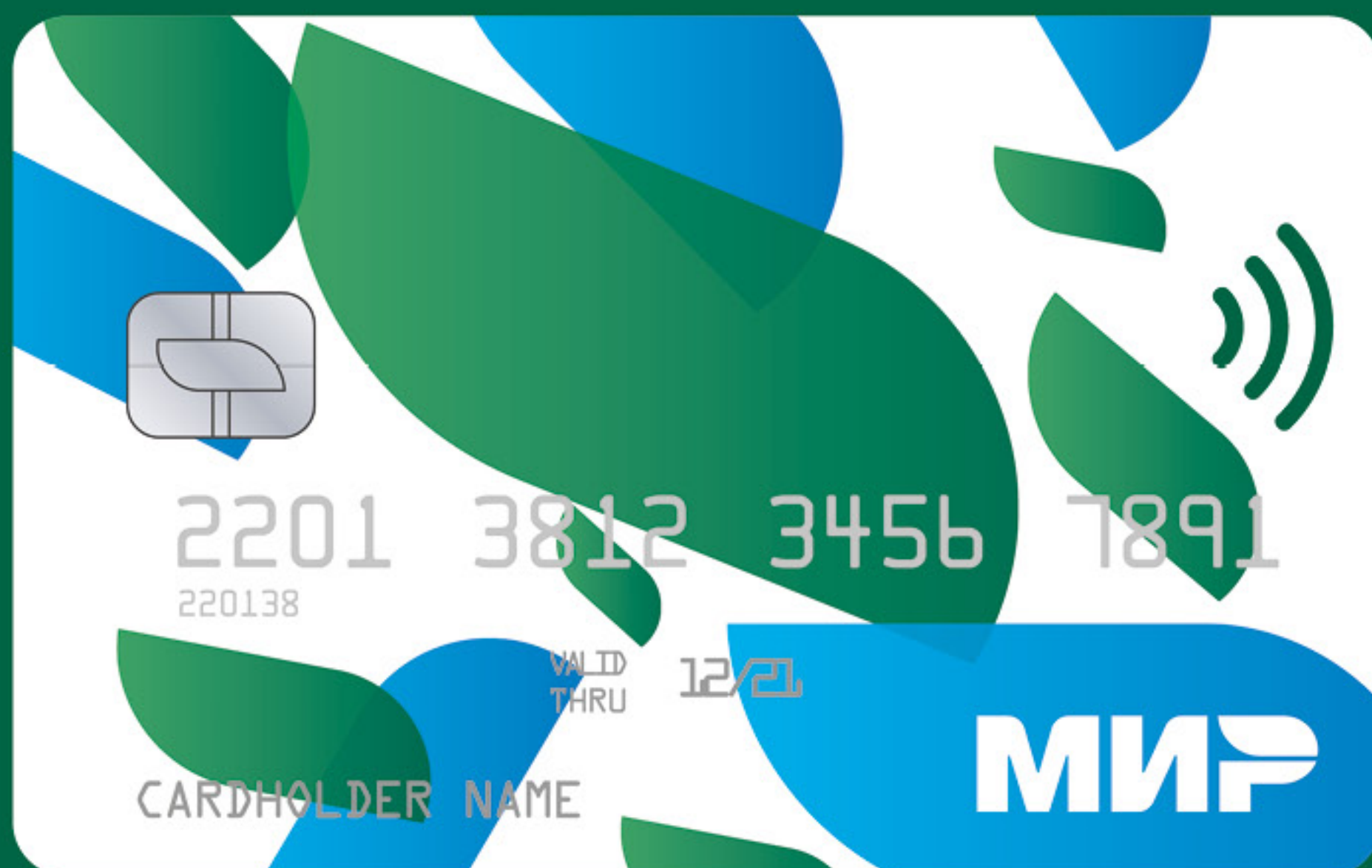
Основной проблемой при таком встраивании становится распределение ключей аутентификации клиентской компоненты. Например, если мы говорим об отделениях банка, то такой компонентой является компьютер операциониста. Такие компьютеры в банке учитываются, они используют встроенные или наложенные средства защиты, и на них могут быть распределены их аутентификаторы. Однако биометрические технологии приходят не только на стационарные места операционистов, но и на собственные устройства клиентов банка, обычно мобильные, контролировать которые банк не может, да и не имеет такого права.

Статическое распределение аутентификаторов для мобильных устройств клиентов, к сожалению, проблематично. Если встроить ключ доступа или криптографический закрытый ключ в код мобильного приложения, то завтра он будет известен всем. А если распределять такие аутентификаторы на каждое приложение, то как удалённо связать аутентификатор с конкретным приложением?

(Продолжение в следующем номере)

⁶ <https://developer.sberbank.ru/>

МИР



Карта «Мир» - современная, технологичная и безопасная платежная карта.

Обладает всем привычным платежным функционалом и принимается на всей территории России.

Удобный, выгодный и надежный инструмент для совершения платежных операций.

mironline.ru



Сергей ВИХОРЕВ
советник
по информационной
безопасности
генерального директора
ООО «ИТ-экспертиза»



ДЁРНИ ЗА ВЕРЁВОЧКУ, ДИТЯ МОЁ, ДВЕРЬ И ОТКРОЕТСЯ!

ЭССЕ О ВЛИЯНИИ СКАЗОК НА ИБ

В зрелом возрасте, да ещё обладая профессиональной деформацией сознания, начинаешь по-иному смотреть на сюжеты знакомых сказок, видеть там то, чего раньше не замечал, и удивляться тому, как это отражает современную жизнь. К примеру, старый любимый мультфильм про пионера Петю и Красную Шапочку¹, помните? Там больная подслеповатая старушка просила посетителей самим открывать дверь, дёрнув за верёвоч-

ку. Под видом внучки в дом проник сначала Серый Волк, а потом и Петя Иванов. И только благодаря смекалке пионера не произошло беды: бабушка и внучка остались живы. Правда, в первоисточнике, у Шарля Перро, не всё так радужно: потребовалась резекция желудка Серого Волка.

И что же этот сюжет напоминает?

АССОЦИАЦИИ ИЛИ ПАРАНОЯ

Современные информационные технологии уже повзростели. Всё реже мы находим автономные компьютеры, всё чаще работа осуществляется в сети. Как правило, есть некий центральный

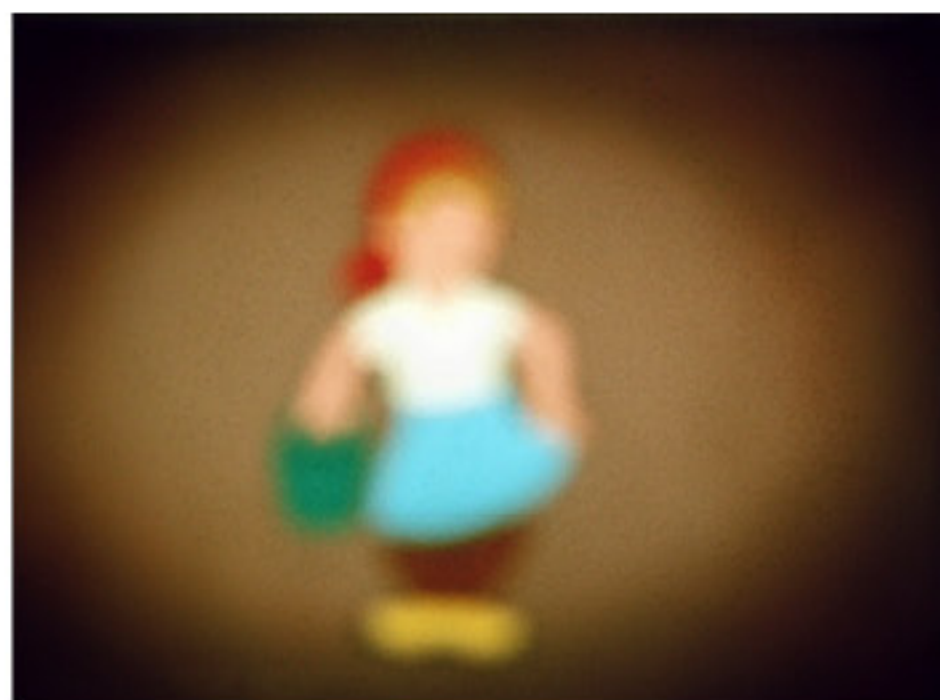
сервер, к которому все пользователи стучатся, чтобы получить доступ к информации. И такой сервер (или целый ЦОД) защищается, чтобы ценная информация, хранимая на нём, никуда не



¹ «Петя и Красная Шапочка» — советский мультипликационный фильм по сценарию Владимира Сутеева по мотивам сказки Шарля Перро «Красная Шапочка», Союзмультфильм, 1958

делась. Проще говоря, сервер (или целая сеть) находится в защищённом сегменте, к которому предъявляются особые требования по безопасности. И он подконтролен, и администратор безопасности следит за тем, чтобы соблюдались правила доступа, чтобы всё ПО было доверенное, чтобы, не дай Бог, не пролез какой-нибудь троян.

Но к этому серверу (или целой сети) вдруг стучится некто Имярек со своим компьютером, который, к великому сожалению, расположен неизвестно где, администрируется неизвестно кем, раньше был подключён неизвестно к какой сети, чем заражён — неизвестно и ещё много-много чего неизвестно. А администратор безопасности ничего проверить не может: территория и зона ответственности — не его, он туда доступа не имеет. Но работать пользователю надо! И это жёсткое требование бизнеса. Таких ситуаций в нашем современном мире — море: это и система ДБО, и сеть банкоматов, и виртуальные сети различных организаций, которые имеют удалённых или мобильных пользователей.



И в этой неоднозначной ситуации, когда исчезает само понятие «периметр», администратор безопасности сервера оказывается в роли той самой подслеповатой бабушки из сказки. Он стоит перед выбором: либо доверится «голосу» как бы доверенного пользователя и пропустить под его личиной в защищённую сеть Серого Волка, либо — не пускать пользователя в закрытую сеть и нарушить все бизнес-процессы.

«Опять пугалки! — скажет кто-то из читателей. — Что тут сложного! Пользователь проходит процедуру идентификации-аутентификации-авторизации, которая отработана, и всё — проблема решена!»

Да нет, не пугалки и не паранойя, а современные реалии информационных технологий, и не всё в них так просто. Положим, удалённый пользователь прошёл все установленные процедуры идентификации-аутентификации-авторизации, и у администратора безопасности нет, кажется, оснований не допускать пользователя в закрытую сеть. Но надо учитывать, что, как правило, к таким удалённым рабочим местам предъявляются требования безопасности, которые обязательно должны быть выполнены до подключения к защищённой сети. Например, должны быть заблокированы USB-порты, отключены некоторые службы операционной системы, установлены антивирусные средства, включены средства шифрования, надо чтобы на этом компьютере не запускались игры из Интернета и прочая, прочая, прочая. А теперь ответьте на вопрос: по результатам успешного прохождения процедуры идентификации-аутентификации-авторизации удалённого пользователя администратор безопасности защищённой сети может быть уверен, что все эти требования удалённым пользователем выполнены?



КОНЦЕПЦИЯ ДОВЕРЕННОЙ СРЕДЫ

В более ранних публикациях я уже выдвигал тезис о концепции «доверенной среды» как противовеса концепции «изолированной среды», предполагающей, что все элементы защищаемой системы должны быть изолированы от окружающей среды, что в современных условиях означает остановку всех бизнес-процессов. В то же время, в силу принципа декомпозиции, каждый элемент защищаемой системы может быть защищён и в этом случае, соединение их в единую информационную систему с помощью защищённых каналов

позволит создать вокруг информации (а не элементов информационной системы!) надёжную оболочку. Однако в этом случае мы должны быть уверены в лояльности всех элементов, то есть доверять им. Если мы сможем быть уверенными в надёжности каждого элемента, нам необязательно изолировать их в замкнутой среде. Это и есть смысл концепции «доверенной среды», которая требует:

- ♦ локализации информационных ресурсов, требующих защиты;
- ♦ счетности всех субъектов отношений и всех объектов защиты;
- ♦ доверенности конфигурации и настроек программного обеспечения и технических средств информационной системы и её удалённых элементов;
- ♦ целостности всех элементов информационной системы и её окружения;
- ♦ подконтрольности всех действий и документированности всех событий, влияющих на безопасность.

Практически все эти действия возможно реализовать на стороне нашего защищённого сервера (сети). За исключением одного: контроля доверенности конфигурации и настроек программного обеспечения и технических средств удалённого компьютера.



PRAEMONITUS, PRAEMUNITUS²

Да, при развитии технологий удалённого доступа в полный рост встаёт проблема не только идентификации самого пользователя, но и оценки доверия к тому устройству, на котором пользователь проводит процедуру идентификации-аутентификации-авторизации. Администратор безопасности должен иметь инструмент, позволяющий определить, что подключаемое к системе устройство действительно

² Предупреждён — значит вооружён (лат.)

Красная Шапочка, а не Серый Волк. То есть такой инструмент должен позволять проводить контроль технических параметров удалённых рабочих мест, влияющих на информационную безопасность. По видимости такой инструмент, назовём его «Системой активного мониторинга состояния рабочих мест при подключении к информационной системе», должен позволять следить за аппаратным и программным обеспечением рабочих мест, определять тип и состав зарегистрированных USB устройств, проверять запущенные в операционной системе процессы и доступность сетевых сред, работу антивирусных средств.

Кроме того, такая система мониторинга должна уметь регистрировать любые события, влияющие на безопасность рабочего места и, в частно-

сти, регистрировать любые изменения в аппаратной и программной среде, нарушения правил информационной безопасности.

Ну, и наконец, система мониторинга должна быть проактивной, осуществлять мониторинг не только в момент подключения рабочего места к информационной системе, но и в течение всего сеанса взаимодействия с определённой периодичностью, а также уметь блокировать подключение рабочего места в случае нарушения установленных требований безопасности информации как в автоматическом режиме, так и вручную.

Надо также учитывать, что в современных информационных системах уже используются различные системы контроля состояния безопасности информации. Поэтому система активного

мониторинга должна быть сопрягаема с другими системами и уметь экспортировать в них события безопасности информации.

* * *

К большому сожалению, на рынке ИБ такие системы практически не представлены. И тут есть о чём задуматься нашим отечественным разработчикам. А может быть именно сейчас и появляется новый класс систем защиты, например, SAMW — system of active monitoring of the workplace... Это — мысли вслух, простой перевод упоминаемой фразы «система активного мониторинга состояния рабочих мест» в стиле Гартнера. Но, может, это и есть начало «систем поведенческого анализа технических средств»?



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

СКАЗКА — ЛОЖЬ? КАКОЙ-ТО ТАМ НАМЕК? РАЗВЕ?

Правда или ложь — результат логической операции. Если предположить, что утверждения, изложенные в статье — ложь, то какой это урок? Типичная профессиональная деформация виденья окружающей жизни. По логике профессионального защитника информации, любая полезная информация является одновременно полезной и несущей зло. И наше (деформированное) мышление видит только вторую составляющую.

Проблема Волк-Неволк, Бабушка-Небабушка стоит сейчас даже более остро, чем описал автор статьи. Но есть несколько «НО». Не то, чтобы все неправильно, нет, в целом всё правильно, НО, я бы сказал, 30 на 70.

Имярек действительно регулярно пытается врываться в защищаемую систему, но периметр уже сильно размыт, порой его просто нет. Доверенная среда не может существовать в открытых системах — защищённость среды определяется защищённостью/слабостью самого слабо-

го звена, а значит, самая маленькая дырочка в воздушном шарике мгновенно приводит в взрыву-разрыву оболочки этого шарика. Концепция безопасности должна строиться из предположения, что участники отношений действуют в условиях «заражённой» среды и доверять им можно только с определённой долей вероятности. Любые детерминистические (основанные на оценке состояния/изменения каких-либо технических параметров) методы аутентификации перестают работать и начинают работать вероятностные механизмы.

Но если продолжать следовать этой логике, то на самом деле предпоследний тезис статьи даёт ответ, как найти выход из ситуации, когда все участники являются пользователями удалённого доступа: надо только научиться анализировать поведение самого предполагаемого контакта и поведения его технических инструментов, надо научиться определять/запоминать/анализировать, что такое нормальное/типичное поведение, а что такое не нормальное, и на основании этого принимать решение Волк/Неволк.

* * *

А вот финальный пассаж — напрасная печаль. Сегодня на нашем российском рынке фактически происходит маленькая революция в продуктах поведенческого анализа и людей, и технических средств, и это вселяет настоящий оптимизм. Не хочу их рекламировать, но они есть и очень неплохо развиваются.

С уважением к моему давнему другу Сергею Вихореву.

BIS-КОММЕНТАРИЙ

СООТВЕТСТВИЕ СТАНДАРТУ БЕЗОПАСНОСТИ ПЛАТЁЖНЫХ КАРТ



**Дмитрий
СЛОБОДЕНЮК**
коммерческий
директор ARinteg

КОМПАНИЯ ARINTEG ПОМОГАЕТ ПРОЙТИ ОБЯЗАТЕЛЬНУЮ ПРОЦЕДУРУ ПРОВЕРКИ ВСЕХ ТОЧЕК ПОДКЛЮЧЕНИЯ К СЕТИ ИНТЕРНЕТ НА НАЛИЧИЕ УЯЗВИМОСТЕЙ

Каждый день в мире детектируется порядка 350 тысяч новых вредоносных программ, которые угрожают безопасности сетевой инфраструктуры финансовых организаций и международных платёжных систем. Защитить транзакции и своевременно установить различного рода уязвимости призвана процедура ASV-сканирования. О том, для чего проводится данная проверка, рассказывают специалисты компании ARinteg — одного из ведущих российских системных интеграторов по информационной безопасности.

ASV-СКАНИРОВАНИЕ: ЧТО ЭТО ТАКОЕ?

ASV-сканирование — это процедура ежеквартальной проверки всех точек подключения к сети интернет на наличие уязвимостей. Разработана Советом по стандартам безопасности данных индустрии платёжных карт (создан по инициативе American Express, Discover Financial Services, JCB International, MasterCard Worldwide и Visa, Inc.).

КТО ОБЯЗАН ПРОХОДИТЬ ПРОВЕРКУ?

Процедура ASV-сканирования на предмет соответствия требованиям международного стандарта безопасности PCI DSS распространяется на все организации, которые хранят, обрабаты-

вают или передают данные держателей платёжных карт.

Такие компании классифицируются, исходя из объёма транзакций, проводимых в течение года:

- ♦ 4 уровень — до 20 тысяч транзакций в год (ежеквартальное сканирование внешних адресов на наличие уязвимостей и заполнение листа самооценки);

- ♦ 3 уровень — от 20 тысяч до 1 миллиона транзакций в год (аналогичные требования, что и для компаний 4-го уровня);

- ♦ 2 уровень — от 1 миллиона до 6 миллионов транзакций в год (ежеквартальное сканирование с привлечением компании-аудитора);

- ♦ 1 уровень — более 6 миллионов транзакций в год (проводится только с привлечением независимого аудитора).

Отдельная градация существует в отношении сервисных компаний и процессинговых центров.

КАК ПОДТВЕРДИТЬ СООТВЕТСТВИЕ ТРЕБОВАНИЯМ СТАНДАРТА PCI DSS?

Для прохождения ASV-сканирования необходимо обратиться к специализированным поставщикам услуг, аккредитованным Советом по стандартам безопасности данных индустрии платёжных карт.

ARinteg статус ASV-провайдера впервые был присвоен более трёх лет

назад. Ежегодно компания успешно подтверждает свой экспертный уровень.

Опираясь на многолетний опыт аудита защищённости внешнего периметра и внутренних сетей, специалисты системного интегратора по информационной безопасности помогают успешно проходить необходимые процедуры проверки на предмет соответствия PCI DSS.

В ЧЁМ ОСОБЕННОСТИ ИНСТРУМЕНТАЛЬНОГО СКАНИРОВАНИЯ?

Наряду с ASV-сканированием компания ARinteg предлагает организациям с развитой сетевой инфраструктурой воспользоваться услугой инструментального аудита информационной безопасности.

Эта проверка представляет собой комплексный анализ технологических уязвимостей автоматизированных систем, корректности работы конфигурационных настроек и степени защиты аутентификационной информации.

Инструментальное сканирование даёт возможность составить объективную картину о текущем состоянии корпоративной информационной системы, на основе которой будут выработаны приоритетные меры для предупреждения киберрисков.

Специалисты компании рекомендуют помимо ежеквартальных проверок



на предмет соответствия стандарту PCI DSS внести в годовой план не менее четырёх инструментальных сканирований. Это позволит каждые полтора месяца получать экспертную оценку актуальности уровня информационной безопасности ИТ-инфраструктуры организации.

КАК ПРОХОДИТ ПРОЦЕДУРА ASV-СКАНИРОВАНИЯ?

Сканирование проводится удалённо в формате выделенного технологического окна в течение 24 часов. Дату и время сканирования можно согласовать индивидуально.

Процедура ASV-сканирования абсолютно безопасна и не влияет на производительность сетевой инфраструктуры.

НЕОБХОДИМО ЛИ ЗАРАНЕЕ ГОТОВИТЬСЯ К ПРОВЕРКЕ?

На время проведения проверки обязательным требованием стандарта PCI DSS является отключение (переключение в режим мониторинга) средств активной защиты, основанных на поведенческом анализе (IPS, WAF).

В случае использования балансировщиков трафика требуется подтверждение синхронизации сетевых потоков.

ЧТО ПРОИСХОДИТ ВО ВРЕМЯ ПРОВЕРКИ?

В рамках тестирования определяется наличие доступных IP-адресов из списка, предоставленного заказчиком, проводится сканирование всего диапазона TCP-портов и стандартных UDP-портов.

Осуществляется попытка точной идентификации используемых версий операционных систем и запущенных сервисов вне зависимости от используемых платформ.

Процедура проверки позволяет:

- ♦ определить уязвимости (как известные CVE, так и уникальные), ошибки конфигурации серверов приложений и DNS-серверов;
- ♦ обнаружить стандартные веб-скрипты;
- ♦ проверить защищённость почтовых сервисов, использования встроенных учётных записей и средств удалённого доступа, а также корректность работы POS-терминалов;
- ♦ оценить подверженность типичным атакам на веб-приложения (SQL-injection, XSS, перемещение по директориям, разбитие HTTP-заголовков) и актуальных версий TLS-шифрования;
- ♦ выявить избыточность стандартных сервисов;
- ♦ детектировать бэкдоры, руткиты, иное вредоносное ПО.

КАКОЙ ДОКУМЕНТ ВЫДАЁТСЯ ПО ИТОГАМ ASV-СКАНИРОВАНИЯ?

По результатам сканирования предоставляется отчёт, в котором указываются подтверждённые и потенциальные уязвимости с развёрнутой информацией по каждой из них — уровень риска, статус PCI, CVSS-оценка, семейство, CVE-код, а также рекомендации по приведению информационной системы в соответствие со стандартом PCI DSS.

В случае выявления недопустимых уязвимостей критичностью выше 4 уровня, заказчик может оспорить их справедливость, предоставив подтверждения ложного срабатывания сканера.

При обнаружении средств удалённого доступа, POS-терминалов или иных механизмов приёма платежей, возможности листинга директорий потребуются обоснование необходимости и защищённости применяемых решений.

Более подробно узнать о преимуществах ASV-сканирования от ARinteg и оставить заявку на проведение проверки можно с помощью специализированного сервиса — <https://asv.arinteg.ru>.



ASV-сканирование — это процедура проверки всех точек подключения информационной системы к сети интернет на наличие уязвимостей в рамках стандарта PCI DSS.

Должно выполняться ежеквартально.

ARinteg — аккредитованный ASV-провайдер.

ОСОБЕННОСТИ

- ▶ Проводится удалённо в выделенном технологическом окне продолжительностью до 24 часов.
- ▶ Не влияет на целостность и стабильность работы ИТ-инфраструктуры.
- ▶ Возможность выбора тарифного плана для разового и ежеквартального сканирования в течение года.

ДЕТЕКТИРУЮТСЯ ИМЕЮЩИЕСЯ УЯЗВИМОСТИ

ВЫДАЕТСЯ ОТЧЁТ О СООТВЕТСТВИИ СТАНДАРТУ PCI DSS



ИНСТРУМЕНТАЛЬНОЕ СКАНИРОВАНИЕ

- Элемент комплексного аудита состояния дел в ИБ.
- Отсутствует привязка к какому-то одному промышленному стандарту (не зависит от положений стандарта PCI DSS).
- Наиболее эффективно при регулярном проведении процедуры.
- Позволяет повысить эффективность проведения PEN-теста.



**Владимир ШИЛИН**

руководитель дирекции системных проектов АО «РНТ», кандидат технических наук

**Роман КОЗЫРЬ**

эксперт по информационной безопасности АО «РНТ»

ЗАКОН В ТРЕНДЕ

187-ФЗ И ЕГО ПРИМЕНИМОСТЬ В БАНКОВСКОЙ СФЕРЕ

С 1 января 2018 года вступил в силу Федеральный закон от 26.07.2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Закон направлен на реализацию мер защиты IT-систем государственных и коммерческих организаций, сбои в работе которых могут привести к тяжёлым социальным, политическим, экономическим, экологическим последствиям, а также помешать обеспечению обороноспособности, безопасности государства и правопорядка. В число сфер деятельности, участники которых указаны в законе как субъекты критической информационной инфраструктуры (КИИ), включены банковская и иные сферы финансового рынка. Согласно указанному в Постановлении Правительства РФ № 127 от 08.02.2018 г. перечню показателей критериев значимости объектов КИИ, значительное число банков относятся к субъектам КИИ и будут обязаны выполнять требования 187-ФЗ.

За неисполнение требований 187-ФЗ предусмотрена ответственность для организаций и ответственных лиц, вплоть до уголовной.

ЭТАПЫ РЕАЛИЗАЦИИ 187-ФЗ

Закон подразумевает поэтапную реализацию его требований, которые мы рассмотрим далее.

Первый этап включает определение принадлежности организации к субъектам КИИ. Реализация возложе-

на на саму организацию, в рамках которой необходимо составить перечень IT-систем (информационных систем), участвующих в деятельности банковской и иных сферах финансового рынка.

Вторым этапом необходимо провести категорирование объектов КИИ в соответствии с ПП РФ № 127. Реализация также возложена на саму организацию, включает в себя создание комиссии по категорированию, определение перечня процессов деятельности организации и выявление критических процессов, разработку перечня объектов КИИ, подлежащих категорированию, определение угроз безопасности и категории значимости для объектов КИИ. Критерии значимости объектов КИИ, напрямую касающиеся банковской сферы, указаны в п. 10 Перечня показателей критериев, утверждённых ПП № 127. В организациях, например, кредитно-финансовой сферы, возможно, потребуется рассмотрение и других критериев из ПП № 127. После этого подготовленный список объектов КИИ по форме, определённой в Информационном сообщении ФСТЭК России от 24 августа 2018 г. № 240/25/3752, необходимо направить во ФСТЭК России. Затем, после подготовки материалов по форме, предусмотренной Приказом ФСТЭК России № 236 от 22.12.2017 г., сведения о категорировании необходимо направить во ФСТЭК России, причём в случае отсутствия необходимости присвоения объектам одной из трёх категорий согласно ПП № 127, ФСТЭК также необходимо уведомить об этом.

В случае отсутствия у организации квалифицированных кадров для выполнения вышеуказанных этапов, возможно привлечь к этому сторонние организации, обладающие достаточной квалификацией, в частности АО «РНТ».

Третий этап заключается в создании или модернизации системы защиты объектов КИИ в соответствии с требованиями приказов ФСТЭК России № 235 от 21.12.2017 г., № 239 от 25.12.2017 г. и при необходимости — № 138 от 09.08.2018 г. Данный этап выполняется подразделением ИБ организации и лицензиатом ФСТЭК России по технической защите конфиденциальной информации. Весь комплекс работ включает в себя подэтапы, указанные ниже:

- ♦ Разработка требований к обеспечению безопасности объектов КИИ. Для этого необходимо провести обследование IT-систем объектов КИИ и анализ возможных угроз согласно присвоенным им категориям.

- ♦ Разработка технического задания на создание системы защиты. В нем определяются требования конкретно к системе защиты, основанные на предыдущем подэтапе, с учётом положений организационно-распорядительных документов по безопасности объектов КИИ, а также требования по взаимодействию с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (ГосСОПКА) в соответствии с приказами ФСБ России № 367 и № 368 от 24.07.2018 г.

♦ Разработка организационных и технических мер по обеспечению безопасности объекта КИИ. На данном подэтапе определяются адекватные средства защиты для объекта КИИ и необходимый комплект документации в соответствии с требованиями приказа ФСТЭК России № 239 от 25.12.2017 г. Далее происходит проектирование системы безопасности и разрабатывается эксплуатационная документация.

♦ Внедрение организационных и технических мер защиты. На этом подэтапе проводятся работы по внедрению системы безопасности и обучение ответственных сотрудников. При необходимости перед внедрением проводятся испытания выбранных средств защиты на специальном стенде с целью убедиться, что средства защиты не создадут проблем функционирования защищаемых объектов КИИ по их основному профилю. Также организуется взаимодействие с ГосСОПКА в соответствии с разработанными ранее требованиями.

♦ Опытная эксплуатация и аттестация объекта КИИ. Во время опытной эксплуатации проверяется стабильность работы защищённых IT-систем и самой системы защиты. По её результатам система защиты либо дорабатывается, либо принимается, и проводится её аттестация на соответствие требованиям по обеспечению информационной безопасности.

Также можно обозначить, условно, **четвёртый этап** — сопровождение созданной системы защиты. Он включает в себя техническую поддержку средств защиты и актуализацию документации и настроек в случае изменений в работе защищаемых IT-систем объектов КИИ. Это осуществляется либо сотрудниками самой организации, либо специализированной организацией на аутсорсинге.

ОБ ОТВЕТСТВЕННОСТИ

Стоит ещё раз упомянуть об ответственности для организаций — субъектов КИИ. Федеральным законом № 194-ФЗ от 26.07.2017 г. в УПК РФ внесены изменения в связи с принятием 187-ФЗ. В главу 28 УК РФ добавлена статья 274, подпункты 3, 4, 5 которой касаются субъектов КИИ и их ответственности за нарушение правил эксплуатации



средств хранения, обработки или передачи охраняемой законом информации, содержащейся в КИИ, либо правил доступа, если оно повлекло причинение вреда для КИИ. Также за несвоевременное предоставление информации во ФСТЭК России по первым двум этапам предусмотрена ответственность по ст. 19.5 КоАП РФ.

ВЫГОДА

Общий вывод из вышеуказанного следующий: несмотря на затраты на реализацию требований закона, итоговую выгоду можно получить в виде минимизации простоя сервисов из-за компьютерных атак и обеспечения непрерывности бизнеса. Также выполнение 187-ФЗ снимет большинство вопросов проверяющих органов в части выполнения требований федеральных органов исполнительной власти.

ЕСЛИ ТРЕБУЕТСЯ ПОМОЩЬ

Весь комплекс услуг по аудиту IT-систем и подготовке проектов документов по их принадлежности к КИИ и категорированию, проектированию, осуществлению поставок средств защиты и проведению работ по их внедрению, разработку всей необходимой документации, а также аттестацию и

последующее сопровождение систем защиты объектов КИИ может провести АО «РНТ», обладающее достаточным штатом квалифицированных специалистов и всеми необходимыми лицензиями на данные виды деятельности.

* * *

В заключение необходимо сказать, что сроки реализации требований закона на момент написания этой статьи следующие: выполнение первых двух этапов согласно ПП № 127 предполагается до 20.02.2019 г., после чего, согласно рекомендациям ФСТЭК России, создание систем безопасности значимых объектов КИИ должно пройти до 01.09.2019 г. Однако сейчас идёт активная работа по формированию итогового текста проекта по внесению изменений в ПП № 127, который также повлияет и на сроки. В текущем проекте срок выполнения первого этапа указан до 01.06.2019 г., второго этапа — не позднее 6 месяцев со дня окончания первого этапа в самой организации. Скорее всего, изменения в ПП № 127 будут приняты, и время, данное для определения и категорирования объектов КИИ, будет продлено.

**Роман ЖУКОВ**директор центра компетенций
информационной безопасности
«Гарда Технологии»

ГАРДА АНАЛИТИКА

ПЛАТФОРМА ИНФОРМАЦИОННОЙ И ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Активный рост киберугроз, развитие средств связи и интернет-технологий вывели безопасность бизнеса на первый план. Информация стала общедоступной, возможность коммуникаций — тотальная. Для выявления всего поля угроз требуются системы нового класса, способные обрабатывать миллионы событий в режиме реального времени и отображать результаты анализа в едином интерфейсе.

Анализ всех типов коммуникаций из максимально возможного числа информационных систем, машинное обучение, непрерывное обогащение данных и их анализ за секунды даёт возможность службе безопасности быть в курсе всех событий в сети компании. Это позволяет оперативно реагировать на несанкционированные действия пользователей и внешних злоумышленников, обеспечивать проактивную защиту.

Так работает новая платформа информационной и экономической безопасности на основе технологии больших данных — «Гарда Аналитика».

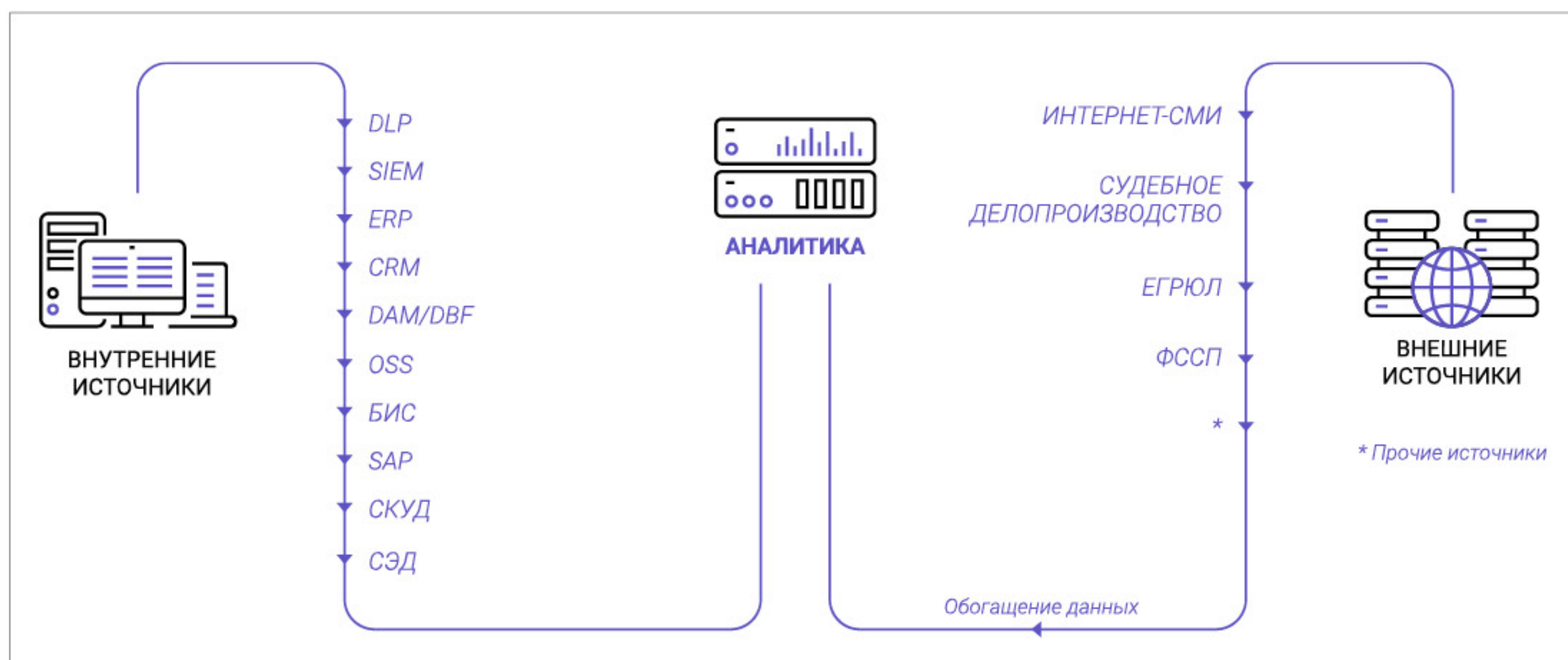
Согласно исследованию Kuppinger-Cole и BARC «Большие данные и информационная безопасность» BI-Sur-

ГАРДА АНАЛИТИКА

«Гарда Аналитика» — платформа информационной и экономической безопасности:

- ♦ решение класса Big Data Security Analytics (аналитика безопасности больших данных);
- ♦ обеспечивает видимость информации за пределами существующих возможностей в информационных системах;
- ♦ работает как центр управления безопасностью организации;
- ♦ интегрируется с внутренними прикладными системами: SIEM, ERP, CRM, DLP, DAM/DBF, OSS и пр.;
- ♦ использует внешние информационные системы для обогащения данных. (ЕГРЮЛ, ФССП, судебные делопроизводства и пр.);
- ♦ связывает события, полученные из различных систем и бизнес-приложений;
- ♦ производит сбор и анализ огромных объёмов данных — обрабатывает свыше 25 тысяч событий в секунду, в оперативном доступе находится сотни миллиардов связей и десятки одновременно подключённых источников данных;
- ♦ объединяет в себе сразу несколько передовых технологий анализа и работы с большими данными: описательная статистика — автоматизированный поиск аномалий в потоке событий, предсказательная аналитика — прогнозирование на основе накопленных данных, поведенческий анализ и машинное обучение.

«Гарда Аналитика» — полностью российская разработка, не требует сторонних лицензионных компонентов.



vey¹, решения класса Big Data Security Analytics — новая эра применения больших данных в сфере безопасности бизнеса и новое оружие против киберугроз.

По мере насыщения информационного поля организации и подключения всё большего числа прикладных систем происходит тотальная цифровизация документов и процессов. Отслеживать все непрерывные изменения в них специалисту, отвечающему за безопасность, практически невозможно.

«Гарда Аналитика» обеспечивает глобальную видимость информации за счёт интеграции и анализа информации из внутренних и внешних источников. Система собирает и анализирует данные не только из имеющихся систем безопасности, но и из прикладных информационных систем компании и внешних источников, таких как ЕГРЮЛ, ФССП и прочих, работая при этом в режиме реального времени. Исходные события постоянно обогащаются новыми сведениями, предоставляя службе безопасности полную картину происходящего в организации и за её пределами.

Принцип работы системы заключается в автоматизации процессов обнаружения отклонений в поведении сотрудников и систем, за счёт непрерывного

«Гарда Аналитика» — это не просто новый инструмент, а целый комплекс мероприятий, с принципиально новым подходом, включающий возможность создания и непрерывной актуализации базы сценариев

сбора и анализа поступающих данных. Платформа определяет и строит связи между ними, позволяя раскрывать мошеннические схемы, выявлять злоумышленников и оперативно реагировать на различные виды инцидентов. Качество и высокая степень автоматизации выявления угроз достигаются за счёт применения методов машинного обучения и поведенческой аналитики. Именно это и позволяет использовать «Гарда Аналитика» как реальный инструмент контроля оперативной обстановки в компании.

«Гарда Аналитика» — это не просто новый инструмент, а целый комплекс мероприятий, с принципиально новым подходом, включающий возможность создания и непрерывной актуализации базы сценариев.

Возможность гибко адаптироваться к новым угрозам — одна из ключевых особенностей платформы. При создании «Гарда Аналитика» уделялось особое внимание выстраиванию целой экосистемы безопасности, позволяющей подключать большое число раз-

нородных источников событий. В частности, бесшовная интеграция наших решений по защите от утечек информации, мониторингу бизнес-приложений, баз данных и сетевого трафика позволяет обеспечить глобальную видимость всей внутренней обстановки в компании за пределами возможностей отдельно взятых информационных систем.

«Гарда Аналитика» открывает широкие возможности для решения задач безопасности, таких как оперативная оценка кандидата или контрагента, контроль бизнес-процессов организации, анализ финансовых операций, контроль целостности и защита критических данных в информационных системах, обнаружение атак, заражений и теневых информационных технологий, выявление транзакционного и телекоммуникационного фрода, мошенничества при закупках, производстве и сбыте.

¹ <https://bi-survey.com/big-data-security-analytics>

**Денис ГОЙДЕНКО**старший специалист отдела реагирования
на угрозы ИБ, PT Expert Security Center,
Positive Technologies

ИНЦИДЕНТ: ПОЧЕМУ, КАК И ЧТО В ИТОГЕ?

КАЖДЫЙ АСПЕКТ ТРЕБУЕТ РАБОТЫ

Подход, согласно которому система ИБ в теории способна защитить от всех возможных угроз, постепенно заменяется пониманием того, что даже хорошо выстроенная защита может иметь недостатки, чреватые инцидентами. В реальности ИБ спотыкается о банальное несоблюдение основ кибергигиены: в большинстве аудитов мы сталкиваемся с необновленным ПО, с отсутствием культуры патч-менеджмента, с дырявым периметром. Компании нередко рискуют потерять критичные данные и, в итоге, деньги и репутацию. Всё это отчасти определило историю 2018 года, когда число инцидентовросло в среднем на треть[1] в квартал. Эффективная система реагирования на инциденты позволяет перевести эти события из разряда катастроф в неприятные, но разрешимые рабочие моменты. Но при её создании стоит учесть ряд нюансов.

ПРИЧИНЫ ИНЦИДЕНТОВ

Доверчивость и любопытство. Один из главных рисков — люди, открывающие вложения в письмах, не думая об их безопасности. Более 25% сотрудников не только открывают фишинговые письма, но и переходят по зараженным ссылкам[2]. Часто эти письма маскируют под приглашения на мероприятия, сообщения от регуляторов (например, ФинЦЕРТ) и других игроков банковского рынка. В 61% атак на банки

в первой половине 2018 года мы отмечали именно эти методы. Ими пользуются небезызвестные группировки Cobalt[3] и Silence[4]. Наиболее вероятная мишень преступников при этом — банки среднего звена, у которых можно украсть значительные суммы денег и которые не готовы вкладывать сверхбюджеты в безопасность.

Аморфная инфраструктура. IT-инфраструктура — многокомпонентный механизм автоматизации бизнес-процессов финансовой организации. Но она же может стать источником проблем ИБ. Выставленные в интернет сервисы удалённого доступа, которые когда-то включили для «удобства», да так и оставили; аутентификация по словарным паролям; сетевое оборудование с дефолтными настройками; неправильно настроенные веб-сервисы вкупе с отсутствием сегментации внутренней сети и плохим управлением привилегиями — всё это даёт злоумышленнику простор для творчества. Более того, более 70% всех атак в финансовой сфере нацелены именно на инфраструктуру[5] организаций. В ходе анализа защищённости в прошлом году выявлялось в среднем не менее двух векторов проникновения во внутреннюю сеть конкретной организации[6], максимальное число обнаруженных векторов — 10, а возраст самой старой выявленной уязвимости около 18 лет. Надо понимать, что злоумышленнику зачастую достаточно всего лишь

одной уязвимости, позволяющей преодолеть сетевой периметр и впоследствии получить контроль над инфраструктурой. В частности, по нашей статистике в 68% случаев внешний злоумышленник может преодолеть сетевой периметр, а получить полный контроль над локальной вычислительной сетью от имени внутреннего злоумышленника можно в 100% случаев.

Небезопасная информационная безопасность. Наше исследование показало, что современные подходы к защите характерны для финансовых организаций из топ-10 (по выделяемому бюджету), в остальных банках ситуация менее позитивна[7]. Так средства защиты веб-приложений применяют около 70% банков из топ-10 по ИБ-бюджету и 13% среди остальных; собственные SOC имеют все банки из нашего топ-10 и только 40% — среди остальных; SIEM-системы применяют 65% финансовых компаний (среди банков из топ-10 по бюджету на ИБ этот показатель 100%). Но даже если системы защиты установлены и развёрнуты, может быть неправильно настроена политика сбора и хранения логов, а их мониторингом никто не занимается. Не всегда уделяют должное внимание и разграничению прав пользователей. Если пользователь работает под администраторской учётной записью, вредоносному ПО легче обосноваться на его ПК в случае «пробоя» средств защиты. Если в организации нет разделения доступа

пользователей к сетевым ресурсам в зависимости от их бизнес-ролей, злоумышленнику легче получить доступ к критичным данным. Бывает, что в организации не ведётся работа по выявлению и устранению известных уязвимостей в ПО и ОС (у 25 % опрошенных нами банков нет контроля установки обновлений ПО, а 8% в принципе не отслеживают информацию о новых уязвимостях). В итоге инфраструктура может стать добычей хакера, вооружённого эксплоитами десятилетней давности.

Партнёр с «сюрпризом». Не всегда кибербезопасность организации зависит от самой организации. Например, в ходе работ мы часто встречаем атаки типа «supply chain», когда взламывают не саму организацию, а её поставщиков и контрагентов, для того чтобы использовать их инфраструктуру и реальные учётные записи для развития атак. Эта тактика уже использовалась злоумышленниками, когда через инфраструктуру компании M. E. Doc распространялся вирус NotPetya[8]. Этот подход часто использует группировка Cobalt: один из последних ярких примеров — громкая атака на банк «Юнистрим», которая обернулась фишинговой рассылкой от его имени[9] другим кредитным организациям. В среднем каждая вторая успешная атака, которую расследовал экспертный центр безопасности компании Positive Technologies, была проведена через скомпрометированный «ранее надёжный» источник. Также внимания заслуживает VPN, особенно site-to-site — если у вас в инфраструктуре всё хорошо, это не означает, что и у ваших партнёров тоже.

Планомерная работа по устранению недостатков в каждом из направлений построения ИБ увеличивает эффективность системы в целом

ТЕХНОЛОГИЧЕСКИЕ ИНСТРУМЕНТЫ

Злоумышленник не сможет достичь своей цели, если атака будет вовремя выявлена и остановлена. Это возможно на любом её этапе, если применяются соответствующие меры защиты. Например, системы выявления вредоносного ПО (типа PT MultiScanner) способны обнаружить и заблокировать фишинговые письма, средства анализа трафика (типа PT Network Attack Discovery) позволяют выявить атаку прямо в трафике. Выявить активность злоумышленника во внутренней сети (например, попытки горизонтального перемещения внутри инфраструктуры) в минимальные сроки также можно благодаря анализу трафика. А использование нестандартных портов, попытки эксплуатации уязвимостей или манипуляции с банкоматами на компьютере банковского специалиста во время его отсутствия зафиксирует система класса SIEM.

Однако система ИБ требует и уникальной экспертизы в области форензики и реагирования на инциденты, тактик и техник злоумышленников. Мало выявить и заблокировать вредоносное ПО, важно понять, что именно выявлено и каков был вектор заражения. Нужно выявить в потоке событий признаки, характерные для злоумышленников. На

практике расследование инцидентов дополнительно осложняется тем, что злоумышленники для своих действий часто применяют штатные утилиты операционных систем, стараются действовать без сохранения файлов на диск, используют методы шифрования и стеганографии и пр.

РАССЛЕДОВАНИЕ ДО... ТОЧКИ

Инцидент — это почти всегда сочетание нескольких факторов. Поэтому планомерная работа по устранению недостатков в каждом из направлений построения ИБ увеличивает эффективность системы в целом. Всегда остаётся шанс, что злоумышленник использует уязвимости нулевого дня, но даже в этом случае грамотная система ИБ позволит быстрее выявить круг затронутых активов, провести локализацию и восстановление. При этом колоссальное значение имеет именно качественно проведённое расследование по итогам любого инцидента: необходимо анализировать всю инфраструктуру, а не только явно затронутые киберпреступниками сегменты, выявлять векторы проникновения, полную цепочку действий преступника. Это исключит возможность дальнейшего присутствия киберпреступника в инфраструктуре и существенно усложнит последующие попытки атак.

ЛИТЕРАТУРА

1. «Кибербезопасность — 2018–2019: итоги и прогнозы», Positive Technologies, декабрь 2018 г.
2. «Как социальная инженерия открывает хакеру двери в вашу организацию», Positive Technologies, март 2018 г.
3. «Cobalt strikes back: новые атаки на финансовые организации», Positive Technologies, август 2017 г.
4. «Кибербезопасность — 2018–2019: итоги и прогнозы», Positive Technologies, декабрь 2018 г.
5. «Актуальные киберугрозы. III квартал 2018 года», Positive Technologies, январь 2019 г.
6. «Уязвимости корпоративных информационных систем», Positive Technologies, май 2018 г.
7. «Сколько стоит безопасность», Positive Technologies, декабрь 2017 г.
8. «Все, что вы хотели узнать о NotPetya, но боялись спросить», Positive Technologies, июнь 2017 г.
9. «Юнистрим» позвонил дважды, Коммерсантъ, 23.11.2018 г.

ИССЛЕДОВАНИЯ ЗАЩИЩЁННОСТИ ПО 382-П



Сергей НЕЙГЕР
сотрудник компании
«Перспективный
мониторинг»

КАКИЕ МОГУТ БЫТЬ СЛОЖНОСТИ С ПЕНТЕСТОМ?

С августа по декабрь 2018 года «Перспективный мониторинг» подвергся массовой атаке. Но не со стороны злобных киберпреступников, а со стороны добросовестных «безопасников». ПМ получил множество подозрительно похожих запросов на услуги. «Сделайте нам пентест!», «Хотим социальную инженерию!». Работали по всем каналам — сайт, мероприятия, личные контакты, рекомендации. Совпадение? Не думаем.

ПЕНТЕСТЫ ЕЖЕГОДНО!

В финансовой сфере особенно тщательно следят за нормативной базой, поэтому изменения в Положении «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» № 382-П в части регулярного проведения тестов на проникновение и анализа уязвимостей не прошли незамеченными: согласно новой редакции документа их надо проводить ежегодно.

ТИПИЧНЫЕ УСЛУГИ

Когда мы проанализировали желания потенциальных заказчиков, мы смогли выявить четыре «типичные» для таких запросов услуги: тестирова-

ние на проникновение сайта финансовой организации, пентест внешнего периметра, проверка мобильного приложения и проверка осведомлённости сотрудников в области информационной безопасности.

Кажется, какие могут быть сложности с пентестом сайта? Вот вам решение, ломайте! В одном проекте конца 2018 года «пентестом сайта» оказалось тестирование семи поддоменов с абсолютно разными веб-приложениями, которые разрабатывали разные команды в разное время, каждое со своим бекэндом. К этому также добавляется тестирование в различных режимах — black-box и gray-box. Делать пентест без предоставления учётной записи часто не имеет смысла: злоумышленники могут стать клиентами или «утнать учётку» клиента и использовать её для реальной атаки на информационные системы. Обычно в таких исследованиях мы проверяем оборудование платформы web-сервиса, операционные системы, вспомогательное ПО, архитектуру web-сервиса, сетевые сервисы и службы.

С одной стороны, в 382-П есть требование проверять всё программное обеспечение, с которым будет взаимодействовать клиент финансовой организации для осуществления переводов денежных средств. С другой стороны, мобильное приложение — это такой же клиент для ДБО, как и связка

«браузер + веб-приложение». Поэтому игнорировать тестирование банковского приложения, проведя пентест сайта — это как оставить открытой форточку, запирая дверь на все замки.

ПОМОЖЕМ ПРОВЕРИТЬ

Думаете, что старая шутка про «тяп-ляп и в продакшен!» точно не про вас? Мы поможем вам проверить, так ли это на самом деле, и дадим непредвзятую оценку уровня безопасности приложения, независимо от того, разработала его сама финансовая организация или аутсорсер.

Типовой состав услуги: анализ защищённости ПО для Android и iOS, исследование защищённости канала передачи данных и серверной части мобильных приложений. Заказчик предоставляет нам исходный код и скомпилированное приложение, которое нужно проанализировать. Мы проводим статический и динамический анализ кода, следим за доступом приложения к файловой системе, памяти устройства и ресурсам ОС. Если нужно — сделаем реверс-инжиниринг приложения (это если мы с заказчиком совсем по-честному моделируем действия злоумышленников и имеем доступ только к бинарным установочным файлам без исходного кода).

После этого найденные уязвимости классифицируются и ранжируются по степени критичности, разрабатываются рекомендации по повышению уровня защищённости приложений.

ЧЕЛОВЕЧЕСКИЙ ФАКТОР

Если спрос на пентесты веба и приложений относительно стабилен, то увеличение числа запросов на оценку осве-

Игнорировать тестирование банковского приложения, проведя пентест сайта — это как оставить открытой форточку, запирая дверь на все замки

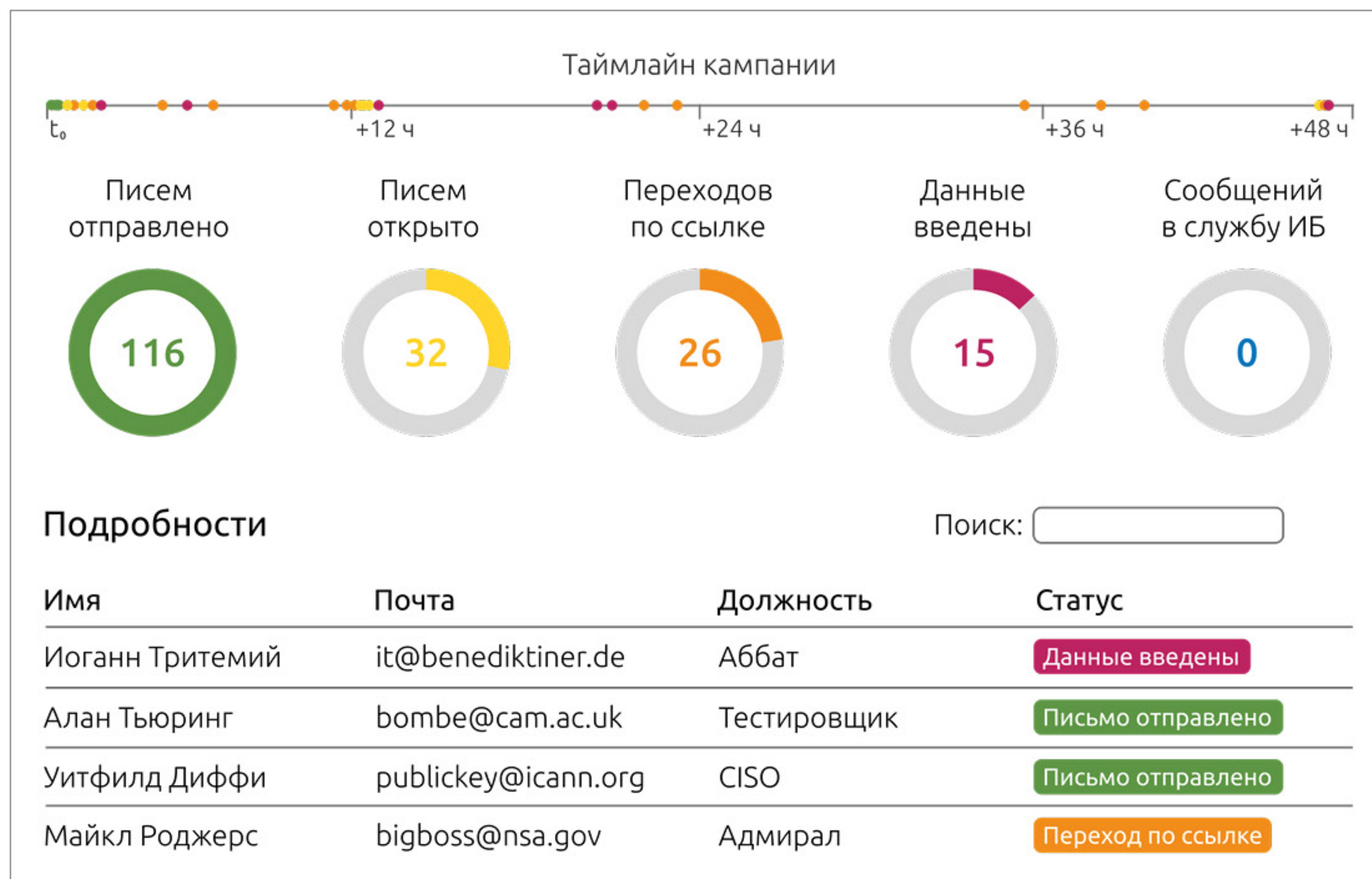


Рисунок 1

домлённости пользователей в вопросах ИБ удачно и приятно совпало с открытием в «Перспективном мониторинге» отдельного направления Open Source Intelligence (OSINT).

«Человеческий фактор» — одна из самых распространённых угроз информационной безопасности. Злоумышленники успешно пользуются любопытством, жадностью и желанием развлечься обычных пользователей. Чтобы снизить риски эксплуатации человеческих ошибок применяются технические и административные методы защиты. Один из таких методов — повышение осведомлённости в области ИБ.

При проведении атак на организацию с применением методов социальной инженерии наши специалисты по OSINT собирают информацию из общедоступных источников: о сотрудниках, руководстве, организационной структуре, продуктах, заказчиках и партнёрах. Параллельно с этим готовятся очень похожие на настоящие сайты и вложения в сообщения и разрабатывается правдоподобная «леген-

да» атаки. Например, перед Новым годом сотрудники отлично открывали письма с конкурсами и обещаниями подарков от руководства тестируемых компаний.

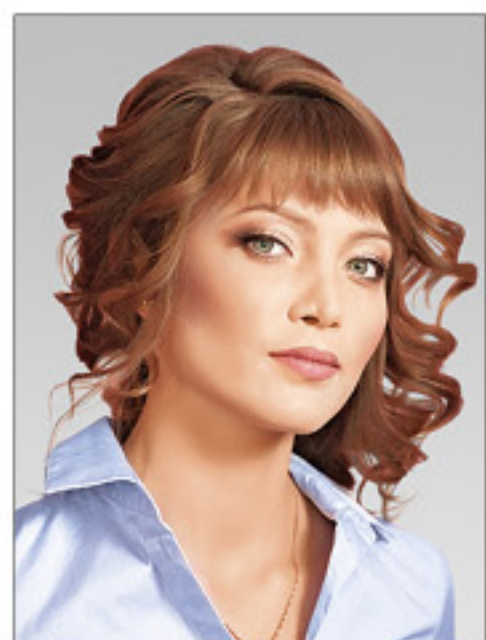
СТО ПРОЦЕНТОВ!

После проведения рассылки вся статистика по открытию писем и переходам по фишинговым ссылкам доступна в наглядном дашборде (Рисунок 1). Заказчик узнаёт, кто и когда «попался» и к каким негативным последствиям это могло бы привести. Отчёт об исследовании содержит описание методов социальной инженерии, которые использовались во время проверки, оценку возможности проникнуть в информационную систему организации и рекомендации по повышению уровня защищённости.

В тех проектах, где мы использовали методы социальной инженерии, удалось добиться отличного результата — 100 из 100. В каждой проведённой атаке были скомпрометированы логины и пароли сотрудников или произошло за-

ражение «вредоносным» программным обеспечением (в наших атаках мы используем эксплойты на реальные уязвимости, но без «нагрузки», которая могла бы причинить вред информационным системам). Иногда сотрудники сообщали в службу ИБ о фишинговых письмах, но гораздо чаще начинали ждать несуществующих подарков после авторизации на сайте-опроснике. Задача пентестера — найти слабые места в защите, а не повод кого-нибудь показательно уволить. К счастью, наши заказчики это понимают и признают, что «ну да... скорее всего кто-то кликнет».

Само тестирование на проникновение можно очень условно назвать «защитной мерой». Пентест показывает направления, по которым следует развивать организационные и технические меры защиты. Но лучше знать куда двигаться, чем бродить по кругу.



Александра БЯЛЬКИНА
руководитель департамента
развития продуктов, Cross Solutions
(АО «Кросс Технолоджис»)

СУДЬБА ОФИЦЕРА ИБ

ПОЧЕМУ ОН ЛОВИТ ТОЛЬКО ТЕХ ВНУТРЕННИХ НАРУШИТЕЛЕЙ, КОТОРЫХ УДОБНО ЛОВИТЬ?

Данных, в том числе конфиденциального содержания, становится всё больше. Исследования IDC за 2018 год показывают, что прирост объёма хранимой в электронном виде информации составляет около 40% в год. При этом нет определённости относительно инструментов обеспечения безопасности, применяемой методологии и способов фактической реализации требований, которые могут зависеть от дополнительных факторов.

МИНИМИЗАЦИЯ РИСКОВ

Есть множество способов контроля за утечками информации и их предотвращения, в том числе применение решений класса DLP в качестве инструмента активного или пассивного воздействия на попытки вывода информации по цифровым каналам. Чаще других фиксируются утечки чувствительных данных по электронной почте, через Интернет-порталы и социальные сети, а также попытки несанкционированного копирования материалов в электронном виде на съёмные носители и пр. Таким способом защищается корпоративная информация в виде документов, предотвращается передача баз данных и архивов информации с персональ-

ми данными, реквизитами банковских карт, исходными кодами программных продуктов, уникальной рецептурой, конструкторской документацией и пр.

Чтобы минимизировать риски утечек данных, офицерам ИБ в организациях приходится решать сложные организационные и технические задачи, которые регулярно включают в себя следующие три пункта:

1. Классификация чувствительной информации в компании. Нужно понимать, какие данные имеются в компании и что из них следует защищать.
2. Разграничение доступа к чувствительным данным. Нужно понимать, где они хранятся, кто и с помощью чего с ними работает.
3. Актуализация модели угроз и построение списка каналов утечки информации. Нужно понимать и контролировать современные каналы утечки данных, например, фотографирование документов на мобильные телефоны с последующей передачей в открытую сеть через сервисы обмена мгновенными сообщениями.

Первые две задачи покрываются DLP-системами посредством контентного анализа используемых сотрудниками файлов. В таком подходе требуется время на обучение системы и

минимизацию ложных срабатываний. Совместно с DLP-системами для этого могут применяться системы типа Data Classification, которые за пределами нашей страны являются распространёнными, но нечасто используются в России.

На практике выделяют два подхода к классификации чувствительной информации:

1. автоматизированная классификация (автоматическое сканирование и анализ контента информации) на основе правил, включая текст, регулярные выражения и пр. Чаще всего это функция реализована в решениях класса DLP.
2. ручная классификация (обучение сотрудников основам работы с чувствительной информацией с предложением самостоятельно по предварительно согласованной инструкции категоризировать созданные ими и/или обработанные/отредактированные электронные документы на основе понятных правил) (Data Classification).

МАРКИРОВАНИЕ: КАК И ЗАЧЕМ

Остановимся подробнее на втором типе систем и рассмотрим его на примере платформы маркирования и классификации электронных документов Docs Security Suite (далее — DSS).

Система DSS предлагает сотруднику каждый раз после завершения работы с электронным документом присвоить ему определённую категорию: «Персональные данные», «Банковская тайна», «Для служебного пользования», «Конфиденциально», «Коммерческая тай-

Не знаешь, какая информация у тебя имеется, — не знаешь, насколько эффективно (достаточно, но не избыточно) ты её защищаешь

на» и т.д. Выбор отразится в структуре документа, а в скрытой части автоматически проставятся метки конфиденциальности из заранее настроенного списка меток.

Таким образом достигаются и обеспечиваются следующие параметры безопасности электронного документа, как объекта защиты:

1. принудительное маркирование документа непосредственным автором или редактором документа;
2. учёт техническими средствами электронных документов в организации, содержащих чувствительные данные;
3. экспертная классификация электронных документов по установленным в организации критериям на этапе создания документа;
4. разграничение доступа пользователей к документам с различными метками конфиденциальности;
5. учёт и регистрация действий пользователей внутри организации с электронными документами, содержащими метки;
6. формирование древа родительских и дочерних электронных документов;
7. создание режима и повышение культуры информационной безопасности работников организации, обрабатывающих конфиденциальную информацию.

Интеграция систем Data Classification с DLP ручной классификацией позволяет избежать ошибок первого рода, получаемых при автоматизированном сканировании и контентном анализе документов, а также даёт возможность компании «вступить в диалог» с сотрудником о важности данных, которые он использует или создаёт. По каждому документу собирается полная информация: кто, когда использовал его, какие операции производил. И на выходе — доказательная база для расследования инцидентов ИБ, которая в том числе обеспечивает снижение стоимости расследования за счёт сокращения не только количества самих инцидентов, но и времени, требуемого для проведения процесса расследования.

МАРКИРОВАНИЕ: ПРАКТИЧЕСКАЯ ПОЛЬЗА

Первая задача, которую они позволяют решить — это обучение сотрудников работе с информацией разных



Рисунок 1.

Иллюстрация возможностей DSS по простановке визуальной (видимой) метки на отредактированном пользователем документе

категорий, вовлечение их в процесс работы с документами, разделение ответственности компании с сотрудником за сохранность данных, неразглашение информации о нём в открытых источниках. Это помогает снизить количество инцидентов, в том числе совершаемых «по незнанию». Вторая важная задача — проведение максимально оперативного расследования инцидентов. В половине случаев утечки происходят по вине внутренних нарушителей. Их действия по объёму ущерба сопоставимы с деятельностью внешних злоумышленников.

Помочь в решении этой проблемы может аудит действий сотрудников с документами компании как возможность обогащения информацией DLP. Метка, которая установлена сотрудником, позволяет однозначно подсказать DLP необходимые действия по предотвращению инцидента или уведомлению о нём ответственного сотрудника. Однако злоумышленники всё реже используют заведомо контролируемые каналы передачи информации — электронную почту, копирование на USB и пр. Мобильные телефоны, с помощью которых можно сделать фото и/или передать через мессенджер личную информацию, — всё чаще. И здесь на помощь придёт

кодирование дополнительной информации в тексте документа.

Предлагаемый в Docs Security Suite механизм или уникализации — использование стеганографических методов кодирования информации путём манипуляций с текстом редактируемого документа.

При открытии документа в соответствии с алгоритмом кодирования изменяются параметры текста у всего электронного документа, возникает дополнительная цифровая скрытая метка. Она дополняет основную метку (например, «Банковская тайна»), и обладает следующими свойствами:

- ♦ динамически изменяется каждый раз при открытии документа;
 - ♦ содержит имя пользователя или рабочей станции, с которой обрабатывается электронный документ, дату, время или идентификатор сессии, связанный с именем пользователя.
- Плюсы применения уникализации:
- ♦ факт содержания скрытой метки не виден обычному пользователю;
 - ♦ сессия работы с документом обладает уникальным идентификатором;
 - ♦ уникализация является свойством метки, которое применяется автоматически;
 - ♦ формируется доказательная база от случаев утечки информации в том чис-



Рисунок 2.
Иллюстрация возможностей DSS по уникализации электронного документа, содержащего метку конфиденциальности

ле по некорпоративным неконтролируемым каналам, таким как мобильные телефоны.

Как использовать этот механизм при расследовании инцидентов? Ввиду того, что алгоритм уникализации является прозрачным для сотрудника службы ИБ при обучении работе с системой Docs Security Suite, мы можем как использовать автоматизированные средства сопоставления «утекшего» документа с оригиналом, так и вычислить уникальный идентификатор вручную (при понимании алгоритма кодирования и декодирования скрытой информации). И ручной механизм зачастую бывает

единственно возможным в случае наличия некачественной фотокопии документа (угол поворота, освещение в помещении при фотографировании, качество камеры и пр.).

ЗАКЛЮЧЕНИЕ

Таким образом, для обеспечения комплексной защиты электронных документов следует в процессе внедрения организационных и технических аспектов режима информационной безопасности учесть следующие вехи:

1. Разработать внутренние положения организации по работе с электронными документами и их маркированию

с указанием ответственности за нарушение установленных правил;

2. Вовлечь сотрудников в процесс маркирования и классификации документов;

3. Провести для них обучение по использованию инструментов маркирования;

4. Внести в должностные инструкции сотрудников обязанность по маркированию документов и ответственность за корректность проведённых операций;

5. Периодически проводить аудит промаркированных документов для выявления некорректных меток;

6. При необходимости использовать механизм разграничения прав доступа ИРМ или шифрования на основе меток конфиденциальности;

7. Помимо типовых средств контроля и борьбы с утечками использовать дополнительные для расследования утечек через создание фотографий.

* * *

Эти меры нацелены на оптимизацию процесса управления инцидентами информационной безопасности в компании, и, последовательно применённые, позволят выявлять утечки не только тех нарушителей, которых «удобно» ловить, но тех, чьи деструктивные или несанкционированные действия до настоящего времени остаются незамеченными! Решение DSS способно снизить трудозатраты офицеров ИБ и упростить менеджмент инцидентов ИБ.



Алексей ПЛЕШКОВ
независимый
эксперт по ИБ

BIS-КОММЕНТАРИЙ

Конец 2018 года наглядно продемонстрировал, что персональные данные и банковская тайна даже самых защищённых финансовых организаций коварно и регулярно перетекают от владельцев в хранилища злоумышленников. Объявления об их продаже есть не только на чёрном рынке, но доступны даже в поисковиках. Основные причины утечек чувствительных данных сегодня связаны с нарушениями со стороны лиц, имеющих к ним доступ. А потому такие меры, как маркирование документов, учёт, контроль и ограничение доступа к информации, а также своевременное выявление и расследование связанных инцидентов — выходят на первый план. При больших объёмах обрабатываемых документов применять средства ручного контроля и визуальной фильтрации не эффективно, однако для многих офицеров информационной безопасности это остаётся единственным возможным способом, в условиях ограниченного финансирования и кадровой неуккомплектованности подразделений.

Docs Security Suite

платформа управления, контроля
и аудита прав доступа к электронным документам
на основе меток конфиденциальности

МЫ ПРЕДЛАГАЕМ:

- ✓ Настройка меток конфиденциальности и маркирование документов
- ✓ Разграничение для пользователей доступа к конфиденциальным документам компании в соответствии с должностными обязанностями
- ✓ Шифрование критичных документов компании
- ✓ Автоматическая классификация документов на общих файловых хранилищах
- ✓ Фиксация действий пользователей с конфиденциальными документами компании
- ✓ Уникализация документов компании
- ✓ Уникализация сессий работы сотрудников с документами компании

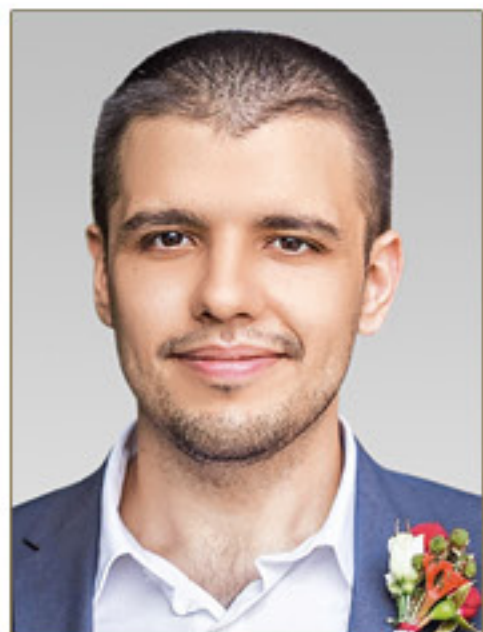
МЫ РЕШАЕМ:

- ✓ Повышение эффективности систем контроля за утечками информации (DLP)
- ✓ Выявление нарушителей в компании
- ✓ Защита от бесконтрольной утечки информации, фотографируемой на личные устройства пользователей

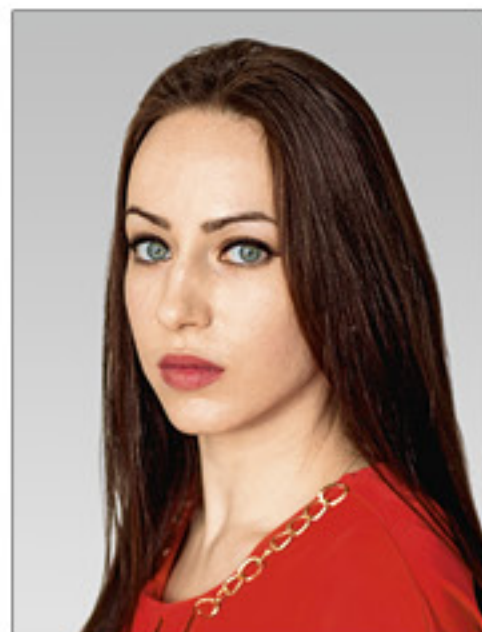


Cross Solutions

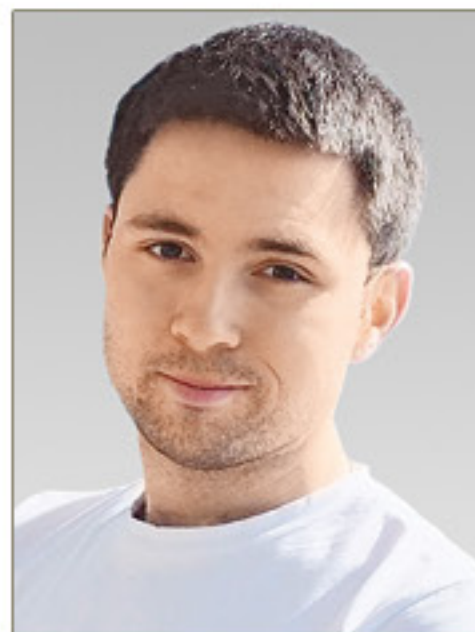
+7 (495) 741-88-64
www.cross-solution.ru



Сергей АГАФИН
начальник отдела
ООО «КРИПТО-ПРО»



Татьяна ЛАРИНА
инженер-аналитик
ООО «КРИПТО-ПРО»



Станислав СМЫШЛЯЕВ
директор по ИБ
ООО «КРИПТО-ПРО»,
к. ф. - м. н.



Алексей ЮДИН
директор направления
ПАО «Ростелеком»

ЕБС: ОТ ОБЩИХ ТРЕБОВАНИЙ К КОНКРЕТНЫМ РЕШЕНИЯМ

Несмотря на развитие информационных технологий, человеку до сих пор нужно лично прийти в отделение банка, чтобы стать его клиентом. Это обременительно для обеих сторон. С появлением Единой биометрической системы (ЕБС) — «Ключа Ростелеком» — пользователю достаточно зарегистрироваться один раз, после чего можно удалённо получать услуги в любом банке, работающем с ЕБС.

При регистрации биометрических данных пользователя происходит контроль качества предоставленных данных и обеспечивается их безопасное хранение. ЕБС осуществляет удалённую идентификацию и аутентификацию пользователя. Обычно этот двоякий процесс в документах по ЕБС принято называть просто «удалённая идентификация». В дальнейшем мы будем использовать именно этот термин в статье. При идентификации ЕБС определяет степень соответствия полученных биометрических данных эталону, созданному при регистрации.

ПРАВОВАЯ БАЗА

В соответствии с положениями № 115-ФЗ от 07.08.2001, введёнными № 482-ФЗ от 31.12.2017:

- ♦ банки обязаны при личном присутствии клиента и с его согласия размещать биометрические персональные данные в ЕБС;
- ♦ банки вправе предоставлять услуги без личного присутствия клиента после

его успешной удалённой идентификации с использованием ЕБС.

Процессы регистрации и удалённой идентификации регламентируются статьёй 14.1 № 149-ФЗ от 27.07.2006, введённой № 482-ФЗ. Банки должны обеспечить и защиту от угроз безопасности, предписанную Указанием Банка России и ПАО «Ростелеком» № 4859-У/01/01/782-18 от 09.07.2018.

В соответствии с информационным письмом № ИН-03-13/40 Банка России от 28.06.2018, все подразделения банков должны выполнить указанные требования до конца 2019 года.

РЕГИСТРАЦИЯ БИОМЕТРИИ И ТРЕБУЕМЫЕ КЛАССЫ ЗАЩИТЫ

При регистрации создаётся эталонный образец биометрических данных. При удалённой идентификации предоставляемые пользователем биометрические данные сравниваются именно с этим эталонным образцом.

Если при регистрации в ЕБС у клиента отсутствует учётная запись в Единой системе идентификации и аутентификации (ЕСИА) или она не подтверждена, оператор поможет в регистрации и подтверждении. Далее сотрудник банка записывает биометрические данные — голос и фотографию. Банк передаёт эти данные в защищённом виде в головной офис банка. При этом биометрия заверяется сотрудником и отправляется по защищённому каналу с использовани-

ем средств криптографической защиты информации (СКЗИ) класса КСЗ. Все действия оператора фиксируются согласно Постановлению Правительства РФ № 747 от 29.06.2018.

В головном офисе банка биометрические данные проходят проверку на соответствие требованиям, установленным Приказом Минкомсвязи от 25.06.2018 № 321. В случае успешного прохождения контроля качества пользовательская информация подписывается усиленной квалифицированной электронной подписью (ЭП) банка и направляется в ЕБС через систему межведомственного электронного взаимодействия (СМЭВ). На стороне ЕБС биометрические данные также проходят контроль качества, и в случае успеха на их основе формируется биометрический контрольный эталон пользователя.

Согласно упомянутому Указанию Банка России, биометрические данные пользователя должны передаваться банком по защищённому каналу, их защита от угрозы нарушения конфиденциальности осуществляется с использованием СКЗИ класса КСЗ.

Неизменность передаваемых данных подтверждается банком с помощью усиленной квалифицированной ЭП. Для этого банки должны использовать HSM, сертифицированный ФСБ России по классу КВ2/КВ. Если банковские системы будут взаимодействовать с данным HSM напрямую, то необходимо проводить процедуру оценки

влияния данных систем на HSM в соответствии с ПКЗ-2005. Подобные процедуры связаны со значительными денежными и временными затратами.

Отсюда возникает потребность в создании унифицированного решения, которое будет осуществлять всё необходимое взаимодействие с СКЗИ и предоставлять банковским системам упрощённый интерфейс, изолируя HSM от банковской инфраструктуры. Тогда будет достаточно проведения исследований только данного решения, это упростит банкам процесс интеграции.

УДАЛЁННАЯ ИДЕНТИФИКАЦИЯ И ТРЕБУЕМЫЕ КЛАССЫ ЗАЩИТЫ

В результате удалённой идентификации банк получает персональные данные пользователя (ПДн) и информацию о степени соответствия предъявленных биометрических данных эталонным. На основе полученной информации о пользователе банк принимает решение о предоставлении запрашиваемой услуги.

Удалённая идентификация состоит из трёх этапов.

1. Получение банком в ЕСИА маркера доступа, позволяющего начать идентификацию пользователя в ЕБС (при условии успешной аутентификации пользователя в ЕСИА).

2. Получение банком в ЕСИА маркера доступа, позволяющего банку запросить ПДн пользователя и информацию о степени соответствия его биометрии (при условии успешного подтверждения личности пользователя в ЕБС).

3. Получение банком в ЕСИА и ЕБС ПДн пользователя и информации о степени соответствия его биометрии (при предъявлении маркера доступа, полученного на II этапе).

Приведённая Схема 1 иллюстрирует взаимодействие участников протокола удалённой идентификации.

Согласно № 4859-У, ПДн пользователя и информация о степени соответствия должна передаваться в банк по защищённому каналу с использованием СКЗИ класса КСЗ. Для обеспечения защиты от подмены или удаления информации о степени соответствия биометрии пользователя банк должен про-

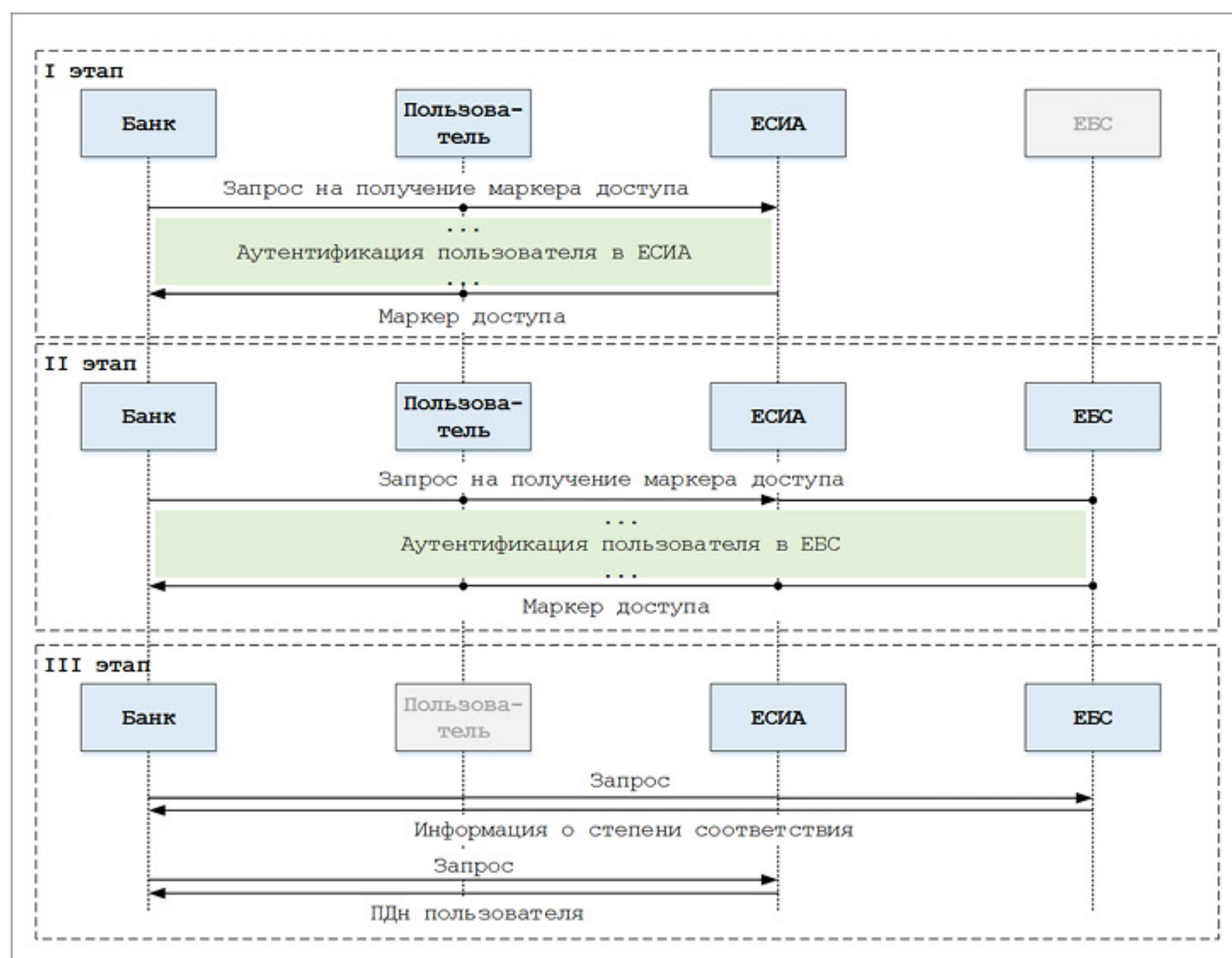


Схема 1. Взаимодействие участников протокола удалённой идентификации

верить подпись данной информации с использованием СКЗИ класса КВ2/КВ.

Запросы банка на получение маркеров доступа должны быть подписаны ЭП. В дополнение к защищённому соединению между банком и ЕСИА это позволяет защитить банк от злоумышленников, выполняющих действия от его имени.

Между банком и устройством пользователя устанавливается защищённое соединение с аутентификацией банка, например, с помощью протокола TLS в соответствии с методическими рекомендациями ТК 26 МР «Использование наборов алгоритмов шифрования на основе ГОСТ 28147–89 для протокола безопасности транспортного уровня (TLS)». На стороне банка для этого используется СКЗИ класса КСЗ, а на стороне пользователя — СКЗИ класса КС1. На персональном компьютере этим средством может быть «Крипто-Про CSP», используемый совместно со стандартными браузерами ОС Windows (IE, Edge), «Яндекс.Браузер» или «Спутник Браузер»; на мобильном устройстве — приложение Ростелекома «Ключ — удалённая идентификация». В первом случае пользователь может отказаться от использования СКЗИ и продолжить процесс удалённой иден-

тификации, принимая возможные риски. Во втором случае без СКЗИ работать нельзя.

ТИПОВОЕ РЕШЕНИЕ ПО ИБ ДЛЯ БАНКОВ

При работе с ЕБС банкам нужно использовать СКЗИ, сертифицированные ФСБ России по соответствующим классам защиты.

Для встраивания HSM, сертифицированного по классу КВ2/КВ, банку нужно использовать дополнительное ПО, которое будет взаимодействовать с HSM. При этом разработчику данного ПО необходимо:

- ♦ Согласовать с ФСБ России техническое задание на разработку ПО.

- ♦ Провести оценку влияния разрабатываемого ПО на выполнение требований, предъявляемых к HSM.

Процесс выглядит так: сначала выбирается испытательная лаборатория, с ней и с ФСБ согласуется техническое задание на проведение работ по оценке влияния. Затем проводится исследование, и его результаты направляются лабораторией на экспертизу в ФСБ. Процесс завершается при получении положительного заключения ФСБ России.

Это требует большого количества временных и денежных ресурсов. Для

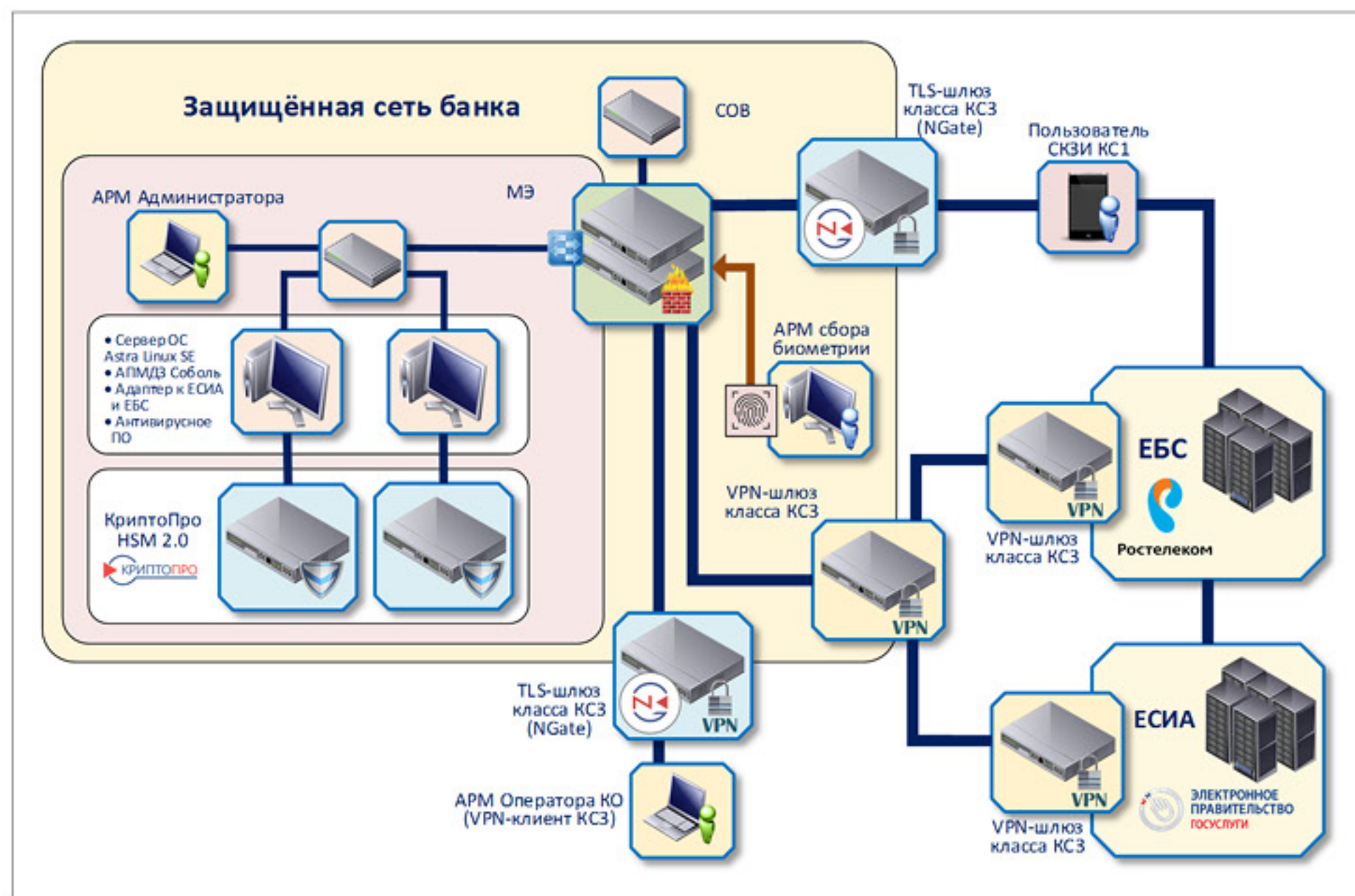


Схема 2. Архитектура типового решения

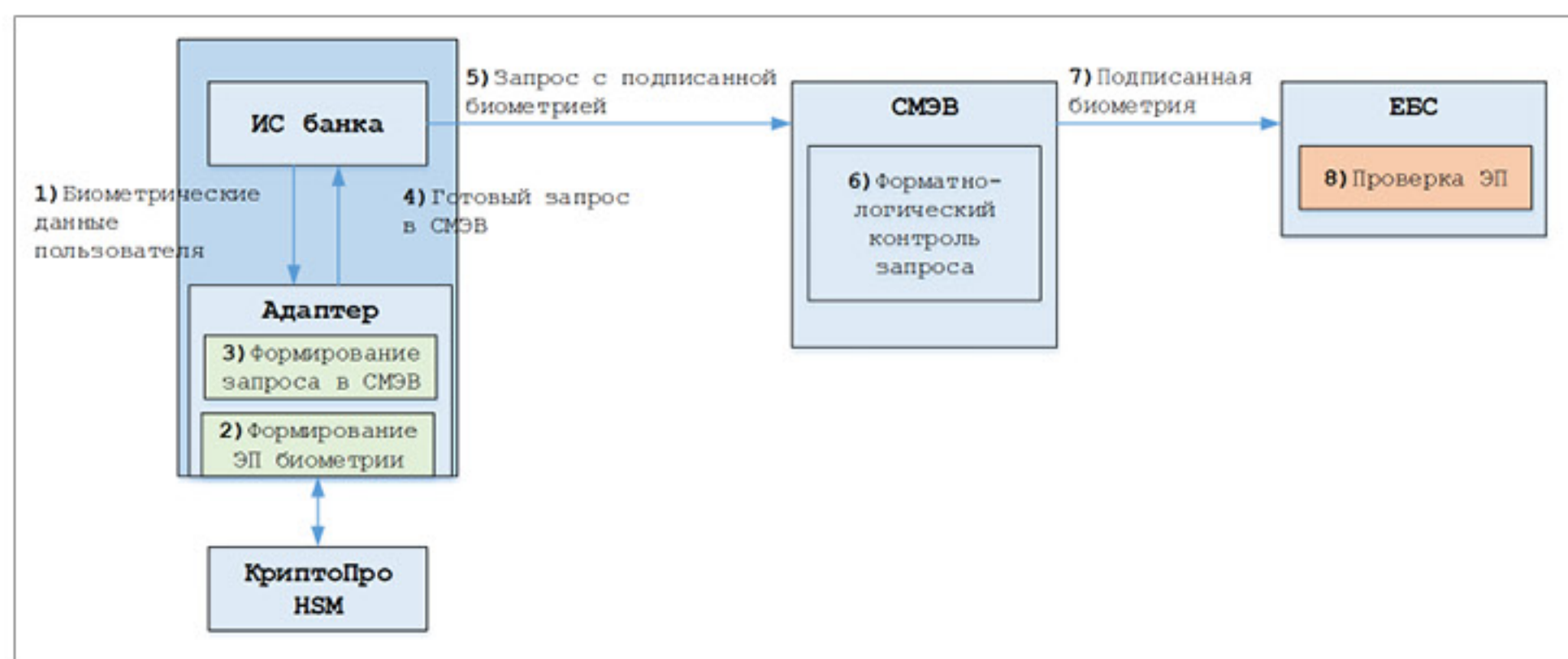


Схема 3. Адаптер к ЕСИА и ЕБС

снижения расходов банков ПАО «Ростелеком» совместно с ООО «КРИПТОПРО» было разработано типовое решение. Его архитектура представлена на Схеме 2.

Решение включает следующие аппаратные и программные компоненты:

- ♦ программно-аппаратный криптографический модуль «КриптоПро HSM» версии 2.0 (класса KB2/KB);
- ♦ сервер с ОС Astra Linux Special Edition;
- ♦ межсетевой экран;
- ♦ средство обнаружения вторжений;
- ♦ TLS-шлюз с поддержкой ГОСТ (класса КСЗ);
- ♦ антивирусное ПО;
- ♦ аппаратно-программный модуль доверенной загрузки «Соболь»;
- ♦ адаптер к ЕСИА и ЕБС — ПО, формирующее запросы в ЕБС через СМЭВ

при регистрации биометрии и осуществляющее необходимое взаимодействие с ЕСИА и ЕБС при удалённой идентификации пользователя.

Для формирования и проверки ЭП при регистрации биометрии и при удалённой идентификации адаптер к ЕСИА и ЕБС использует «КриптоПро HSM».

Регистрируя биометрию, адаптер принимает на вход данные, отправляет их на подпись в «КриптоПро HSM», в результате чего создаётся пакет, содержащий подписанную биометрию для направления в ЕБС (Схема 3).

При поступлении в адаптер запроса на удалённую идентификацию запускается процесс по конкретному пользователю. В случае успешного завершения процесса адаптер возвращает банку ПДн пользователя и информа-

цию о степени соответствия его биометрии от ЕБС. В ходе процесса адаптер взаимодействует с устройством пользователя, а также с ЕСИА и ЕБС, осуществляет формирование подписанных запросов в ЕСИА и проверку подписи полученных из ЕБС данных.

Адаптер совместно с дополнительными средствами защиты (АПМДЗ «Соболь», антивирусное ПО) устанавливается на сервер с ОС Astra Linux SE. Сегмент сети банка, в котором размещается адаптер совместно с «КриптоПро HSM», должен быть защищён сертифицированным межсетевым экраном и отделён от остальной информационной инфраструктуры банка.

Адаптер в составе с «КриптоПро HSM» может обеспечивать горячее резервирование и балансировку нагрузки. Для этого могут использоваться уже имеющиеся средства балансировки нагрузки, либо дополнительные, например, HAProxy.

Защищённое соединение с устройством пользователя обеспечивается TLS-шлюзом «КриптоПро NGate» класса КСЗ.

Типовое решение реализует следующие функции, необходимые для выполнения банками требований по ИБ:

- ♦ формирование подписи биометрических данных пользователя с использованием СКЗИ класса KB2/KB при их передаче от банка в ЕБС;
- ♦ установление TLS-соединения с устройством пользователя с использованием СКЗИ класса КСЗ;
- ♦ формирование подписи запросов в ЕСИА на получение маркеров доступа;
- ♦ проверка подписи информации о степени соответствия биометрических данных пользователя, поступающей от ЕБС, с использованием СКЗИ класса KB2/KB.

Получение положительного заключения ФСБ России на описанное типовое решение ожидается весной 2019 года. Это решение упрощает подключение к ЕБС за счёт предоставления простых интерфейсов и избавляет банки от необходимости проведения ресурсоёмких оценок влияния.



Иван БИРУЛЯ
директор по безопасности
компании «СёрчИнформ»

«СЕРЕБРЯНЫХ ПУЛЬ» НЕ ОСТАЛОСЬ

ВСЕ ИНСТРУМЕНТЫ В БЕЗОПАСНОСТИ УЖЕ ИЗОБРЕТЕНЫ

В банковской сфере складывается местами парадоксальная ситуация: максимальная оснащённость ИБ-инструментарием сочетается с глухотой к реальным угрозам. Как такое возможно? Рассуждает директор по безопасности «СёрчИнформ» Иван Бируля.

— Прошёл год со времени вступления в силу закона 187-ФЗ, вступил в силу закон 167-ФЗ, обновлено Положение 382-П. Начался сбор биометрии для более точной идентификации клиентов банков. Какие ещё меры могут сегодня радикально повлиять на уровень безопасности в финансовой сфере?

— Банки всегда были и остаются локomotifом внедрения новых технологий, в том числе тех, которые касаются информационной безопасности. Появление новых законов в этом плане — не революция в безопасности, а усовершенствование механизмов, которые есть. Появление ФинЦЕРТа и автоматизированная система взаимодействия с банками было отличной новостью. Понятно, что компаниям не хочется делиться информацией об инцидентах, но именно это в конечном счёте влияет на поднятие общего уровня в сфере ИБ.

— Меры регулирования в основном касаются внешних атак. Вы же часто утверждаете, что основные угрозы безопасности банков — внутрен-

ние нарушители. На чём основана эта уверенность?

— Во-первых, на собственном опыте — я больше семи лет работал в банке в должности начальника отдела безопасности, и за это время успел составить свою карту угроз со стороны сотрудников. Банки находятся, пожалуй, под самым пристальным надзором по сравнению с другими организациями. Это настолько эффективный контроль, что сейчас финансовая сфера — одна из самых защищённых. Мои коллеги считают, что по этой причине банки перестали быть лакомым куском для мошенников — слишком дорого их атаковать.

Но фишинг и социальная инженерия — то, от чего оказалось гораздо сложнее уберечься. Со стороны атакующих это самый простой и дешёвый способ. По данным ФинЦЕРТа человеческий фактор находится на первом месте среди всех причин, которые определяют успешность внешних атак на инфраструктуру.

Что касается преднамеренных действий со стороны самих сотрудников, наши данные подтверждают, что это большая проблема. По данным опроса 1024 ИБ-специалистов на Road Show SearchInform, 40 % банков сталкиваются с тем, что сотрудники используют ресурсы компании в собственных целях. При этом доля руководителей среди нарушителей велика — больше 35 %. Эта цифра выше, чем в других отраслях.

— Тогда кто, по вашему мнению, самые опасные нарушители в банках?

— Как раз руководители и есть самые вероятные нарушители, даже когда у них нет злого умысла. Причина их уязвимости банальна: нет времени на безопасность. Например, не глядя соглашаются на настройки приватности, хранят критичную информацию на телефонах. Я знал директора, который всегда использовал один и тот же пароль, а когда его нужно было изменить, менял лишь последнюю цифру. Один из топ-менеджеров банка из верхушки «сотни» всю использует личную почту для переписки по деловым вопросам.

Второе место занимают ИТ-специалисты, которые сегодня, по сути, управляют всей корпоративной инфраструктурой. Так что это ещё одна категория критически важных инсайдеров. В моей практике самой частой причиной проблем с ИТ-специалистами был не их злой умысел, а банальная халатность: забыл обновить систему или заблокировать учётную запись после увольнения сотрудника.

Хотя человеческий фактор никто не отменял: бывали случаи, когда системные администраторы злоупотребляли правами намеренно. В знакомой компании у системного администратора после увольнения сохранились все права доступа. Он подключился к системе удалённо и загрузил в неё файл-бом-

бу — программу с отложенным запуском. Она активировалась через две недели и стёрла конфигурации сетевого оборудования. В результате работа встала: сотрудники не могли отправить и получить письма, зайти в Интернет, а звонки sales-менеджерам переадресовывались директору. Если бы в компании была установлена DLP, она бы сигнализировала о том, что в ИТ-инфраструктуру компании был загружен сомнительный файл, у ИБ-специалиста было бы 2 недели, чтобы устранить проблему.

— **А как насчёт рядовых сотрудников: операционистов, кассиров, консультантов?**

— Это важная категория вероятных нарушителей. Скажем честно, уровень зарплат у них довольно скромный, при том, что они имеют доступ к критичной информации. Момент важный, поскольку заработать сверх положенного не прочь многие, и предложения есть: банковские карты и базы данных пользуются спросом на чёрном рынке. Люди на хороших должностях гораздо реже готовы рисковать местом ради односторонней выгоды в 50–60 тысяч рублей.

И ещё важный момент. Вопросы идентификации клиентов — это нерешённые проблемы безопасности банков. Я сам недавно с ней столкнулся — пришлось полчаса отвечать на вопросы для идентификации личности. А в следующий раз операционист настолько бегло проверила паспорт, что протягивать его мог почти кто угодно. Нарушение регламента из-за банальной усталости тоже частая практика.

— **Но если банки буквально напичкованы суперсовременными инструментами защиты, откуда утечки данных? Та же история со Сбербанком, которая и вовсе стала публичной...**

— В случае со Сбербанком не возмусь делать стопроцентные выводы. Конечно, нет сомнений, что на его вооружении есть весь необходимый ИБ-инструментарий, более того, штат ИБ-специалистов в этом банке самый большой в нашей сфере. Но, предположу, в этом и парадокс: чем больше коллектив ИБ-специалистов, тем выше риск простой человеческой ошибки. Ещё одна причина в том, что не всегда в банках установлено хорошее ПО,

не всегда оно должным образом эксплуатируется.

Например, я считаю, что DLP-система должна быть в 100% банков — при существующем уровне угроз, о которых мы говорим. А они стоят далеко не везде. Там, где стоят, не всегда эффективно используются. Но есть и гораздо более абсурдные ситуации. Есть немало число организаций, где DLP закуплены, но не развёрнуты. Если речь о каком-то мелком региональном банке, это не удивляет. Но я знаю о подобной ситуации как минимум в одном банке из первой тридцатки топа!

— **Как такое возможно при жёстком регулировании?**

— Законы, стандарты — это рамки и набор практик, которые добропорядочным банкам дают в руки инструментарий, а менее ответственным — возможность «закрыть вопрос» перед регуляторами. Сейчас не приходится рассчитывать на какие-то «серебряные пули» в безопасности. По большому счёту все инструменты в руках у специалистов по безопасности есть. Вопрос в том, как они ими пользуются, есть ли в компании воля, чтобы их применять.

Но есть и обратный тренд, который я отмечаю в разговорах со знакомыми банкирами. Многие банки сегодня используют систему ИБ-рисков для оценки финансового результата по аналогии с оценкой качества кредитов. Думаю, со временем это станет не просто доброй волей самых сознательных банкиров, но и требованием регулятора.

— **«СёрчИнформ» — производитель DLP-систем, которые вы называете обязательными к использованию в современных банках. Но ваша компания — сторонник довольно спорной позиции не использовать блокировки утечки информации. Поясните ее, пожалуйста.**

— Такая позиция кажется спорной, если не знать логику инсайдеров. Наверное, уже не осталось злоумышленников, которые не догадываются, что ИБ-служба контролирует каналы передачи информации, как минимум почту, USB, браузер. И наша статистика подтверждает: в подавляющем большинстве случаев по этим каналам идёт ненамеренная утечка. От такой утечки нужно страховать — я не вижу ниче-

го плохого в блокировке, скажем, корпоративной почты, чтобы такие случаи исключить. Но если речь не об ошибке, а о продуманном, осознанном действии, инсайдер будет куда изобретательнее, он будет всеми силами стараться обойти систему безопасности. Организовывать неконтролируемые тоннели в интернет (например, расшаривать Wi-Fi сеть с личного мобильного), применять шифрованный VPN до облачного сервиса, подключаться к инфраструктуре через TeamViewer, наконец. В итоге получается, что чем больше мы блокируем, тем больше переводим серьёзные инциденты из контролируемой угрозы в неконтролируемые. В данном случае единственный качественный результат даст обнаружение инцидентов на ранней стадии. Утечка — это процесс, а сам момент пересылки — всего лишь его финал. Наш подход позволяет этот финал предвидеть и до него не доводить.

— **Звучит как выбор между плохим и худшим...**

— Это выбор приоритетов. Сейчас в СМИ перегрета тема утечки персональных данных. Да мы и сами упираем на то, что вопрос нужно ставить на особый общественный контроль. Но если смотреть с точки зрения бизнеса, тут нет финансовых потерь. Главная финансовая угроза компаний — мошенничество, коррупция, промышленный шпионаж. А это всё хорошо спланированные действия сотрудников, которые нужно скрупулёзно расследовать: какую информацию человек собирается сливать, кому, о чём с ним договаривается и т.д. Всё это позволяет делать DLP.

Топорные блокировки сделают действия злоумышленников только более изощрёнными. Использование блокировки очень быстро компрометирует сам факт использования DLP в компании, ведь методом проб и ошибок сотрудники очень быстро обнаруживают, какие каналы в компании контролируются, а где есть лазейка.

— **В 2018-м вы выпустили новый продукт — ProfileCenter в составе DLP-системы. И уже к концу года заявляли о более чем десятке продаж. Какую задачу решает профайлинг?**

— Это метод превентивной работы. То, о чём многие ИБ-специалисты дав-

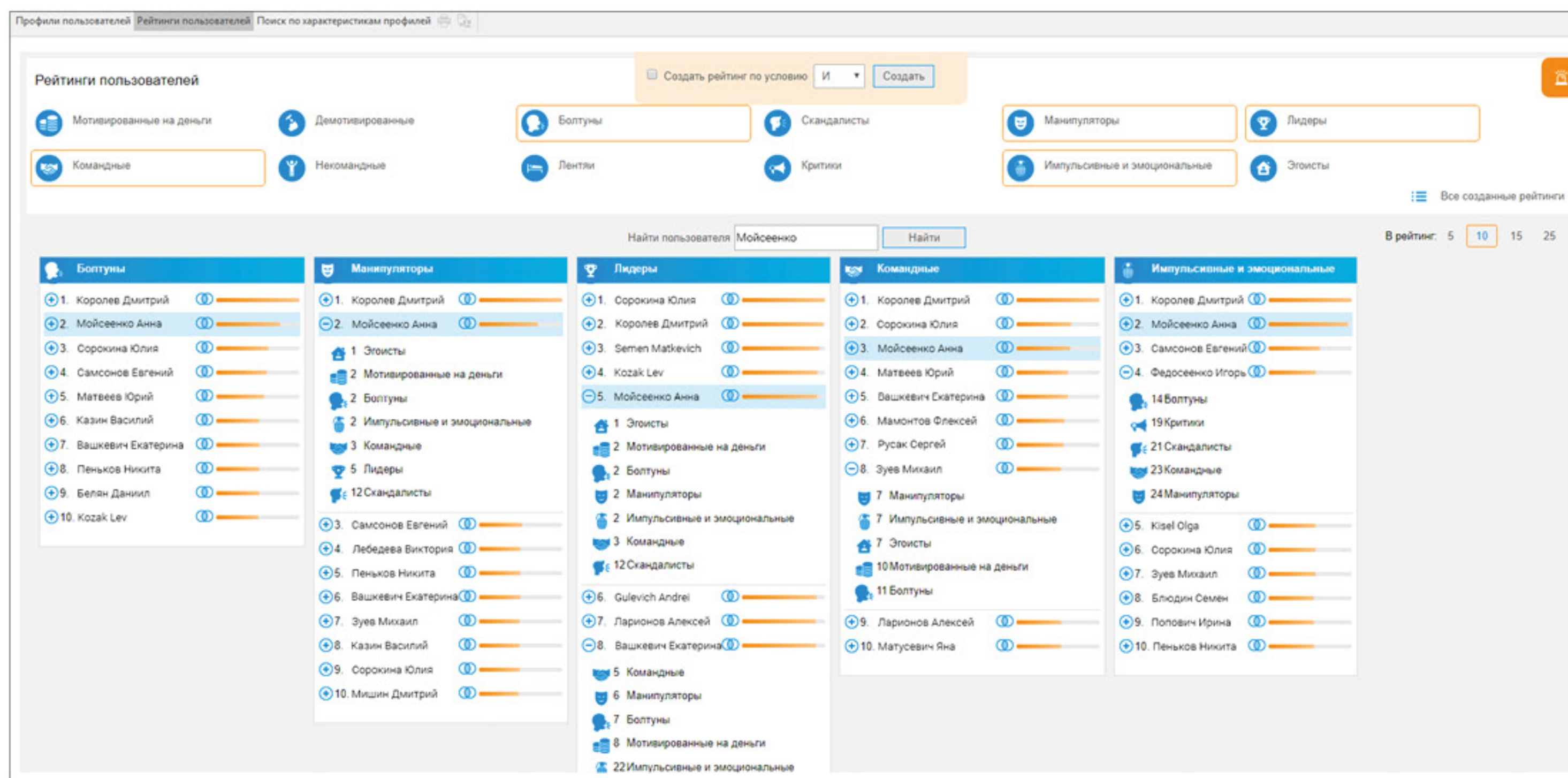


Рисунок 1. Скриншот интерфейса модуля ProfileCenter

но мечтали. Он зарекомендовал себя у работников спецслужб и ИБ-специалистов для входного контроля сотрудников. А нам удалось автоматизировать процесс, чтобы видеть в динамике, как меняется личность человека, его стрессоустойчивость, лояльность, готовность к противоправным действиям. Понятно, что опытный ИБ- или HR-специалист ведут эту работу точно. А что делать, если коллектив в много сотен и даже тысяч сотрудников?! И, напомню, все они имеют доступ к критической информации! Именно в этих ситуациях и работает автоматизированный профайлинг.

На основе переписок пользователя, собранных DLP-системой, программа создаёт профиль человека и корректирует его в динамике изменений. В понятном интерфейсе ИБ-специалист видит раскладку как по каждому конкретному пользователю, так и по кол-

лективу в целом (см. рис. 1). Видит рейтинги, например, самых амбициозных, самых разговорчивых, самых мотивированных на деньги и т.д.

Специалист получает информацию, за кем из сотрудников следить время от времени, за кем — постоянно; подходит или нет сотрудник на ту или иную должность; насколько безопасно давать ему доступ к информации, ресурсам компании; кому из сотрудников достаточно «внушения» и профилактической беседы, а с кем следует регулярно проводить тренинги по информационной безопасности; кого следует более строго наказывать за нарушение правил и т.д. Так, огромные коллективы становятся видны как на ладони.

Но мы в компании всегда призываем проверять это на практике. Пробной версией профайлинга и нашей DLP «КИБ СёрчИнформ» можно пользоваться в течение месяца. Об-

ратитесь к нам по контактам ниже и оцените уровень безопасности в компании.

— Получается, что те методы, которые реализуете в DLP вы, это уже не только о безопасности...

— Я вижу, как меняется наша профессия. И да, сейчас важен обмен информацией между различными подразделениями компании. ИБ-специалист, обладая огромной информацией о коллективе и имея мощные инструменты аналитики — DLP-системы — становится советником руководителя и кадровой службы, подсказывая, где тонкие места не просто в безопасности, но и в самом бизнесе. В свою очередь для успешной работы он не может быть оторван от бизнеса, должен разбираться в его бизнес-процессах, понимать расклад по конкурентам, чувствовать остроту кадрового вопроса. Это востребованные сегодня компетенции.

Протестируйте бесплатно ProfileCenter и DLP «КИБ СёрчИнформ» с полным функционалом. Узнайте подробности:

- ♦ по телефону +7 (495) 721-84-06
- ♦ или по ссылке из QR-кода.

Не забудьте сообщить менеджеру кодовое слово BIS Journal.



**Андрей ПЕРКУНОВ**

директор департамента сетевой инфраструктуры, руководитель направления «Информационная безопасность», компания СТИ

**Сергей СМЕЛОВ**

технический консультант Ivanti
Россия, СНГ, Грузия и Монголия

РАЗРЫВАЯ ЗАМКНУТЫЙ КРУГ

КАК РЕШЕНИЯ ПО АВТОМАТИЗАЦИИ PATCH
MANAGEMENT В ГЕТЕРОГЕННОЙ СРЕДЕ ОБЕСПЕЧИВАЮТ
РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД К БЕЗОПАСНОСТИ

В последнее время в сегменте ИБ произошло несколько значимых событий, которые оказали и будут ещё долго оказывать существенное влияние на этот рынок: эпидемия WannaCry и других шифровальщиков, виток роста финансовых киберпреступлений, атаки на криптоиндустрию, количественный и качественный рост атак на смартфоны, возвращение целевых атак, направленных на уничтожение данных. Количество вирусов и вредоносных программ, направленных на кражу информации, растёт с каждым днём. История расследования всех резонансных инцидентов ИБ, атак и эпидемий показывает, что всё начинается с эксплуатации одной или нескольких уязвимостей в операционных системах, системном ПО или пользовательских приложениях. Если посмотреть глубже — на историю развития средств защиты, то можно увидеть, что все они направлены на защиту от возможности эксплуатации тех или иных уязвимостей, а не на решение сути проблемы — исправление или устранение источника потенциальных проблем и брешей в ИТ-системах. А ведь именно неза-

крытая уязвимость может стать фактором, от которого зависит успех атаки злоумышленников.

ЗАЧЕМ НУЖЕН PATCH MANAGEMENT

При этом по оценкам большинства аналитиков количество уязвимостей растёт из года в год, выходя за рамки не только серверных или операционных систем Microsoft. Взрывной рост уязвимостей платформы Android — показательный пример проблем, которые возникают в гетерогенной современной среде. Финансовые организации находятся под повышенным давлением и рисками, связанными с необходимостью не просто определения, а быстрого исправления и устранения уязвимостей в серверных платформах, клиентских системах, базах данных и приложениях.

Системные администраторы по-прежнему используют учётные записи «по умолчанию» в различном системном программном обеспечении и не торопятся обновлять устаревшие версии продуктов. Может показаться удивительным, но зачастую это характерно и для финансовых организаций: информация об уязвимости была опубликована год или два назад, обновле-

ние, закрывающее брешь, выпущено компанией-разработчиком, но на компьютерах пользователей оно отсутствует. 99,9% эксплойтов, которые были использованы при совершении атак, находились в базе данных известных уязвимостей CVE уже год и более (по данным отчёта Data Breach Investigations Report от компании Verizon). К сожалению, это распространённая практика. Безусловно, управление обновлениями (Patch Management) не является панацеей, однако, введение данных практик в регламент обслуживания позволит существенно снизить риски финансовых потерь от атак злоумышленников через использование известных уязвимостей.

Patch Management должен выполняться на регулярной основе, все целевые системы и хосты должны быть проинвентаризированы, просканированы и на них установлены патчи, так как достаточно одной уязвимой системы или приложения в сети для компрометации, которая послужит источником масштабного заражения и распространения вредоносного ПО. Эффективная стратегия Patch Management для финансовых организаций является гарантией защищённости и устойчивого функционирования корпоративных систем.

ПРОТИВОРЕЧИЯ МЕЖДУ СЛУЖБАМИ ИБ И ИТ

С точки зрения служб ИБ исправление уязвимостей должно осуществляться как можно быстрее, и патчи должны устанавливаться немедленно после выхода исправления. Однако с точки зрения служб эксплуатации и поддержки систем, стабильность работы и гарантии отсутствия проблем после установки патчей для бизнеса стоят далеко не на первом плане, поэтому и должны быть интегрированы в процесс Patch Management.

Платформы управления Patch Management помогают разрешить конфликт между сотрудниками ИБ и ИТ для ускорения исправлений и при этом обеспечения стабильной работы систем и тестирования корректности установки исправлений. Платформы и решения можно разделить на несколько категорий в зависимости от задач, на решении которых они специализируются.

РЕШЕНИЯ ДЛЯ ПАТЧИНГА ОС WINDOWS

Это наиболее распространённый в компаниях класс решений, в первую очередь по причине наличия условно бесплатного продукта Microsoft WSUS (Windows Server Update Services), позволяющего автоматизировать задачи загрузки обновлений безопасности. Он распространяется по сети в средах Windows для компаний, использующих ОС Microsoft. Однако WSUS не подходит для большинства крупных и гетерогенных сред и нередко используется в комбинации с другими решениями по патч-менеджменту. WSUS не является платформой корпоративного уровня для реализации эффективной стратегии по патч-менеджменту, так как не обладает рядом ключевых возможностей:

- ♦ масштабированием для возможности управления более 1000 компьютеров;
- ♦ у неё отсутствует множество функций по настройке и гибким политикам, необходимым для крупных инсталляций;
- ♦ отсутствует поддержка патчинга гетерогенных сред и сторонних приложений;

♦ отсутствуют возможности полноценного тестирования патчей перед развёртыванием и откатом назад;

♦ ограниченные возможности по отчётности и соответствию требованиям (compliance).

Тем не менее во многих компаниях бытует мнение, что патчинг Windows является достаточным для закрытия большей части уязвимостей. Оно в корне неверно, статистика эксплуатации уязвимостей и использования эксплойтов говорит об обратном.

В последних версиях ОС Microsoft изменила политику выпуска обновлений, чтобы упростить данный процесс и снизить вероятность нестабильной работы из-за версионности и взаимного влияния пакетов обновлений между собой. Администраторы теперь не могут устанавливать только отдельные обновления или наоборот не устанавливать часть патчей, которые могут повлиять на стабильность — они должны применять все исправления единым пакетом (ежемесячный пакет исправлений безопасности). Это в некоторых аспектах упрощает развёртывание, так как не нужно тестировать и проверять взаимовлияние различных пакетов обновлений между собой. Тем не менее, остаются сложности с совместимостью и работой приложений за счёт модели «всё или ничего».

РЕШЕНИЯ ПО ПАТЧИНГУ КАК ЧАСТЬ CLIENT MANAGEMENT TOOLS

Крупные организации могут использовать специализированные решения для управления парком клиентских устройств (в первую очередь рабочих мест пользователей — desktop) и использовать встроенный функционал Patch Management как часть общей задачи управления активами. Примером такого продукта может выступать Microsoft System Center Configuration Manager (SCCM). Данное решение позволяет управлять политикой патчинга в крупных средах, оно исключает большую часть недостатков WSUS, но в то же время обладает главным недостатком — не поддерживает гетерогенные среды и требует применения дополнительных продуктов (Add-on для SCCM), чтобы добавить функционал закрытия уязвимостей в прикладном и стороннем ПО.

Примером такого решения для SCCM может выступать Ivanti Patch Manager for SCCM, который бесшовно интегрируется в консоль управления SCCM и процесс патчинга и добавляет возможность управления и исправления уязвимостей для всех типов приложений и служб, а не только приложений Microsoft. Для некоторых компаний, в первую очередь использующих решения на платформах Windows, такой вариант может быть оптимальным.

СПЕЦИАЛИЗИРОВАННЫЕ РЕШЕНИЯ ПО ПАТЧИНГУ СТОРОННЕГО ПО И ПОЛЬЗОВАТЕЛЬСКИХ ПРИЛОЖЕНИЙ

В настоящий момент необходимость данного класса решений значительно повысилась, и всё больше служб ИБ сталкивается с комплексной задачей устранения уязвимостей в сложных гетерогенных средах и любом ПО, используемом в организации. Периодический, постоянный и целостный патчинг гетерогенного ПО (т.е. программного обеспечения, не поставляемого поставщиками ОС, например, Microsoft или Apple) является сложной и подчас неразрешимой на первый взгляд задачей для служб ИБ. Большинство разработчиков прикладного ПО не предоставляют единого и автоматизированного метода получения, а что более важно — распространения и применения патчей для крупных корпоративных сред. Все разработчики (Adobe, Google и др.) имеют различные политики выпуска исправлений, способы их установки, форматы... Поэтому сложно отследить взаимозависимости и влияние на приложения, отсутствует информация об успешности или неуспешности установки исправления и т.д.

Специализированные решения для патчинга корпоративного уровня обеспечивают все этапы процесса управления и устранения уязвимостей в организации, таким образом значительно экономя затраты и время на анализ, получение, тестирование, перепакровку и установку обновлений в гетерогенной среде, тем самым гарантируя закрытие уязвимостей от потенциальных эксплойтов и направленных атак. Кроме

того, возможность реализации схемы Patch Management по гибкому сценарию с использованием агента или без-агентской схемы открывает дополнительные возможности по управлению безопасностью конечных устройств. Например, постоянную проверку соответствия конфигурации конечных систем требованиям безопасности или постоянный мониторинг установки, запуск и использование авторизованных и неавторизованных приложений.

РЕШЕНИЯ ПО ПАТЧИНГУ СЕРВЕРНЫХ ПЛАТФОРМ, СРЕДСТВ ВИРТУАЛИЗАЦИИ И ОБЛАЧНЫХ СИСТЕМ

Средства по автоматизации уязвимостей серверных платформ в первую очередь направлены на поддержку большого числа этих платформ и системных сервисов, которые используются в их составе и направлены на решение проблем с применением изменений в серверных системах, устойчивая работа которых является критической для любой организации. Поэтому патчинг серверных платформ в первую очередь должен производиться с учётом соблюдения уровней сервиса и возможных простоев с владельцами ИТ-процессов и систем.

Средства патчинга должны обладать специальными механизмами для обкатки, проверки, тестирования исправлений, применения их в строго определённые временные окна, а также учитывать особенности, связанные с системами виртуализации, работой распределённых кластерных систем и сложных многозвенных приложений. Кроме того, требуется поддержка специализированных и порой специфических серверных платформ, таких как различные классы Linux, Unix, AIX, BSD систем, а также облачных сервисов. Основным критерием выбора здесь выступает покрытие всех типов используемых серверных платформ и удовлетворение ключевым функциональным задачам заказчика.

ОСНОВНЫЕ КРИТЕРИИ ВЫБОРА РЕШЕНИЯ

В различных решениях может быть реализована та или иная часть функционала по автоматизации Patch Management,

которая относится к рабочим станциям, серверам, сторонним приложениям или закрывает комплексные задачи. Основные критерии оценки следующие:

1. наличие интегрированного функционала анализа известных уязвимостей;
2. возможность обеспечения соответствия требованиям безопасности и проверки конфигураций безопасности;
3. поддержка развёртывания патчей с учётом требований политик функционирования систем и технологических расписаний;
4. поддержка возможности патчинга для устройств, не находящихся в корпоративной сети. Например, для мобильных сотрудников, подключённых к сети Интернет, но не имеющих полноценного доступа к внутренним корпоративным ресурсам;
5. полноценная поддержка всех типов конечных устройств и BYOD-платформ;
6. всесторонняя поддержка сторонних программ и приложений. Основным критерием здесь является близкое к 100 % покрытие используемых корпоративных приложений и программ, а также возможность добавления сценариев патчинга для специализированных программ или программ, специфичных для работы организации (например, версии 1С, различные платформы АБС и пр.), а также глубина метаданных, используемых для установки обновления безопасности;
7. развитый функционал корпоративного уровня, позволяющий настраивать гибкие политики и сценарии развёртывания исправлений:
 - ♦ «режим скрытой установки» (silent installation), пользовательские сообщения на русском языке и др.;
 - ♦ возможность добавления различных скриптов для развёртывания пакетов исправлений.
8. возможность интеграции или развёртывания в виде дополнения для Microsoft SCCM или WSUS для расширения поддержки патчинга сторонних приложений с учётом имеющихся ограничений служб Microsoft;
9. поддержка Patch Management для серверных платформ и виртуальных сред;

10. возможность патчинга без необходимости установки агента на целевые системы, что особенно важно для центров обработки данных и серверных систем.

Всесторонний процесс управления уязвимостями и Patch Management как часть общей стратегии управления рисками необходимо не откладывать к реализации с учётом текущего ландшафта угроз и распространения сложных таргетированных угроз и специфических атак. Использование решений Patch Management при этом желательно рассматривать как средство сформированного процесса и стандартов по управлению конфигурациями безопасности и уязвимостями активов, для чего необходимо понимать существующую ИТ-инфраструктуру, используемое ПО и взаимозависимости между её компонентами. Необходимо реализовывать процесс тестирования перед развёртыванием в продуктивную среду и согласовать временные рамки установки обновлений с владельцами информационных систем.

* * *

Для тех систем и приложений, для которых невозможно обеспечить исправление уязвимостей, нужно использовать компенсационные средства безопасности, в частности, микросегментацию на сетевом уровне, средства предотвращения атак (Intrusion Prevention System), которые имеют сигнатуры, блокирующие эксплойты на данные уязвимости. Следующим шагом является исключение или максимальная минимизация ручных операций и скриптов по установке обновлений безопасности посредством внедрения комплексного решения по Patch Management и предоставление актуальных данных по текущему состоянию и рискам по не устранённым уязвимостям. При внедрении решения стоит рассматривать его также как часть общего решения по управлению конечными устройствами (Unified Endpoint Management), в том числе и как перспективу по управлению мобильными устройствами и платформами (Mobile Device Management).

КИБЕР-ОБМЕН — ИСКУССТВО «САМОПОЗНАНИЯ» ИБ-СИСТЕМ



Антон ТИХОНОВ
ведущий технический
специалист
направления McAfee,
компания MONT

Буквально на днях, слушая беседу своих коллег об организации безопасности веб-приложений, я понял, что не все моменты мне понятны. Поправить дело я решил с помощью Гугла, который, как обычно, помог мне стать чуточку «умнее» и полезнее для моего отдела. Мои действия выстроились в ясный поток активностей, который начался процессом коммуникации с коллегами, в результате которого была произведена передача неизвестного ранее индикатора и в результате была выработана ответная реакция. Всё это очень чётко напомнило часто встречающийся поток действий при функционировании адаптивных систем организации ИБ.

«Знай своего врага и знай себя, и ты сможешь провести тысячу битв без поражений» © Искусство войны. Сунь-Цзы

Переводя эти слова на язык кибербезопасности, ты должен знать свои уязвимости, понимать тактику атакующего и быть способным использовать его слабые места. Обмен подобной информацией имеет решающее значение для разработки стратегии обнаружения и защиты. Можно начать с собственной инфраструктуры организации ИБ и представить, как собственные ИТ и ИБ средства работают вместе для организации защитного барьера организации. Как пример можно привести распространение информации о критической уязвимости ОС среди всех решений по защите конечных точек, или блокировку сетевых активностей хоста или пользователя решением по

сетевой безопасности после получения точной информации об уязвимости, или зловредом в коде, обнаруженном другим участником адаптивной экосистемы ИБ. Чем выше точность передаваемой информации, чем больше возможностей двустороннего информационного обмена, тем выше общий уровень безопасности системы и тем меньше возможностей для проникновения доступно злоумышленнику.

КИБЕР-ОБМЕН (CYBERSHARING)

Подготовка к кибер-обмену начинается с базовых вопросов «Почему?» и «Что?»:

- ♦ определение проблемы;
- ♦ перечень используемых функций/продуктов;
- ♦ простое описание целевого состояния;
- ♦ привязка действий к одной из доступных функциональных возможностей (прослушивание сообщений, отправка запроса, выполнение действия, публикация сообщения).

Использование надёжной и простой для понимания интеграционной платформы избавляет от сложностей, связанных с процессом интеграции, позволяя сконцентрироваться на самом важном. Кибер-обмен начинается с осознания решаемой проблемы (к примеру, блокирование доступа к корпоративной сети хоста, конфигурация ПО, которое не соответствует предъявляемым требованиям), представления классов вовлечённых решений (решение по защите конечных точек, решение по контролю сетевого доступа (NAC), понимания того, что должно происходить (если конфигурация

хоста неверная, то заблокировать доступ к сети) и интерпретации этих задач в реальные функции (запросить у хоста информацию о конфигурации, передать полученную конфигурацию NAC решению, в зависимости от статуса выработать реакцию (разрешить/запретить доступ).

Сам по себе принцип кибер-обмена не является чем-то новым, в отрасли было много попыток создать нечто подобное различными производителями. По причине реальной отраслевой необходимости появлялось множество различных реализаций, но сейчас всё это в прошлом, т.к. появилось чёткое понимание, что создать всё силами только одного производителя невозможно, обмен — это основа для обороны наших данных и общей победы над киберпреступниками.

ИНФОРМАЦИЯ К РАЗМЫШЛЕНИЮ

Создание коннектора для подключения одного решения к другому может быть довольно затратным по времени и сложности предприятием, ведь придётся использовать частные API, что сопряжено с большим количеством работ по сопровождению всего созданного интеграционного комплекса. Это довольно часто отпугивает компании даже от начала планирования подобных работ.

ЧТО ТАКОЕ OPENDXL?

Сегодня вместо часто изменяющихся API есть возможность использования Data Exchange Layer (DXL), готовой и зарекомендовавшей себя коммуникационной платформы, позволяющей



Рисунок 1. Эволюция DXL

решениям и механизмам ИБ делиться и получать информацию с использованием специализированных тематических сообщений. Этот тип взаимодействия можно оценить как обмен сообщениями в социальной сети Twitter, где в качестве «твиттов» будет некое сообщение, содержащее в себе ИБ информацию (IoC, команду, скрипт и т.п.), а «фоловерами» будут ваши решения ИБ.

OpenDXL открывает возможность построения адаптивной системы коммуникации решений ИБ, позволяющей обмениваться информацией, проводить точные и быстрые реакции на инциденты ИБ и интегрировать в общее коммуникационное поле различные технологии информационной безопасности вне зависимости от фирмы-производителя.

Сама технология спроектирована так, чтобы максимально расширить получаемый в результате проведенной аналитики контекст, снизить количество операций в процессе реагирования на возникающие угрозы, упростить сложности от внедрения новых разрозненных решений различных производителей и увеличить ценность уже используемых решений. OpenDXL обеспечивает беспрецедентный уровень взаимодействия сервисов в реальном времени.

ЭВОЛЮЦИЯ DXL

За весь период развития DXL, от появления в 2014 году до открытия исходного кода в 2018, технология с каждым шагом включала в себя всё больше и больше возможностей для интеграции решений в единую целостную систему (Рисунок 1).

♦ McAfee partners.

Изначально DXL использовался исключительно для взаимодействия решений McAfee.

♦ SIA Partner.

Следующий шаг эволюции DXL — предоставление возможности для технологических партнёров Security Innovation Alliance (SIA) присоединиться к единой коммуникационной платформе.

♦ В 2016 году был представлен широкой публике SDK и открытый клиент для включения в платформу in-house приложений.

♦ В 2017 году финализированный SDK открыл возможность подключения к экосистеме любых участников, включая и прямых конкурентов McAfee.

♦ В 2018 году появился полностью открытый стек компонентов единого решения (клиент, брокер, консоль управления) для построения интеграционной платформы без привязки к компании производителю.

На сегодняшний день более 4 тыс. различных организаций участвует в функционировании платформы OpenDXL.

НЕМНОГО ТЕХНИКИ

OpenDXL состоит из следующих компонентов (Рисунок 2):

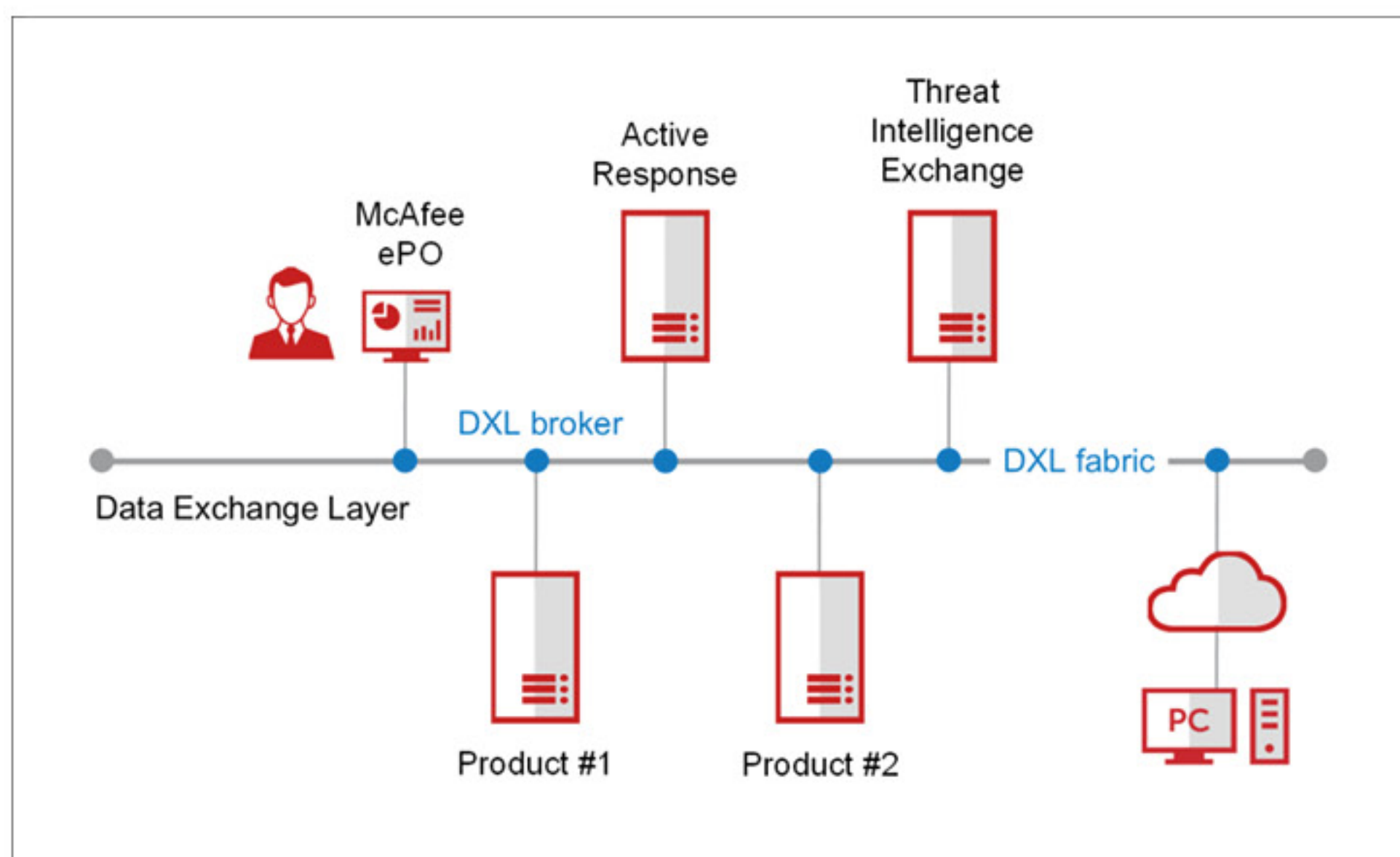


Рисунок 2. Компоненты OpenDXL

♦ OpenDXL брокер — центральное решение экосистемы, осуществляющая маршрутизацию сообщений от клиентов системы и фиксацию структуры коммуникации. Является аналогом McAfee DXL Broker с открытым исходным кодом.

♦ Консоль OpenDXL — настраиваемая Веб-консоль, предоставляющая высокоуровневый пользовательский интерфейс для взаимодействия со структурой DXL. Одним из основных модулей компонента является Fabric Monitor, позволяющий инициировать вызов служб DXL, ручную отправку/получения сообщений через графический интерфейс.

♦ Python Клиент OpenDXL & JS Клиент OpenDXL — необходим для разработки коннекторов к структуре DXL, выполняющих роль компонента, реализующего приём/передачу сообщений, запрос и предоставление сервисов.

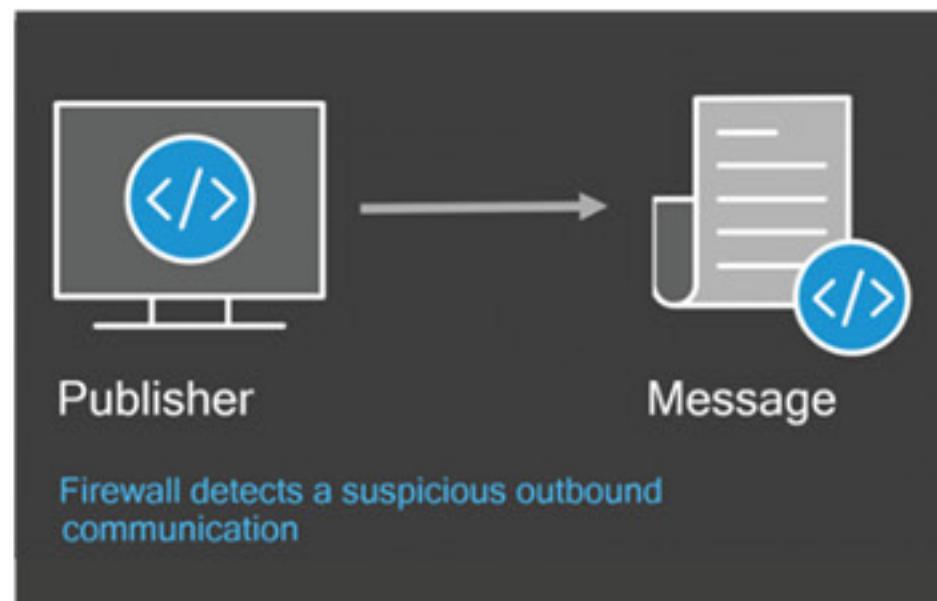
В коммуникации OpenDXL происходит обмен сообщениями в режимах «точка-много точек» и «точка-точка», в сообщении может передаваться как базовое описание конкретной угрозы (IoC), так и более сложная сущность, включающая в себя в том числе и рекомендации по ответным реакциям.

НАСТРОЙКА КОММУНИКАЦИИ

Для настройки коммуникации доступно четыре основных типа действий:

1. Публикация события

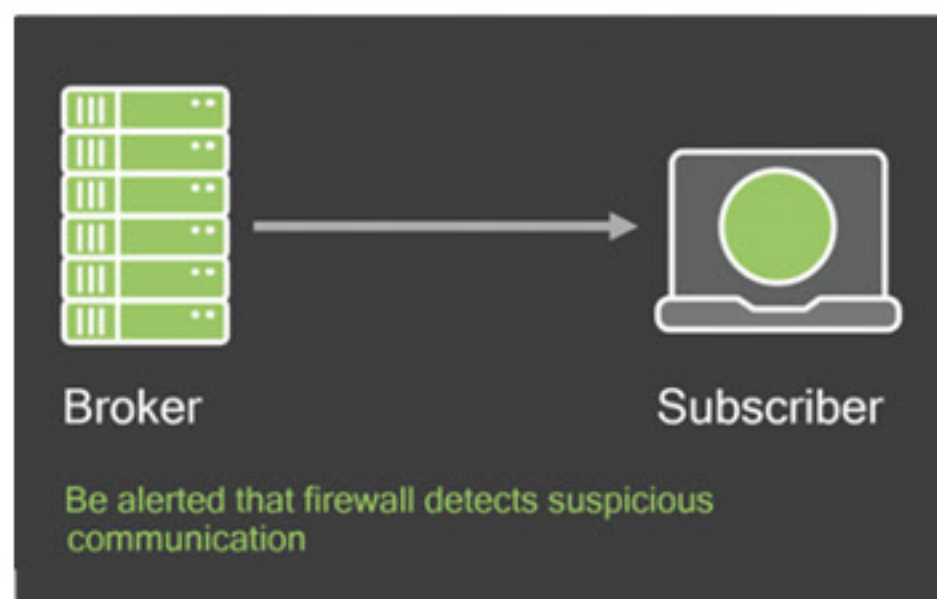
Есть возможность опубликовать некое событие. Подразумевается, что разрешается распространение информации из одной системы для информирования других (Пример 1).



Пример 1: межсетевой экран определяет подозрительную сетевую коммуникацию.

2. Получение события

Есть возможность получить событие через подписку на обновления в «теме», относящейся к определённому типу (Пример 2).



Пример 2: наша система получает информацию от межсетевого экрана о том, что обнаружена подозрительная сетевая активность.

3. Задать вопрос

Есть возможность запросить доступ к услуге (Пример 3).

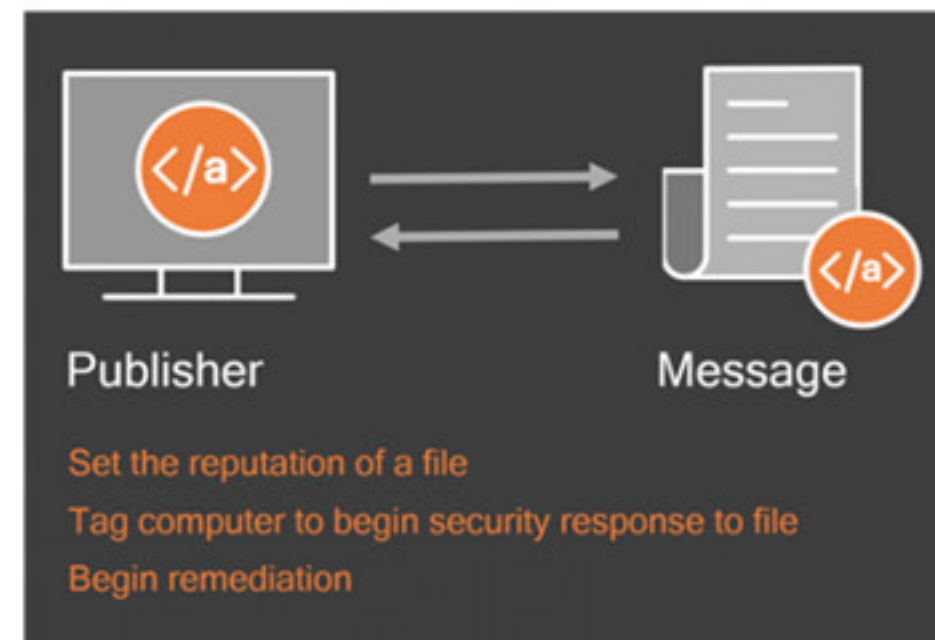


Пример 3: Коммуникация в режиме точка-точка (unicast) в формате запрос — ответ. Решение отправляет DXL запрос, после чего ожидает ответа. Тут

возможно получение такой информации, как репутация файла, параметры безопасности, применённые на системе.

4. Выполнить действие

DXL может выполнять различные действия в качестве ответной реакции на запрос (Пример 4).



Пример 4: В качестве действия может быть обновление или назначение репутации файла, запрос дополнительной информации о событии, инициация процесса устранения последствий события, маркирование хоста с целью выполнения дальнейших автоматизированных действий и т. п.

Имея в запасе данные операции, можно разобрать несложный пример решения задачи предотвращения использования нежелательного объекта на хостах компании.

Разделим задачу на этапы:

1. Определение конкретной задачи: «Мне необходимо предотвратить возможность запуска файлов с известной негативной репутацией».
2. Список вовлечённых решений ИБ. В рамках данной задачи единственным вовлечённым продуктом будет сервер локальной репутации Threat Intelligence Exchange.
3. Простое описание целевого состояния, того, что должно происходить: «При обнаружении в сети объекта, известного как «зловредный», оповестить все системы безопасности об этом».
4. Отнести необходимые действия с одной из четырёх доступных возможностей платформы.

Из четырёх доступных возможностей (Публикация, получение сообщения, отправка запроса, выполнение действия), наша задача «ложится» в публикацию сообщения — Threat Intelligence Exchange публикует информацию о том, что файл является вредоносным.

Из четырёх доступных возможностей (Публикация, получение сообщения, отправка запроса, выполнение действия), наша задача «ложится» в публикацию сообщения — Threat Intelligence Exchange публикует информацию о том, что файл является вредоносным.

Из четырёх доступных возможностей (Публикация, получение сообщения, отправка запроса, выполнение действия), наша задача «ложится» в публикацию сообщения — Threat Intelligence Exchange публикует информацию о том, что файл является вредоносным.

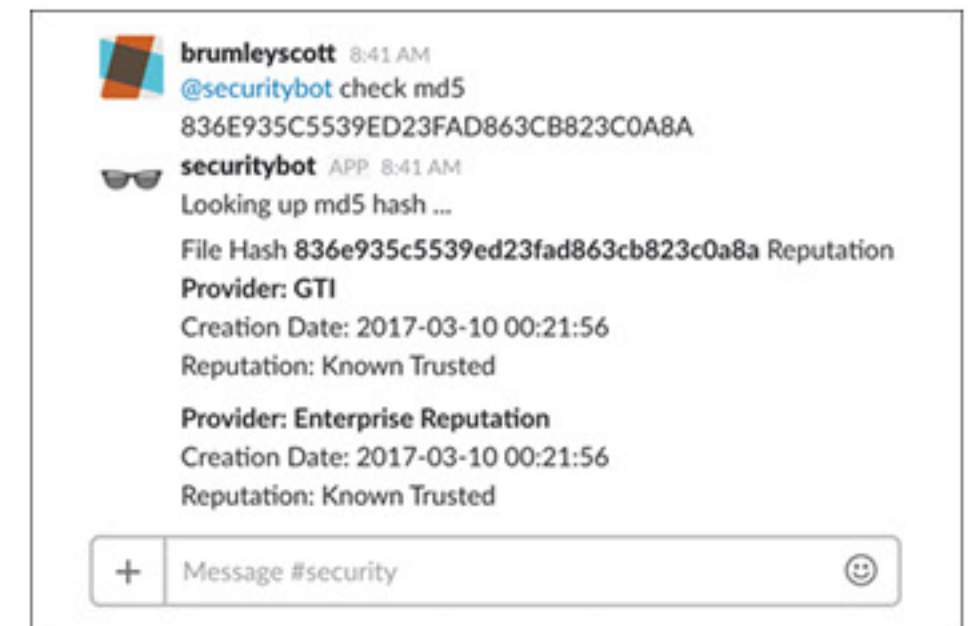


Рисунок 3

ИНТЕГРАЦИЯ

Для начала работ по интеграции достаточно посетить ресурс OpenDXL.com — там можно найти всё, от компонентов платформы и подготовленных к работе окружений разработки, выполненных в виде Docker-контейнеров, до подробной документации и созданных интеграционных модулей.

На сегодняшний день доступно около сотни готовых к использованию модулей из более чем двадцати категорий применения. Например, модуль интеграции корпоративного репозитория репутации объектов Threat Intelligence Exchange и инструмент для коллаборации Slack, позволяющий запрашивать TIE через бота Slack о наличии известной репутации по отправляемой контрольной сумме файла (Рисунок 3).

Также можно инициировать нужный тип сканирования сети через решение Nmap при помощи соответствующего модуля OpenDXL интеграции или организовать передачу файлов по общей шине OpenDXL. На сегодня максимальный размер передаваемого сообщения составляет 1 мегабайт, данный модуль позволяет организовать передачу объекта любого размера частями, соответствующими требованиям OpenDXL.

Сама суть открытости данного проекта предоставляет большое количество степеней свободы для кибер-обмена, нет никаких привязок к производителю, нет ограничений по продуктам для интеграции с DXL. Единственное, что требуется — желание двигаться вперёд и вверх, к созданию стабильной и безопасной коммуникационной платформы ИТ и ИБ сервисов компании на базе OpenDXL.

ДВЕ СТОРОНЫ МОБИЛЬНОЙ ЭЛЕКТРОННОЙ ПОДПИСИ



**Денис
КАЛЕМБЕРГ**
генеральный
директор компании
SafeTech

ЭЛЕКТРОННАЯ ПОДПИСЬ В СМАРТФОНЕ —
УСИЛИВАЮЩАЯСЯ ТЕНДЕНЦИЯ 2019 ГОДА

Завершившийся 2018 год стал годом успешного внедрения и развития новых мобильных финансовых сервисов, причём многие банки сделали упор именно на клиентов — юридических лиц. Внедрение мобильной и «облачной» электронной подписи крупнейшими игроками финансового рынка показало пример, каким образом можно снизить риски использования современного дистанционного банкинга, за счёт этого значительно расширить список предоставляемых сервисов и убрать лимиты по многим типам операций. Предполагаю, что в следующем году этот тренд перейдёт и на банки меньшего масштаба.

АЛЬТЕРНАТИВА SMS И PUSH-КОДАМ

Будучи игроком рынка технологий подтверждения электронных транзакций, мы ещё три года назад заметили, что банки стали искать альтернативу SMS и PUSH-кодам и лучше всего для решения данной задачи им подошла «подпись в смартфоне», что обусловлено сразу несколькими причинами:

- ♦ соображениями обеспечения безопасности — подпись на смартфоне пользователя повышает безопасность операций, поскольку формируется на основе данных конкретной транзакции и уникальных характеристик используемого мобильного устройства;

- ♦ экономические соображения — стремление снизить расходы на услуги операторов связи;

- ♦ стремлением банков сделать работу своих клиентов более простой и удобной — технологии мобильной и «облачной» подписи позволяют подписывать финансовые транзакции одним движением пальца по экрану.

При этом важно понимать, что разным сегментам клиентов и для разных наборов сервисов необходим разный уровень «юридической значимости» подписи. Например, при дистанционном обслуживании физических лиц или среднего/мелкого бизнеса вполне достаточно простой или усиленной неквалифицированной подписи, а для предприятий с гос. участием или взаимодействия с госструктурами (сдача налоговой отчётности, регистрация юрлиц и т.д.) необходимо использовать сертифицированные криптосредства и усиленную квалифицированную подпись (КЭП).

Мы рады признать, что компании SafeTech удалось разработать и предоставить клиентам удобные и безопасные технологии для удалённого подтверждения электронных транзакций и подписи документов — решения, которые позволяют российским банкам активно внедрять как новые сервисы с использованием КЭП, так и усиленную подпись для замены SMS-кодов в системах обслуживания физических лиц, а также предприятий среднего и малого бизнеса.

ЕДИНОЕ РЕШЕНИЕ

Первое решение, PayControl, для формирования «электронной подписи в смартфоне», позволяет клиентам с высоким уровнем безопасности и удобства подтверждать свои операции, создаваемые в любых цифровых каналах (Интернет-банкинг, мобильный банкинг, операции CNP, телефонный банкинг, в частности, Private-bank, и т.д.). PayControl может работать как в виде отдельного приложения для смартфона, так и встраиваться непосредственно в приложение мобильного банкинга. Только в течение нынешнего года этот продукт внедрили такие банки, как: Альфа-банк, Россельхозбанк, Ак Барс банк и многие другие. Поддержку PayControl «из коробки» обеспечивают крупнейшие разработчики систем дистанционного банкинга в РФ (БСС, iSimpleLab, ArtSoft, Информационные системы и другие).

Второе решение, КриптоПро myDSS — совместная разработка с компанией КриптоПро — позволяет просто и удобно подтверждать квалифицированной электронной подписью цифровые транзакции и документы прямо со смартфона. КриптоПро myDSS уже используется в крупнейших российских банках, например, клиенты ВТБ могут с его помощью зарегистрировать в налоговой юрлицо не выходя из дома, в процессе запуска ещё несколько проектов, связанных с предоставлением сервисов, не имеющих сегодня аналогов на рынке. Но об этом мы расскажем уже в новом, 2019 году.

Мобильная квалифицированная электронная подпись Решение КриптоПро myDSS на базе технологии PayControl



Квалифицированная электронная подпись в системах электронного документооборота при помощи смартфона.

Мобильное приложение myDSS является частью решения КриптоПРО DSS (сертификат соответствия требованиям ФСБ России СФ/124-3481 от 10.08.2018) и позволяет обеспечить строгую аутентификацию пользователя и контроль подписываемых документов.

myDSS проще, дешевле и удобнее, чем токены, смарт-карты или программные криптопровайдеры.

Что такое myDSS

КриптоПро myDSS – это приложение для смартфона, которое позволяет подписывать квалифицированной электронной подписью документы и контролировать действия пользователя в системах дистанционного банкинга, порталах госуслуг, системах ЭДО, электронных торговых площадках и т.д.

В основе myDSS лежит технология PayControl, которая обеспечивает строгую криптографическую аутентификацию пользователей, безопасное online-взаимодействие, отображение документа и подтверждение операций. Это позволяет сервису облачной электронной подписи КриптоПро DSS выполнить требования, предъявляемые регулятором к средствам электронной подписи.

Безопасность

Приложение myDSS выполняет визуализацию электронного документа и формирование подтверждения на его подписание в КриптоПро DSS.

Криптографическая аутентификация и защищенный обмен между приложением и сервером КриптоПро DSS гарантируют, что только легальный пользователь сможет воспользоваться ключами подписи.

Ключи электронной подписи пользователей хранятся в сертифицированном КриптоПро HSM в неизвлекаемом виде.

Юридическая значимость подписи

Документ и другие действия пользователя заверяются квалифицированной электронной подписью, что обеспечивает неотказуемость действий. Пользователь не только подтверждает содержание документа, но и в дальнейшем не имеет возможности отказаться от совершенного действия.

КриптоПро myDSS

Совместная разработка компаний КриптоПро и SafeTech на базе сертифицированного программно-аппаратного средства криптографической защиты информации КриптоПро HSM, КриптоПро DSS и системы подтверждения электронных транзакций PayControl.



Дмитрий РОМАНЧЕНКО
директор Центра технологий безопасности
компании «ИБС экспертиза»

ЛУЧШИЕ ПРАКТИКИ

УПРАВЛЕНИЕ ДОСТУПОМ К ИНФОРМАЦИОННЫМ РЕСУРСАМ ДЛЯ КОРПОРАТИВНОГО СЕКТОРА

Комплексное управление доступом к информационным ресурсам — актуальная задача для организаций, в которых количество информационных систем превышает 50, численность пользователей — более 1500, а частота изменений полномочий доступа составляет десятки в день. Факторы, усложняющие эту задачу: разнообразие технологических платформ управляемых информационных систем, большое количество организаций в холдинге, территориальная распределенность площадок организации, сложность процессов управления доступом. Важный фактор успеха — уровень зрелости ИТ-инфраструктуры и ИТ-процессов организации в целом.

ОПТИМАЛЬНЫЙ СЦЕНАРИЙ

Часто приходится сталкиваться с мнением, что задача централизованного управления доступом к информационным ресурсам сводится только к внедрению системы IDM-класса. Перспективный подход состоит в том, что эта задача должна рассматриваться как системный проект, существенно затрагивающий ИТ-процессы организации в целом, ИТ-инфраструктуру, информационную безопасность, кадровые процессы.

В состав эффективного решения должны входить как минимум следующие компоненты: IDM-система, инструменты управления идентификаторами (смарт-карты и проч.), инструменты идентификации субъектов

доступа, система однократного входа (SSO), удостоверяющий центр электронной подписи. Должна быть обеспечена online-интеграция с системами управления персоналом (HR), корпоративным каталогом (чаще всего Microsoft AD), электронной почтой, службой ServiceDesk, корпоративным порталом ИТ-услуг, СКУД-системой, SIEM-системой. Интеграция с управляемыми информационными системами может осуществляться либо с помощью нативных коннекторов к этим системам, либо опосредованно через корпоративный каталог.

ИДЕНТИФИКАЦИЯ СУБЪЕКТОВ ДОСТУПА

Успешная реализация базируется на единой для организации технологии идентификации субъектов доступа. В базовом варианте это универсальное электронное удостоверение (смарт-карта), содержащее информацию о лице (ФИО, должность и фотографию), электронную RFID-метку для прохождения СКУД на периметре и в помещениях организации, а также защищенный контроллер и память для хранения электронных сертификатов для доступа в информационные системы и для электронной подписи (ЭП). Если в организации используется технология усиленной квалифицированной ЭП, то должна использоваться сертифицированная смарт-карта.

В более развитых реализациях технология идентификации может быть

дополнена идентификацией по биологическим реквизитам (отпечаток пальца, рисунок вен ладони, снимок радужной оболочки глаза, 3D-модель лица, семпл голоса и проч.). Необходимо понимать, что сегодняшний ажиотаж вокруг биометрии в российском медиа-пространстве призван продвинуть определённые продукты или сервисы компаний-разработчиков, и только интеграция технологий даёт ощутимый эффект с точки зрения практической безопасности.

ЧТО ДАЁТ КАЧЕСТВЕННАЯ РЕАЛИЗАЦИЯ

Успешное создание системы позволит организации получить единое электронное удостоверение для доступа пользователей к её ресурсам: от прохода на территорию до доступа к корпоративным ИТ-ресурсам. Будет обеспечена полная интеграция всего процесса управления доступом: на объекты, в помещения, в сеть, к информационным системам. Использование электронного удостоверения позволит технически реализовать централизованную эшелонированную модель доступа и ограничить возможность передачи паролей доступа к ИС другим пользователям, а также повысит информационную безопасность в целом за счёт использования электронных сертификатов (RSA, ГОСТ). Все реализованные процессы будут идентичны как для сотрудников организации (штатных, временных), так и для посетителей.



Система позволит формализовать, упорядочить и автоматизировать процесс управления доступом к информационным ресурсам организации, вести и поддерживать в актуальном состоянии реестр информационных ресурсов, сократить время предоставления доступа к ИС, контролировать непротиворечивость прав доступа.

АРХИТЕКТУРНАЯ ОСЬ РЕШЕНИЯ

Архитектурной осью решения является выстраивание сквозного процесса обмена информацией и управления: HR — IDM-система — корпоративный каталог (AD). От качества реализации связки зависит успех всего проекта. Лучшие практики предполагают, что IDM-система должна поддерживать все ключевые кадровые операции, реализуемые в HR-системе организации. На рынке представлено множество продуктов, относимых к IDM-решениям, но лишь малая часть обеспечивает гибкость, требуемую для практической реализации управления доступом в крупных организациях. Производители функционально бедных решений пытаются компенсировать данный не-

Успешное создание системы позволит организации получить единое электронное удостоверение для доступа пользователей к её ресурсам: от прохода на территорию до доступа к корпоративным ИТ-ресурсам

достаток «открытостью» платформы, что предполагает возможность запрограммировать решение под конкретную реализацию. Однако отсутствие проработанных функциональных блоков в конечном итоге только усложняет проект и намертво привязывает организацию к компании, внедрившей систему. Наилучшим выбором являются IDM-решения с богатыми возможностями конфигурирования процессов, при этом имеющие солидную базу нативных коннекторов к управляемым системам и открытые интерфейсы.

Для успешной реализации должны быть унифицированы кадровые процессы и процессы управления корпоративным каталогом (AD). Это первый значимый рубеж проекта: сотрудники HR понимают, что производимые ими операции имеют мгновенные послед-

ствия для всей ИТ-инфраструктуры организации (и потому цена их ошибок может быть очень высокой), а администраторы AD лишаются своего «все-силия» (ведь корпоративный каталог превращается в объект автоматического управления). Если удаётся пережить этот первый шок, то проект может двигаться дальше.

Успех реализации в существенной мере зависит и от готовности организации корректировать ролевые модели доступа к отдельным информационным системам с возможностью их взаимной увязки в бизнес-роли. Введение абстракции бизнес-ролей позволяет выстраивать правила исключения конфликта ролей (SOD). Создание оптимального каталога ролевого доступа является весьма непростой задачей, что часто недооценивается при создании системы.

ОБЕСПЕЧЕНИЕ ИДЕНТИФИКАЦИИ СУБЪЕКТОВ ДОСТУПА

Подсистема идентификации субъектов доступа — одна из важнейших частей комплекса. В повседневной корпоративной практике СКУДы относятся к физической безопасности, доступ к ИТ-инфраструктуре — к ИТ (частично к ИБ), доступ к приложениям — к области ответственности владельцев этих информационных систем. Собрать доступ ко всем указанным сущностям на базе единой технологии идентификации, выстроить сквозной процесс эмиссии (или снятия) идентификаторов — вот второй рубеж проекта.

Система эмиссии электронных удостоверений должна быть полностью интегрирована с IDM-системой, так же как и со СКУД-системой, и управляться HR-процессами. Операция выпуска электронного удостоверения должна быть организационно и технологически интегрирована в процесс приёма сотрудников на работу. В случае использования технологии биометрической идентификации снятие биологических атрибутов также должно быть интегрировано в процесс приёма сотрудников на работу.

САМООБСЛУЖИВАНИЕ ПОЛЬЗОВАТЕЛЕЙ

Для снижения затрат на управление доступом весь штат организации должен быть непосредственно вовлечён в работу в системе. Пользователь самостоятельно запрашивает ресурсы, а ответственные лица согласуют этот доступ. Для такой бесшовной интеграции и обеспечения максимального комфорта пользователей фронтальная часть IDM-системы должна быть интегрирована в корпоративный портал и ServiceDesk организации. Под интеграцией здесь понимается процессная и технологическая интеграция.

ОБЕСПЕЧЕНИЕ ОДНОКРАТНОГО ВХОДА (SSO)

Наибольший комфорт пользователи получают при реализации технологии однократной аутентификации (SSO). Качественная реализация предполагает, что SSO обеспечивается как в периметрах корпоративной сети

организации, так и за её пределами в защищённом режиме. Однократно аутентифицированный пользователь должен иметь возможность доступа ко всем ресурсам, к которым у него есть право доступа, без повторной аутентификации, либо с таковой (если это требует уровень доступа).

В случае удалённого доступа в качестве идентификатора должно использоваться то же электронное удостоверение и сертификаты, выпущенные в процессе его эмиссии, в том числе и для организации защищённого технологией шифрования канала подключения. Шлюзы доступа, используемые для удалённого доступа, должны находиться в едином контуре интеграции с IDM-системой, обеспечивая возможность предоставления удалённого доступа по аналогии с любым другим видом доступа.

ВЫПУСК ЭЛЕКТРОННЫХ СЕРТИФИКАТОВ

Для создания квалифицированной электронной подписи, а также для доступа в ИТ-инфраструктуру должны выпускаться ключи и сертификаты подписи при помощи удостоверяющего центра (УЦ). УЦ также должен быть интегрирован с IDM-системой, а процессы выпуска и отзыва сертификатов должны быть завязаны на HR-процессы. Процесс записи электронных сертификатов на смарт-карту должен быть составляющей процесса эмиссии электронных удостоверений. Сотрудник, получивший электронное удостоверение в центре эмиссии, должен иметь возможность его немедленного использования во всех процессах физического и информационного доступа.

ОТ ЧЕГО ЗАВИСИТ УСПЕХ ПРОЕКТА

Реализация функционально законченного решения возможна только в виде широко интеграционного системного проекта при аккуратном выборе компонентов. Практический опыт показывает, что современное состояние развития российских продуктов ИБ позволяет строить весьма эффективные решения при оптимальном соотношении цена/качество.

На успех проекта влияют все факторы: оптимальность выбора решений, качество проекта, готовность множества подразделений организации к существенным изменениям в своей роли и осознание ответственности за свои действия, верный выбор технологического партнёра для реализации проекта.

Существенной ошибкой является попытка внедрять отдельные продукты (часто даже в виде отдельных проектов) вместо единого системного проекта. Часто такой путь продиктован закупочной политикой организаций. Опыт показывает, что это тупиковый путь с часто весьма неэффективными инвестициями.

Ещё одной крайностью является выбор иностранного решения, которое (часто только в маркетинговых материалах) реализует all-in-one для комплексного управления доступом. Практика показывает, что даже в самых развитых иностранных решениях не бывает в равной мере качественно реализованных компонентов. Также решения могут не соответствовать российской практике и требованиям регуляторов: к этому относятся вопросы выпуска криптографических ключей и сертификатов, отсутствие коннекторов к типовым российским решениям, отсутствие поддержки российских смарт-карт, отсутствие интеграции с российским СКУД, отсутствие должной сертификация компонентов решений и пр.).

Цена ошибки в таком системном проекте складывается из стоимости неверно выбранных решений (продуктов), стоимости работ интегратора и организации, простоев организации, стоимости перевнедрения. Учитывая типовую длительность такого интеграционного проекта (7–10 месяцев), стоимость решений (десятки и сотни млн руб.), а также потери организации от простоев, суммарная стоимость неудачного внедрения может составлять сотни млн руб.

В противовес этому, корректно выстроенный комплекс и последовательный процесс внедрения позволяют организации получать постепенно нарастающий положительный эффект от внедрения.



Марина ДОНИЙ
заместитель генерального
директора по проектной работе
компании Аванпост

ОТ ЗАКАТА ДО РАССВЕТА

РОССИЙСКИЕ РЕАЛИИ РЫНКА IDM

В настоящее время российский рынок IDM стоит на перепутье. За два десятка лет пройден длинный путь. IDM-решения из сложных неповоротливых систем западного происхождения превратились в гибкие, многофункциональные программные продукты, простые во внедрении и эксплуатации. За последние несколько лет на отечественном IDM-рынке появились новые российские и зарубежные вендоры. В свою очередь, конечные потребители уже получили представление о том, какие задачи и как решаются системами такого класса. Уровень доверия к российским вендорам со стороны заказчиков значительно вырос, так как наиболее зрелые продукты прошли всестороннюю проверку в проектах разного масштаба и доказали, что не уступают лучшим зарубежным решениям. Развитию наших систем способствует и курс на импортозамещение, взятый государством в 2015 году. Казалось бы, сейчас самое благоприятное время для бурного роста отечественного рынка IDM-решений, но пока этого не происходит. Чтобы понять причины и предпосылки такого положения дел, нужно окунуться в историю и посмотреть, как всё начиналось.

НАЧАЛО: ПЕРВАЯ ВОЛНА ВНЕДРЕНИЙ

В начале 2000-х годов западные ИТ-гиганты безоговорочно доминировали на российском ИТ- и ИБ-рынках. Несомненно, уровень зрелости ИТ-систем и опыт их использования у иностранных производителей был обширнее и глубже, поэтому российское сообщество с большим рвением перенимало лучшие мировые практики. Именно в те далёкие годы однажды стало известно, что консультанты компании Oracle активно ходят по российскому рынку и предлагают решение по управлению доступом к информационным ресурсам организации. Компания, имеющая долгую позитивную историю, развитую сеть продаж в России, огромный спектр решений, используемых большинством крупных организаций, довольно быстро вызвала интерес публики к новому доселе неизвестному ИБ-решению.

Позже к Oracle подтянулись такие гиганты как IBM и Microsoft, также имеющие решения класса IDM, и могли составить достойную конкуренцию продуктам от Oracle на отечественном рынке.

Первая волна внедрения охватила наши компании-гиганты: ТНК ВР, Альфа Банк, Промсвязьбанк. Сейчас сложно найти достоверную информацию о том, как начинал свой путь развития IDM в России, потому как основная масса проектов первой волны не была успешной, да и рынок ИБ всегда характеризовался ещё большей закрытостью, чем ИТ. Оглядываясь назад, понимаешь, что причины неуспеха почти очевидны. Неожиданное появление нового продукта с «большими» возможностями сделало его привлекательным практически для каждой уважающей себя крупной компании, однако заказчики и интеграторы лишь смутно понимали, что такое

IDM-решения из сложных неповоротливых систем западного происхождения превратились в гибкие, многофункциональные программные продукты, простые во внедрении и эксплуатации

IDM и какие конкретно задачи он может решить.

При этом внедрение западных IDM-продуктов требовало огромных денежных затрат. Однако финансовая обстановка в стране была позитивной, что позволило крупным компаниям проводить опыты с новомодным ПО. Сложность использования данных решений и отсутствие специалистов требовало участия производителей в трудном процессе внедрения. Ситуация ещё усугублялась тем, что интеграторы учились и набирались опыта на первых внедрениях. Неудивительно, что проекты длились по несколько лет.

На мой взгляд, можно выделить две самые существенные проблемы того времени:

- ♦ Слишком сильное влияние внедрения IDM-системы на все сквозные бизнес-процессы компании. Т.е. тогда многие заказчики не могли предположить масштаб и сложность проектов такого рода, а также (и это самое главное!) предвидеть последствия неудачных внедрений. Кроме того, автоматизацию существенно осложнял недостаточный уровень проработки ИТ-процессов компаний.

- ♦ Неприспособленность западных продуктов к особенностям российского рынка.

Первая волна внедрений прошла со скрипом, с негативными последствиями для компаний, посеяв при этом страх у потребителей.

РАЗВИТИЕ: ВТОРАЯ ВОЛНА ВНЕДРЕНИЙ

К 2009 году на рынке IDM произошли существенные изменения. Решения стали более зрелыми. Пришло некоторое понимание того, какие задачи всё-таки можно успешно решать с помощью систем управления доступом, появились

первые квалифицированные специалисты, имевшие реальный опыт внедрения и эксплуатации таких систем. Среди интеграторов, кто уже накопил опыт успешного выполнения проектов по IDM того времени, можно назвать Computel, Инфосистемы Джет, R-style (ныне RedSys), NVision.

Казалось бы, обстановка на рынке IDM выглядела позитивной, но в 2010–2011 годы интерес к импортным продуктам для управления доступом начал снижаться. Нашей компании эта тенденция позволила предложить потребителю более гибкое и простое отечественное IDM-решение.

IDM перешёл из разряда эксклюзивных решений для крупных зрелых компаний-гигантов в категорию привычных продуктов, которые стали доступными не только для крупного бизнеса, но и для средних предприятий.

Появление на российском рынке IDM-системы местного производства послужило толчком к новому витку роста интереса заказчиков к IDM и к оживлению внимания зарубежных производителей к этому сегменту в России. К 2013 году наш рынок пополнился новыми западными вендорами IDM, такими как SailPoint и Dell (тогда компания Quest).

Мы до сих пор можем наблюдать присутствие ранее названных западных компаний в правом верхнем углу «магического квадрата» аналитического агентства Gartner.

И хотя динамика развития рынка IDM в России была несомненно положительной, ранее возникшие и все ещё нерешённые проблемы реализации проектов по внедрению оставались. Так, сроки ввода в эксплуатацию IDM-решения значительно сократились, но они всё ещё оставляли желать лучшего, а результаты оставались непрогнозируемыми. Кроме того,

стоимость внедрения и владения такими системами была по-прежнему неоправданно высокой. Вендоры-гиганты не готовы были реализовывать функционал, специфичный для отечественного потребителя, или такая доработка требовала длительных сроков. Заказчики не хотели и не могли ждать, а производителям нечего было им предложить, кроме смутных долгосрочных обещаний. В то же время развитие продуктов приводило к необходимости обновления, что создавало сложности и новые затраты, вполне сопоставимые с внедрением с нуля. Недовольство бизнес-пользователей и всё ещё не до конца сформировавшаяся у них привычка использования систем управления доступом, а также недостаточная гибкость систем и слабая их приспособленность к российским реалиям вновь потребовала качественных изменений в IDM-сегменте.

ВЫНУЖДЕННАЯ ТРАНСФОРМАЦИЯ

С 2012 года начался период, когда на наш рынок стали выходить продукты нового поколения, разработанные в условиях новой технологической реальности.

Новые инструменты разработки ПО и подходы к управлению ею, существенно упростили создание ИТ-систем, сделали её более адаптивной, что снизило стоимость разработки.

Новые решения (Avanpost IDM, SailPoint) стали более простыми и более гибкими. Такие системы стало проще внедрять, причём они уже не требовали больших затрат на сопровождение.

Отмечу, что в это же время изменилось понимание того, как надо использовать IDM-системы. Всего несколько лет назад при выборе платформы считалось, что первична автоматизация в плоскости ИТ. Теперь же накопленный опыт использования IDM-систем заставил посмотреть на них значительно шире. Заказчики чаще стали акцентировать внимание на аудите прав доступа, необходимости соответствовать требованиям регуляторов, использовании ролевой модели в политике предоставления доступа, а также темам compliance, управ-

Пришло некоторое понимание того, какие задачи всё-таки можно успешно решать с помощью систем управления доступом, появились первые квалифицированные специалисты, имевшие реальный опыт внедрения и эксплуатации таких систем

ления рисками и управления SOD-конфликтами. Такое изменение в понимании назначения и ценности этих систем для современного предприятия привело к созданию нового класса решений — IGA.

НЕ БЫЛО БЫ СЧАСТЬЯ, ДА НЕСЧАСТЬЕ ПОМОГЛО

Сейчас никто не знает точно, куда пошёл бы рынок IDM, если не кризис 2014 года. События этого периода привели к тому, что активные проекты по внедрению иностранных решений были остановлены и заморожены. Для крупных западных производителей на российском рынке наступили тяжёлые времена. В то же время, экономическая обстановка в стране позволила выйти на рынок обновлённым решениям класса IDM от российских производителей. Первым отечественным IDM-решением становится Avanpost IDM компании Аванпост. За ним последовали «КУБ» от компании Траст-Верс и SolarInRights компании Solar Security (сейчас Ростелеком — Solar).

2014 год можно считать поворотным в части понимания и трансформации IDM-проектов. Российские решения, разработанные с пониманием специфики ведения бизнеса в нашей стране, выигрывали в цене перед западными продуктами. Они были ориентированы на потребности конечных потребителей и лучше интегрировались с различным инфраструктурным и прикладным ПО.

Западные производители вынужденно попытались адаптироваться под новые условия российского рынка. Возможно, они смогли бы перестроиться, но курс на импортозамещение ИТ, возникший в 2015 году, стал ещё одной большой ложкой дёгтя для иностранных производителей систем IDM/IGA.

Изменившаяся внутренняя обстановка диктовала свои правила. Проекты должны были стать проще, реализовываться быстрее и дешевле. Отечественные производители без проблем встроились в эту концепцию, что позволило им выйти на уровень внедрения в нижнем сегменте крупного бизнеса. Интеграторы, у которых опыт внедрения систем IDM уже измерялся годами, без

Стало заметно, что интерес к отечественным продуктам проявляется не только со стороны компаний государственного сектора, попавшего под политику импортозамещения ИТ, но и со стороны коммерческих организаций

труда смогли предлагать свои услуги более мелким компаниям. Тем более, что российский рынок к этому времени получил возможность выбора IDM-решения.

Внутренние и внешние политические и экономические изменения привели к тому, что рынок IDM претерпел серьёзную трансформацию.

ЗАКАТ ИЛИ РАССВЕТ?

2018 год стал ещё одной значимой вехой в становлении рынка IDM в России. Первые крупные внедрения, начатые в 2014–2016 гг, были завершены. Появился проверенный временем и практикой работы успешный опыт создания и использования систем управления доступом на базе IDM-платформ. Российские решения созрели для внедрения в крупных компаниях. Примером может являться использование Avanpost IDM в Федеральной Налоговой службе и Россельхозбанке, RS-IAM в Пенсионном Фонде РФ. Также стало заметно, что интерес к отечественным продуктам проявляется не только со стороны компаний государственного сектора, попавшего под политику импортозамещения ИТ, но и со стороны коммерческих организаций. Примером такого внедрения является ПАО «Северсталь», где Avanpost IDM успешно вошёл в ИТ-инфраструктуру компании, став её неотъемлемой частью.

Первичные функции IDM-продукта реализованы и прошли многолетнюю обкатку на стороне заказчика. Российские вендоры сфокусировали внимание на расширении функционала продуктов.

Экономическая и геополитическая обстановка вокруг России говорит о том, что пора в как можно большей степени избавляться от западного влияния. При этом цена на разработку и

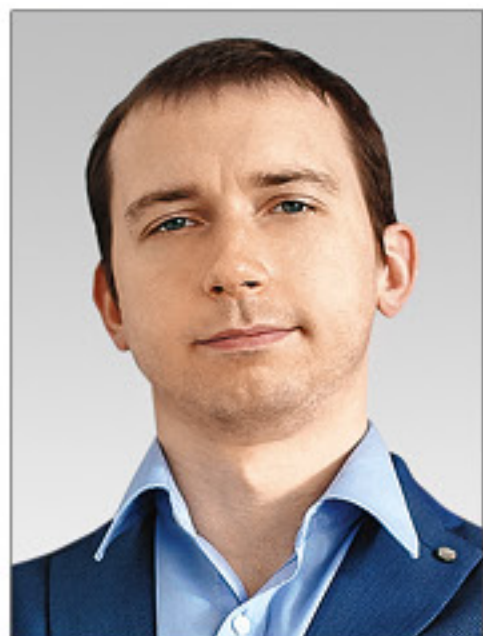
внедрение отечественного ПО не должна зависеть от изменений на мировой арене.

Какие варианты развития событий в ближайший год наиболее вероятны?

Компании, которые защищены от санкций, где всё ещё используется западные IDM-продукты, должны будут пересмотреть подход к развитию систем, построенных на базе подобных решений. Сейчас рынок предлагает много новых гибких лёгких продуктов, не требующих титанических ресурсов на внедрение и сопровождение, и при этом соответствующих политике импортозамещения.

Компании, попавшие под ограничения, активно переходят с западных IDM-систем на новые отечественные. Причём времени на смену технологической платформы тратится существенно меньше, чем десяток лет назад. Да и стоимость владения новыми российскими продуктами более привлекательна в сравнении с импортными системами.

Подводя итоги, зададимся вопросом, что же будет с рынком IDM в России? Мы всё понимаем, где и по каким правилам в контексте политики импортозамещения будут сосредоточены финансовые потоки. Но пока однозначно не ясно, как эти потоки будут двигаться: то ли они пойдут на конкретную разработку, ориентированную на конечного заказчика, то ли они будут направлены в сторону интеграторов (госкомпаний), на откуп которым будет отдано право выбора стратегии по развитию задач по управлению доступом. Как будут развиваться события отечественного рынка IDM-решений, мы увидим в ближайшие годы.



Павел КОРОСТЕЛЕВ
руководитель отдела
продвижения
продуктов компании
«Код безопасности»

VGATE:

КАК ЗАЩИТИТЬ ЧАСТНОЕ ОБЛАКО ОТ РИСКОВ?

В «СЛЕПОЙ ЗОНЕ» ТРАДИЦИОННЫХ СРЕДСТВ ЗАЩИТЫ

За последние годы в концепции построения ИТ-инфраструктуры произошли значительные изменения. Одно из них — это повсеместное внедрение средств виртуализации. Благодаря такому подходу организация получает возможность экономии средств за счёт отказа от дорогостоящего оборудования, а также гибкость и отказоустойчивость. Но использование средств виртуализации — это ещё и дополнительные риски информационной безопасности.

КЛЮЧЕВАЯ ТОЧКА

Среда виртуализации — это ключевая точка в частном облаке. Значительная часть организаций, независимо от их размера и масштабов бизнеса, виртуализовала свою серверную инфраструктуру более чем на 50 %. В этом случае вся инфраструктура получает дополнительный уровень абстракции — кластер гипервизоров, который объединяет ресурсы нескольких физических серверов и выдаёт из получившегося пула ресурсы для виртуальных машин. Он позволяет значительно повысить гибкость и скорость изменений в инфраструктуре.

Однако такой подход создаёт несколько проблем:

1. Гипервизор находится в «слепой зоне» традиционных средств защиты, они работают либо на уровне виртуальной машины, либо на уровне сети. Даже если решение позиционируется как средство защиты облаков, оно обеспечивает защиту только внутри виртуальных машин и поможет, если виртуальную машину атакуют через сеть.

Если же злоумышленник украдёт учётные данные администратора и атакует виртуальную машину «снизу», со стороны гипервизора, или скопирует файл с виртуальной машиной, он уйдёт незамеченным.

2. Традиционные межсетевые экраны плохо приспособлены к защите виртуализованных сетей: они меняются намного чаще физических, постоянно требуется корректировать существующие правила фильтрации. Помимо прочего, они предполагают, что физическое устройство заменяется на виртуальное. Этот подход не обеспечивает необходимой производительности, уязвим перед вредоносными действиями администратора виртуальной среды и создаёт высокую нагрузку на администратора.

3. Если система, развёрнутая в виртуальной среде, подпадает под требования законодательства в области защиты информации, то организация должна нанять специалиста по безопасности именно виртуальной среды для проведения регулярных аудитов безопасности, что не всегда возможно в условиях кадрового дефицита. Нарушение требований в области безопасности чревато взысканиями со стороны регуляторов.

БОЙСЯ АДМИНИСТРАТОРА!

По данным исследования «Защита виртуальной инфраструктуры», проведённого компанией «Код безопасности», две трети компаний опасаются ущерба, нанесённого действиями администратора виртуальной среды, причём как умышленными, так и неумышленными.

Для решения перечисленных проблем организации часто разделяют вир-

туальные машины с разным уровнем критичности на несколько независимых гипервизоров. Это повышает уровень безопасности: в случае компрометации одного сегмента остальные не подвергаются угрозе. Однако это снижает эффект от виртуализации инфраструктуры в целом.

Если заказчик консолидирует в рамках одной среды виртуальные машины с разным уровнем критичности, то необходимо обеспечить дополнительные меры безопасности. Среди ключевых факторов обеспечения безопасности виртуальной среды участники исследования «Кода безопасности» назвали разграничение доступа внутри виртуальной инфраструктуры, защиту данных виртуальных машин, мониторинг событий безопасности и антивирусную защиту.

ТРИ ВОЛШЕБНЫХ АПЕЛЬСИНА

Для эффективной защиты виртуальной инфраструктуры необходимо выполнить следующие действия:

1. Реализовать сегментацию виртуализованной сети, что позволит защитить её части от воздействия друг на друга. При этом политика безопасности виртуального межсетевого экрана должна автоматически подстраиваться под добавление новых виртуальных машин, только в этом случае подсистема безопасности не будет сдерживать скорость изменений в гибкой и быстро меняющейся среде. Также политика фильтрации должна применяться даже в случае миграции виртуальной машины на соседний физический сервер.

2. Контролировать активность администраторов виртуальной сети, причём журнал аудита их действий должен храниться не в самой виртуальной инфраструктуре, а отдельно. Доступ должен предоставляться по принципу минимально необходимых привилегий. Попытки несанкционированного обхода должны фиксироваться, а журнал этих попыток должен храниться отдельно от остальных журналов.

3. В автоматическом режиме настраивать и контролировать выполнение требований законодательства и лучших практик в области защиты среды виртуализации. Причём заказчик должен иметь возможность изменять шаблоны настроек с учётом специфики своей инфраструктуры.

ПО СОВЕТУ GARTNER

Аналитики Gartner выделяют все средства защиты среды виртуализации и облаков в класс продуктов Cloud Workload Protection Platform — средства защиты облачных серверов. В рамках этого класса продукты делятся на два типа:

♦ Защита «Data plane». Это средства для защиты собственно виртуальных машин. Традиционные антивирусы, решения класса Application Whitelisting и т.д.

♦ Защита «Control Plane». Это средства защиты гипервизора, контроля доступа администратора, контроля настроек сети и хранилища данных. Средства этого класса аналитики Gartner называют Cloud Security Posture Management (CSPM).

В своём отчёте Market Guide for Cloud Workload Protection Platform Gartner отмечает, что считает обязательным использование продуктов класса CSPM для масштабных внедрений.

Разработанный компанией «Код безопасности» продукт vGate — это первое в России решение класса Cloud Security Posture Management (CSPM).

КОМПЛЕКСНАЯ ЗАЩИТА

Внедрение vGate позволит надёжно разграничить виртуальные машины с разным уровнем критичности, снизить риски потери данных в результате случайных или намеренных действий администратора и сэкономить время администратора при аудите виртуальной



Рисунок 1

инфраструктуры на соответствие требованиям безопасности.

vGate необходим для комплексной защиты среды виртуализации на базе VMware vSphere и MS Hyper-V. Комплексная защита включает в себя три направления (рисунок 1):

- ♦ защита виртуализованной сети;
- ♦ контроль доступа администраторов к конфиденциальным данным на виртуальной машине;
- ♦ автоматическая настройка и контроль соответствия виртуальной среды требованиям в области ИБ.

ПОЗНАКОМИМСЯ ПОБЛИЖЕ

vGate состоит из нескольких компонентов:

1. Сервер авторизации, расположенный между администратором виртуальной среды и системой управления. Он необходим для независимого аудита действий администратора, а также для запрета несанкционированных действий.

2. Агент на рабочем месте администратора виртуальной среды, который обеспечивает дополнительный уровень аутентификации администратора.

3. Агент в системе управления VMware vCenter или MS System Center Virtual Machine Manager, который кон-

тролирует корректность операций в виртуальной инфраструктуре.

4. Агент для хоста гипервизора, который контролирует настройки непосредственно гипервизора. Сюда же входит модуль межсетевого экрана виртуальных машин, он перехватывает весь сетевой трафик до того, как тот попадёт в виртуальный свитч, а также проверяет, разрешено ли движение этого трафика.

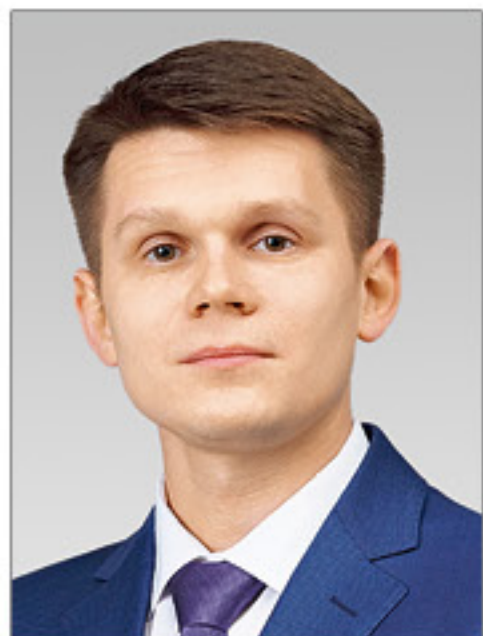
5. Агент на рабочем месте администратора безопасности. Он необходим для централизованного управления vGate и настройки системы защиты.

6. Сервер мониторинга для сбора и корреляции событий виртуальной среды.

Важным преимуществом vGate является то, что для решения своих задач продукт не требует развёртывания агентов на каждой виртуальной машине.

* * *

Внедрение vGate позволяет повысить уровень защищённости виртуальной инфраструктуры, застраховаться от ошибок или вредоносных действий администраторов, а также обеспечить эффективную защиту виртуализованных сетей.



Леонид БОНДАРЕНКО
директор департамента поддержки продаж
ООО «Сикрет Технолоджис»

УТЕЧКИ ДАННЫХ

ФОКУС НА БУМАЖНЫЕ ДОКУМЕНТЫ

ОТЧЁТ ПОДТВЕРЖДАЕТ

Аналитический центр компании InfoWatch ежегодно представляет отчёт об исследовании инцидентов, связанных с компрометацией информации ограниченного доступа, зафиксированных в российских коммерческих и некоммерческих компаниях, государственных органах и организациях — «Утечки данных. Россия. 2017 год» (https://www.infowatch.ru/report_ru2017).

Данный отчёт подтверждает, что инциденты утечек информации происходят в любых компаниях вне зависимости от отрасли: банки и финансы, медицина, торговля, HoReCa, высокие технологии, промышленность и транспорт, госорганы, силовые структуры, образование, муниципальные учреждения.

Также в этом отчёте приведена статистика распределения утечек по каналам. Она говорит, что значительную часть (36%) утечек составляют утечки бумажных документов:

«В то же время резко выросла доля утечек бумажных документов — с 25,7% до 36%. На наш взгляд, повышение роли этого канала, прежде всего, говорит о вопиюще слабом контроле документооборота в компаниях. Ти-

пичная «бумажная» утечка в России — выброс на свалку архива документов с персональными данными. Практически ежедневно появляются сообщения о подобном «мусоре».

Данных за 2018 год ещё нет, но как видно из выдержки отчёта, процент утечек информации на бумажных носителях увеличивается.

КЛАССИЧЕСКИЙ ПОДХОД

Классический и устоявшийся на сегодняшний день подход детектирования и расследования инцидентов утечек информации — внедрение систем контроля утечек информации (Data Loss Prevention, DLP). Но DLP-системы «заточены» на детектирование и предотвращение утечек информации в цифровом виде и имеют для того богатый арсенал, а вот для бумажных документов нужны другие методы и подходы.

Первое, что необходимо сделать — это обеспечить механизм распечатывания документов сотруднику «в руки», а не когда он сидит за своим рабочим местом, а до принтерной комнаты ещё нужно пройти, и в это время распечатанные документы остаются неконтролируемыми.

Чтобы документы распечатались в момент непосредственного нахождения пользователя возле устройства, применяются специализированные системы контроля печати (Secure Managed Printing) с функционалом Pull Printring. При этом происходит задержка печати до того момента, пока пользователь не подойдёт к устройству печати и не предъявит аутентификационные данные в виде персональной смарт-карты, пин-кода, пароля, карты на мобильном телефоне с NFC-чипом. События печати логируются в журнале.

ДОБАВЛЕНИЕ МЕТАДАННЫХ

Но даже в этом случае не достигается необходимого уровня контроля бумажных документов, ведь специфика бумажного документа в отличие от электронного в том, что у бумажного документа нет метаданных, по которым можно отследить кем конкретно этот документ создавался (распечатывался) и кто допустил/совершил утечку бумажного документа.

Соответственно, чтобы обеспечить механизмы контроля бумажных документов и расследования инцидентов, в бумажный документ нужно добавлять метаданные, которые позволят определить кто, когда и где печатал конкретный экземпляр.

Самый очевидный способ — маркирование. Нанесение в определённую область документа данных. Эти данные могут быть нанесены в явном виде, чтобы все могли их прочитать, или в зашифрованном, чтобы содержание гри-

DLP-системы «заточены» на детектирование и предотвращение утечек информации в цифровом виде и имеют для того богатый арсенал, а вот для бумажных документов нужны другие методы и подходы

фа было доступно только, например, службе безопасности. Они могут выглядеть как текстовая строка, штрих-код или QR-код.

Но у этого метода есть недостаток — от такой метки можно избавиться: отрезать её, закрасить, или, если документ несанкционированно фотографируется, просто оставить за рамками фотографии.

УНИКАЛИЗАЦИЯ ДОКУМЕНТА

Соответственно, нужно маркировать документ скрыто, делать каждый конкретный экземпляр бумажного документа уникальным так, чтобы это не было заметно человеку, но распознавалось при разборе инцидента. И уникализацию документа нужно производить равномерно, чтобы нельзя было избавиться от уникальной части или можно было определить конкретный экземпляр по части документа или страницы. Для этого нужно вносить уникальные для каждого экземпляра выводимого документа изменения в расположение элементов текста, и такие изменения не должны изменять или нарушать структуру документа.

При этом качество уникализации и распознавания уникального документа должно позволять расследовать инциденты не только по оригиналу, но и по сканам, копиям или фотографиям, которые могут быть сделаны с более низким качеством, неровно, частично, с помехами, быть грязными или мятыми и так далее.

К алгоритмам уникализации также должны предъявляться строгие требования, так как в организациях с большим объёмом бумажного документооборота количество экземпляров одного и того же документа может быть очень велико, и алгоритмы должны предоставлять возможность создавать большое количество уникальных копий одного документа. И эти уникальные копии должны отличаться, чтобы можно было с большой долей вероятности определить принадлежность этой уникальной копии конкретному человеку.

Также не стоит забывать и о стоимости применения защитных мер. Ведь если хранить в системе каждую уни-

кальную копию каждого документа, то стоимость дисковых массивов, которые понадобятся для хранения этих копий, в течение продолжительного периода времени, необходимого для расследования инцидента, будет достаточно дорогим. Значит в системе уникализации должны храниться не сами копии, а алгоритмы создания конкретной копии с привязкой копии к времени её создания и конкретному человеку, который эту копию получает.

Всё что описано выше в части уникализации печатной копии документов может быть применимо и для электронного документа, который, например, выводится в системе электронного документооборота (СЭД), когда злоумышленник может сделать скриншот экрана или экран сфотографировать.

КОНКРЕТНЫЕ РЕШЕНИЯ

Компания ООО «Сикрет технолджис» ведёт разработку собственных решений, выполняющих функции как контроля печати, так и уникализации документов с учётом вышеописанной специфики, требований и задач по повышению уровня информационной безопасности.

Так в части уникализации разработано решение, базирующееся на алгоритме, который разделяет текст, содержащийся в документе на блоки, внутри которых производятся горизонтальные и вертикальные сдвиги элементов текста, позволяющие сделать уникальный цифровой отпечаток для конкретной копии документа. Результаты уникализации с применением нашего решения визуально незаметны или минимально заметны при просмотре документа без использования инструментов анализа изображений.

ТРИ ЭТАПА

Весь процесс контроля утечек с применением алгоритмов уникализации можно разделить на 3 этапа:

1. загрузка оригинала документа в систему;
2. непосредственно уникализация документа;
3. расследование инцидента (по бумажному документу, скану, фотографии, части документа или страницы).

Загрузка оригинала документа в систему может производиться автоматически при печати, выводе документа в СЭД или вручную. После загрузки документ обрабатывается и для него просчитывается пул формул уникализации.

На втором шаге к выводимому документу применяются формулы уникализации, результат применения формулы записывается в систему вместе с метками времени и информации о пользователе, которому была выдана уникальная копия документа, и непосредственно выдача этой копии на печать или в СЭД.

Расследовать инцидент можно имея бумажную или электронную уникальную копию, фотографию или скан этой копии. Скан или фотография загружается в систему, далее при помощи специальных техник компьютерного зрения производится восстановление нормального состояния документа (как описано ранее исходник может быть ненадлежащего качества), производится поиск оригинала документа и предоставление списка подходящих формул уникализации с выводом процента совпадения и информации о времени вывода и пользователе, которому была выдана уникальная копия документа. Это позволяет определить, кто допустил утечку (ведь случайные утечки не менее опасны и могут нанести не меньший ущерб, чем преднамеренные) и является ли инцидент работой злоумышленника.

* * *

Применение систем уникализации документов и контроля печати позволит снизить вероятность и ущерб от утечек информации по каналам, которые традиционные и широко известные средства закрыть не могут.

Решения данного класса пока не заняли должного места в системах корпоративной безопасности, но игнорировать существенные каналы утечки информации нельзя. Ведь только комплекс мер позволит обеспечить должный уровень информационной безопасности, и для практически каждой угрозы есть актуальные варианты противодействия.

**Роман КОСИЧКИН**

ведущий эксперт Департамента
комплаенса финансово-кредитной
сферы компании «ЦИБИТ»

АУДИТ КАК СПОСОБ ПОВЫШЕНИЯ ДОВЕРИЯ

ТРИ ОТВЕТА НА САМЫЕ ВАЖНЫЕ ДЛЯ ИБ БАНКА ВОПРОСЫ

В последнее время Банк России как один из регуляторов в кредитно-финансовой сфере принял ряд документов, определяющих критерии правильности построения систем ИБ и управления ими. Для проверки соответствия этим критериям в определённых случаях требуется привлечение внешних фирм-аудиторов. Однако, по мнению многих кредитных организаций, аудит является очень затратным мероприятием, как с финансовой точки зрения, так и по использованию других ресурсов. А есть ли для банков польза от аудита помимо формального соответствия требованиям Банка России?

ВАЖНОСТЬ ИБ ДЛЯ БАНКА

Банки являются краеугольным камнем кредитно-финансовой системы государства и важнейшим финансовым институтом современного общества. В связи с этим на них возлагаются особые требования к обеспечению ИБ.

Автоматизированные банковские системы (АБС) содержат конфиден-

циальную информацию о клиентах банка, состоянии их счетов и проведении различных финансовых операций. В процессе хранения и обработки информации в АБС, ее передачи по линиям связи важно, чтобы она не попала в руки злоумышленников, не была изменена или оказалась недоступной легитимным пользователям. При этом следует соблюсти баланс между интересами бизнеса и требованиями ИБ. С одной стороны, нужно обеспечить безопасность данных, но, в то же время, без быстрого и своевременного обмена и обработки информации банковская система не может функционировать правильно.

УГРОЗЫ ДЛЯ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Основной и главной угрозой ИБ по-прежнему остаётся человеческий фактор. Согласно статистике, больше половины правонарушений приходится на сотрудников банка, то есть на тех, кто непосредственно имеет доступ к данным.

Кроме этого, существуют и технические угрозы ИБ банков, к которым относятся взломы информационных систем лицами, не имеющими к ним прямого доступа, такими как криминальные сообщества или конкуренты.

Опасность и угрозу для программного обеспечения могут представлять также различные компьютерные вирусы, программные закладки, которые способны нарушить доступность данных, а также привести к потере конфиденциальности.

КРИТЕРИИ ОЦЕНКИ ИБ ДЛЯ БАНКОВ

До момента появления отечественных отраслевых стандартов ИБ банки управляли безопасностью, основываясь на положениях внутренних нормативных документов. Начиная с середины 2000-х годов Банк России начал принимать документы, определяющие критерии безопасности информационных систем финансовых организаций. В настоящее время требования к ИБ организаций кредитно-финансовой сферы установлены, в том числе, следующими документами Банка России или созданными при его участии:

♦ Положение от 09.06.2012 №382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации

По мнению многих кредитных организаций, аудит является очень затратным мероприятием, как с финансовой точки зрения, так и по использованию других ресурсов

при осуществлении переводов денежных средств» (с изменениями);

- ♦ СТО БР ИББС-1.0–2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации»;

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

В целом данные документы можно рассматривать как руководства, позволяющие менеджменту банка понять, насколько полно мероприятия по обеспечению ИБ охватывают различные аспекты деятельности банка.

ЧТО ТАКОЕ АУДИТ И В ЧЁМ ЕГО ТРУДНОСТЬ?

Чтобы понять, насколько полно выполняются требования руководящих документов, финансовой организации следует провести оценку соответствия, называемую также аудитом (в нашем случае аудит ИБ). Основная задача аудита — объективно оценить текущее состояние ИБ финансовой компании, а также её соответствие установленным критериям.

По отношению к области проверки аудиты подразделяются на внутренний (самооценку) и внешний.

Самооценка информационной безопасности; самооценка ИБ: Оценка соответствия информационной безопасности, выполняемая работниками организации банковской сферы РФ.

Аудит информационной безопасности; аудит ИБ: Независимая оценка соответствия ИБ, выполняемая работниками организации, являющейся внешней по отношению к организации банковской сферы РФ, допускающая возможность формирования профессионального аудиторского суждения о состоянии ИБ организации банковской сферы РФ.

Самооценка ИБ чаще всего проводится структурным подразделением банка, отвечающим за защиту информации, — службой безопасности или IT-департаментом. Данный вид аудита довольно дешёв, поскольку его проведение можно вменить в обязанности, включить в должностную инструкцию сотрудников. Однако у самооценки есть

и недостатки. Главный из них — это субъективность полученных данных, поэтому термин «аудит» применять здесь не совсем правильно.

Внешний аудит проводится командой специалистов независимой компании. Аудиторы могут использовать опыт и знания, полученные во время проведения предыдущих оценок соответствия, и поэтому выполняют работу эффективнее и быстрее.

К недостаткам внешнего аудита относятся денежные траты, значительно превышающие расходы на самооценку, а также чрезмерно большие затраты человеческих ресурсов на помощь при его проведении.

В большинстве случаев банки отказываются от аудита из-за непонимания реальной необходимости услуги. Большинство компаний не готовы отдавать немалые деньги за «всего лишь» проверку на соответствие требованиям.

В ЧЁМ ЖЕ ПОЛЬЗА ОТ АУДИТА?

Несмотря на все трудности и опасения по поводу проведения внешней оценки соответствия результаты квалифицированно выполненного аудита ИБ позволяют построить оптимальную по эффективности и затратам корпоративную систему защиты, адекватную текущим задачам и целям бизнеса.

Отзывы банков, прошедших процедуру аудита на соответствие стандарту и положениям Банка России, говорят о том, что после проведения данных работ не только повышается уровень доверия и лояльности со стороны ЦБ, клиентов и партнёров, но и формируются ответы на самые важные для обеспечения безопасности деятельности банка вопросы:

- ♦ насколько хорошо построена служба ИБ, достаточно ли её ресурсное обеспечение;

- ♦ где находятся слабые места в существующей системе защиты;

- ♦ что нужно сделать, чтобы подразделение ИБ банка своевременно реагировало на инциденты и возможные угрозы.

Результаты аудита, документально зафиксированные в отчёте, являются катализатором для принятия кадровых,

организационных или технических решений в отношении ИБ.

Грамотно проведённый аудит может помочь уменьшить и финансовые потери, которые могли бы быть следствием инцидентов ИБ — простой оборудования, потерю информации, восстановление работоспособности выведенных из строя узлов, репутационные потери;

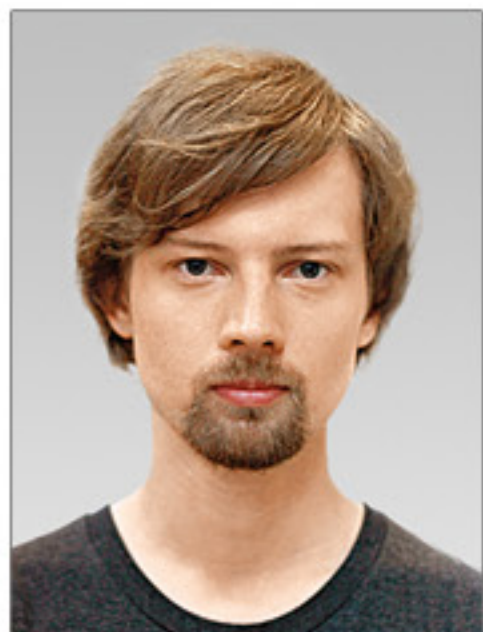
Резюмируя изложенное, можно сказать, что аудит ИБ является сегодня одним из наиболее эффективных инструментов для получения независимой и объективной оценки текущего уровня защищённости банка от различных информационных угроз. Результаты аудита позволяют сформировать системный подход к реализации стратегии развития системы обеспечения информационной безопасности кредитно-финансовой организации. Таким образом, оценка соответствия ИБ является не пустой тратой денег, а вложением в стабильность и будущее развитие.

РЕКОМЕНДАЦИИ ЭКСПЕРТОВ

Как уже отмечалось, по итогам аудита документально фиксируются полученные результаты соответствия заданным критериям. Формально на этом работа аудиторов заканчивается. Но для банка очень важно не просто оценить степень соответствия требованиям, но и понять какие действия в управленческом, нормативном и техническом плане следует предпринять, чтобы улучшить как свою оценку, так и общее состояние системы ИБ.

* * *

Эксперты компании «ЦИБИТ» по окончании процедуры аудита помогут банку определить, в каком направлении следует приложить усилия, чтобы исправить текущие несоответствия. Специалисты компании, по договорённости с банком, могут поспособствовать и в подготовке системы организационно-распорядительной документации, и в организации системы защиты. Недаром девиз компании «ЦИБИТ»: «Мы помогаем соответствовать требованиям!».



Евгений СМЕРНОВ
научный сотрудник
ООО «ЦРТ-Инновации»



Александр МЕЛЬНИКОВ
научный сотрудник
ООО «ЦРТ-Инновации»,
канд. физ.-мат. наук



Екатерина КРЫЛОВА
технический писатель
ООО «ЦРТ-Инновации»,
канд. филол. наук

РОССИЯНЕ ПОБЕДИЛИ НА ЧЕМПИОНАТЕ МИРА ПО... ИДЕНТИФИКАЦИИ!

ЛУЧШИЕ СИСТЕМЫ РАСПОЗНАВАНИЯ ЛИЦ РАЗЛИЧАЛИ
ДВОЙНИКОВ И ОПОЗНАВАЛИ ЗАМАСКИРОВАННЫЕ ЛИЦА

Некотрые биометрические системы распознавания лиц уже демонстрируют уровень точности распознавания, сопоставимый с человеческим [1]. Причём речь идёт о результатах работы не только в контролируемых условиях (когда степень освещённости, положение лица перед камерой и прочее контролирует сборщик базы данных), но и в неконтролируемых. Неконтролируемыми условиями называются ситуации, близкие к реальной практике применения: когда непредсказуемо меняется уровень освещённости, количество и местоположение людей в кадре, система распознавания используется в скрытом режиме.

Среди неконтролируемых условий бывают ситуации, существенно затрудняющие распознавание лиц. Их принято называть сложными условиями. Алгоритмы распознавания лиц восприимчивы к следующим из них: позе, освещению, выражению лица, возрастным особенностям и т.д. Некоторые из этих явлений хорошо изучены, другим до сих пор уделялось недостаточно вни-

мания. В частности, на распознавании двойников и замаскированных лиц до недавнего времени внимание международного научного сообщества не фокусировалось. Эксперименты проводились некоторыми группами учёных [2, 3, 4, 5], но опыт разных коллективов до 2018 года недостаточно обсуждался на мировом уровне.

Прошедший в 2018 году международный научный конкурс Disguised Faces in the Wild (DFW), организованный в рамках конференции по компьютерному зрению CVPR 2018, продемонстрировал успехи учёных из разных стран в этой области. Успехи российской команды внушительные: модель AEFRL, разработанная учёными из Университета ИТМО и компании «ЦРТ-инновации», заняла первое место по одному протоколу и два вторых по остальным.

Всего в конкурсе приняли участие 11 команд из разных стран, предложив биометрические системы, основанные на нейронных сетях, для участия в трёх протоколах проверки:

- ♦ протокол № 1 Impersonation имитировал попытки выдать двойника за конкретного человека,

- ♦ протокол № 2 Obfuscation имитировал попытки замаскировать лицо,

- ♦ протокол № 3 Overall Performance предполагал подсчёт точности распознавания на всей базе данных.

СЕЛЕБРИТИ, САМОЗВАНЦЫ И ДВОЙНИКИ

Для конкурса DFW была собрана одноимённая база данных, включающая изображения 1000 человек, всего более 11000 изображений. Изображения 400 человек использовались для обучения нейронных сетей, изображения 600 человек — для тестирования готовых систем.

Как видно на рисунке 1, в базе данных фотографии представлены несколькими датасетами:

- ♦ normal face image (выделены серым) — нормальные изображения лица анфас для каждого человека,

- ♦ validation face image (выделены жёлтым) — изображения незамаскированного лица для 903 человек,

- ♦ disguised face image (выделены зелёным) — 1–12 изображений замаскированного лица человека,

- ♦ impersonator face image (выделены голубым) — 1–21 изображение двойни-

ков, то есть людей, которые очень похожи на того или иного человека из базы данных, либо имитируют его внешность.

ЭТАПЫ КОНКУРСА DFW И РЕЗУЛЬТАТЫ

Протокол № 1 Impersonation. Протокол имитировал ситуацию, когда один человек пытается выдать себя за другого. Правила конкурса предусматривали сравнение пар изображений из различных наборов данных.

При этом пары изображений одного человека из наборов normal face image и validation face image признавались позитивными (правильными), а пары, составленные из фотографий impersonator face image и одного из других наборов (normal, validation, disguised face



Рисунок 1. Примеры изображений, вошедших в базу данных DFW. Каждый ряд соответствует одному человеку

image) — признавались негативными (неправильными).

Перед участниками конкурса стояла задача научить систему отличать позитивные пары от негативных в условиях, когда негативные пары — это не просто

фотографии двух разных людей, а такие пары фотографий, на одной из которых человек пытается выдать себя за другого, изображённого на второй фотографии.

Результаты конкурса по первому протоколу представлены в таблице 1.

Название команды	Название модели	Частота верно-положительных срабатываний GAR@1%FAR*	Частота верно-положительных срабатываний GAR@0,1%FAR*	Взвешенное 80–20**	Место в рейтинге
ИТМО, Россия	AEFRL	96.80	57.64	88.96	1
NTU, Тайвань	MiRA-Face	95.46	51.09	86.58	2
UMD, США	UMDNets	94.28	53.27	86.07	3
NEU, США	MEDC	91.26	55.46	84.10	4
ZJU, Китай	OcclusionFace	93.44	46.21	83.99	5
WVU, США	DDRNET	84.20	51.26	77.61	6
WVU, США	WVU_CL	81.34	40.00	73.07	7
Bytedance Inc, Китай	ByteFace	76.97	21.51	65.88	8
MSU, США	DR-GAN	65.21	11.93	54.55	9
CVC/UAB, Испания	LearnedSiamese	57.64	27.73	51.65	10
IIT Ropar, Индия	DisguiseNet	1.34	1.34	1.34	11
Tessellate Imaging, Индия	Tessellation	1.00	0.16	0.83	12

Таблица 1. Результаты конкурса по протоколу проверки № 1 (Impersonation)

*GAR (Genuine Acceptance Rate) — это частота верноположительных срабатываний.

GAR@1% FAR — это GAR при фиксированном значении False Acceptance Rate на уровне 1%. То есть, если в 1% случаев при сравнении двух фотографий будет принято решение, что на них изображён один и тот же человек, хотя на самом деле — два разных, то доля правильно определённых пар, будет равна той, которая указана в таблице (в случае российской команды — 96.80%). Аналогично определяется частота верноположительных срабатываний для FAR = 0.1%: если система ошиблась только в 0.1% при сравнении фотографий, то при таком значении порога модель российских учёных верно определит 57.64% позитивных пар. Чем выше значение GAR@1% FAR и GAR@0,1%FAR, тем лучше система распознаёт лица, тем более устойчивой к атакам имперсонации она является.

** Взвешенное 80–20 — это два значения GAR (для 1% и 0.1%), взвешенные и сложенные в соотношении 80 к 20 следующим способом: (GAR@1%) * 0.8 + (GAR@0.1%) * 0.2. Это взвешенное значение используется для определения победителя, так как одна команда может быть лучше по GAR@0.1% но хуже по GAR@1%, как это случилось с участниками, занявшими второе и третье места по протоколу № 1.

Результаты по двум другим протоколам определяются аналогично.

Название команды	Название модели	Частота верно-положительных срабатываний GAR@1%FAR	Частота верно-положительных срабатываний GAR@ 0,1%FAR	Взвешенное 80-20	Место в рейтинге
NTU, Тайвань	MiRA-Face	90.65	80.56	88.63	1
ИТМО, Россия	AEFRL	87.82	77.06	85.66	2
UMD, США	UMDNets	86.62	74.69	84.23	3
NEU, США	MEDC	81.25	65.14	78.02	4
ZJU, Китай	OcclusionFace	80.45	66.05	77.57	5
WVU, США	WVU_CL	78.77	61.82	75.38	6
MSU, США	DR-GAN	74.56	58.31	71.31	7
Bytedance Inc, Китай	ByteFace	74.45	54.16	70.39	8
WVU, США	DDRNET	71.04	49.28	66.69	9
IIT Ropar, Индия	DisguiseNet	66.32	28.99	58.85	10
CVC/UAB, Испания	LearnedSiamese	37.81	16.95	33.63	11
Tessellate Imaging, Индия	Tessellation	1.23	0.18	1.02	12

Таблица 2. Результаты конкурса по протоколу проверки № 2 (Obfuscation)

Название команды	Название модели	Частота верно-положительных срабатываний GAR@1%FAR	Частота верно-положительных срабатываний GAR@ 0,1%FAR	Взвешенное 80-20	Место в рейтинге
NTU, Тайвань	MiRA-Face	90.62	79.26	88.34	1
ИТМО, Россия	AEFRL	87.90	75.54	85.42	2
UMD, США	UMDNets	86.75	72.90	83.98	3
ZJU, Китай	OcclusionFace	80.80	65.34	77.70	4
NEU, США	MEDC	81.31	63.22	77.69	5
WVU, США	WVU_CL	79.04	60.13	75.25	6
MSU, США	DR-GAN	74.89	57.30	71.37	7
Bytedance Inc, Китай	ByteFace	75.53	54.11	71.25	8
WVU, США	DDRNET	71.43	49.08	66.96	9
IIT Ropar, Индия	DisguiseNet	60.89	23.25	53.36	10
CVC/UAB, Испания	Learned Siamese	39.73	18.79	35.54	11
Tessellate Imaging, Индия	Tessellation	1.23	0.17	1.01	12

Таблица 3. Результаты конкурса по протоколу проверки № 3 (Overall Performance)

Протокол № 2 Obfuscation. Протокол № 2 имитировал ситуацию идентификации персоны, замаскировавшей своё лицо. Протокол предполагал сравнение изображений одного и того же человека в парах, созданных из снимков с замаскированным и открытым лицом. Позитивными парами для этого протокола являлись следующие сочетания снимков:

- ♦ normal face image + disguised face image,
- ♦ validation face image + disguised face image,
- ♦ disguise face image1 + disguised face image2 (под disguised face image1, disguised face image2 подразумевались два разных изображения замаскированного лица одного и того же человека).

Негативные пары были составлены из изображений разных субъектов в подборках изображений normal, validation и disguised. То есть портреты из этих подборок одного человека ставились в пару к normal, validation и disguised-изображениям другого человека (в сочетании, например, normal-normal, validation-disguised, normal-validation и т.п., изображения из категории impersonator не включались в такие подборки).

Результаты конкурса по второму протоколу представлены в таблице 2.

Российская команда заняла второе место с моделью AEFRL.

Протокол № 3 Overall Performance. Протокол № 3 предполагал оценку предложенных алгоритмов для всей базы данных. В качестве негативных и позитивных пар использовались все пары, перечисленные выше в протоколах 1 и 2.

Результаты конкурса по третьему протоколу представлены в таблице 3.

Российская команда с моделью AEFRL заняла второе место.

СЕКРЕТ УСПЕХА РОССИЙСКОЙ КОМАНДЫ

Модель AEFRL (Auxiliary Embeddings Face Representation Learning, т.е. Вспомогательные векторы признаков для обучения представлений лиц) [6], подготовленная научными сотрудниками Университета ИТМО и компании ЦРТ-инновации, вошла в число лидеров во всех трёх этапах конкурса, ни разу не опустившись ниже 2 места.

Чтобы обучить нейронные сети выдавать требуемые векторные представления лиц, нужно подготовить обучающую базу, разработать подходящую архитектуру нейронной сети и провести процесс обучения

Модель AEFRL включает в себя детектор лиц MTCNN и 4 нейронные сети. Эти нейронные сети получают на вход изображения лиц, найденные детектором, и выдают на выходе их векторные представления. Последние могут быть использованы для сравнения лиц между собой и решения задачи верификации и распознавания.

Чтобы обучить нейронные сети выдавать требуемые векторные представления лиц, нужно подготовить обучающую базу, разработать подходящую архитектуру нейронной сети и провести процесс обучения. Именно инновационный подход в организации процесса обучения нейронных сетей и послужил залогом успеха решения от российских разработчиков.

Есть несколько основных способов обучения нейронных сетей для решения задачи получения подходящих векторных представлений лиц. Одним из самых эффективных является обучение с использованием групп примеров: пар, триплетов, квадруплетов и т.п. В этом случае сеть выдаёт векторные представления для каждого из примеров, входящих в группу, находит расстояния между ними в векторном пространстве и корректирует собственные веса так, чтобы эти расстояния в итоге приобрели необходимые характеристики. Расстояния между векторными представлениями фотографий лиц одного человека должны быть маленькими, а расстояния между векторными представлениями фотографий лиц разных людей — большими.

Для того, чтобы нейронная сеть могла научиться работать в сложных условиях, необходимо сформировать группы определённым образом. Эти группы должны содержать сложные комбинации примеров — лица разных, но похожих людей, лицо одного человека, сфотографированное в раз-

ных условиях, замаскированные лица и т.д. Существуют различные способы поиска таких сложных примеров. Некоторые из них основываются на поиске сложных пар классов — таких людей в обучающей базе данных, которые похожи друг на друга. Другие предполагают обучение с помощью параллельной обработки больших пакетов данных, внутри которых и производится поиск сложных примеров. Эти методы имеют свои недостатки — невозможно выбрать сложные примеры внутри одного класса, необходимо использовать значительные вычислительные мощности, увеличивается длительность процесса обучения и т.д.

НОВЫЙ МЕТОД

В рамках DFW российская команда предложила новый метод поиска сложных примеров, который лишён некоторых из этих недостатков, а также может использоваться совместно с другими методами. Речь идёт о применении вспомогательных векторов признаков. Перед обучением нейронной сети вспомогательные векторы признаков вычисляются для каждого изображения в обучающей базе. Предполагается, что такие векторы уже в какой-то мере обладают следующим свойством: рассчитанные для двух похожих изображений, в многомерном пространстве они располагаются близко друг к другу, рассчитанные для двух различных изображений, — далеко. В процессе обучения нейронной сети эти векторы признаков нужны для того, чтобы формировать группы обучающих примеров (пары, триплеты и т.п.), используя имеющуюся информацию о сходстве или различии их вспомогательных векторов признаков. Например, фотографии одного человека подбираются в группы

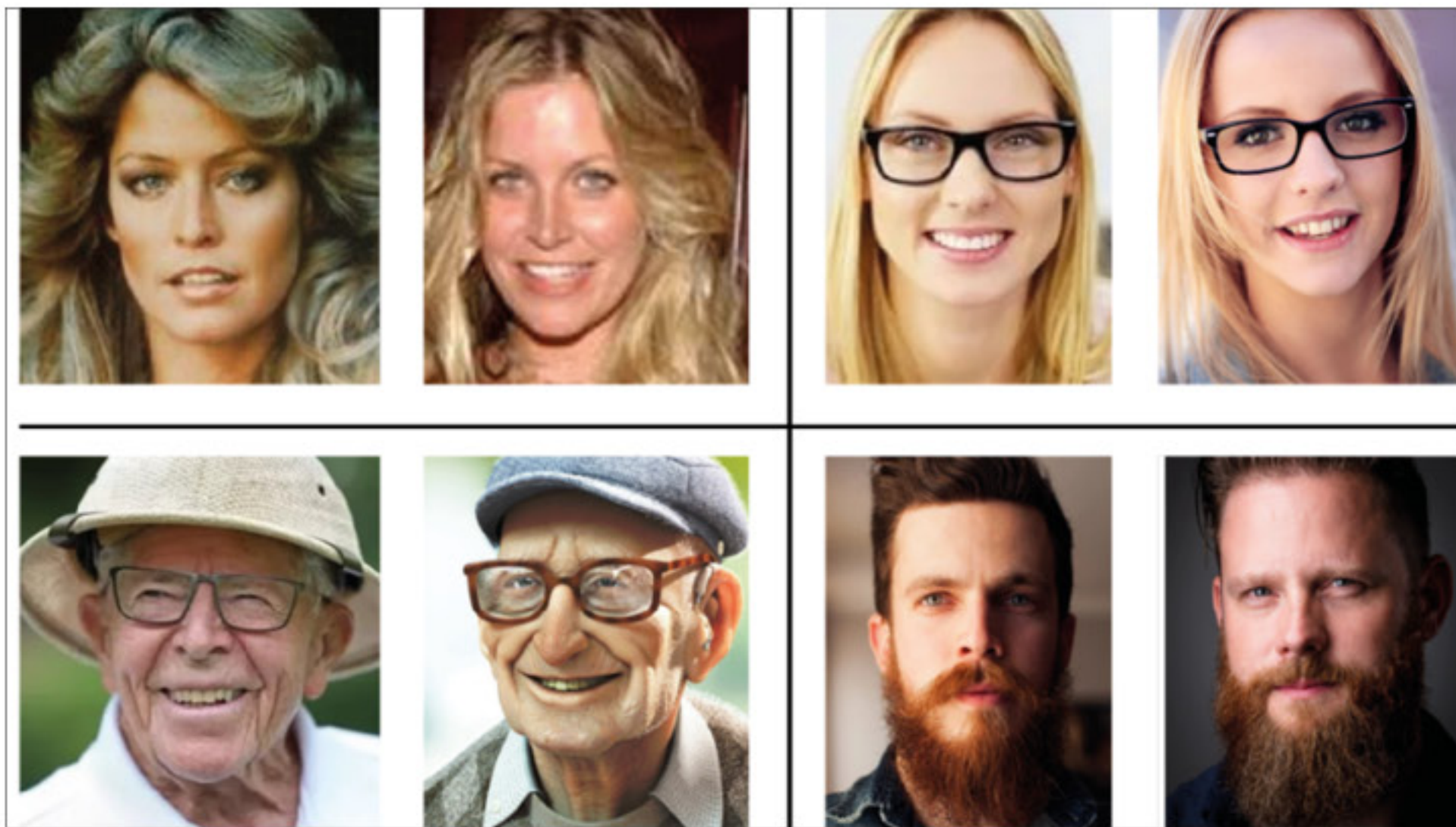


Рисунок 2. Примеры изображений людей с похожими внешними признаками

так, чтобы сформировались сложные позитивные пары (один и тот же человек выглядит по-разному на двух фотографиях), а фотографии разных людей подбираются, чтобы сформировались сложные негативные пары (на двух выбранных фотографиях разные люди очень похожи друг на друга). Использование вспомогательных векторов признаков в процессе обучения помогает нейронной сети лучше ориентироваться в тонкостях различия или сходства человеческих лиц, так что она становится способной демонстрировать очень высокие показатели качества распознавания даже в очень сложных случаях.

Как получить вспомогательные векторы признаков для обучающей базы? Российская команда предложила два способа для решения этой задачи. Во-первых, получить их с помощью нейронной сети, обученной задаче классификации внешних атрибутов лица — возраста, пола, расы, цвета во-

лос, наличия очков или бороды. Такая нейронная сеть на предпоследнем слое формирует векторы признаков, которые затем используются для решения задачи классификации внешних атрибутов. Эти же векторы признаков могут выступать в качестве вспомогательных векторов признаков для поиска сложных примеров. На рисунке 2 изображены пары людей, обладающие близкими векторами признаков, полученными с помощью нейросети, отвечающей за классификацию внешних атрибутов лиц. Использование подобных пар изображений в процессе обучения помогает нейронной сети обращать меньше внимания на особенности внешнего вида, больше концентрироваться на тех чертах, которые относятся непосредственно к личностям обладателей этих лиц.

Во-вторых, вспомогательные векторы признаков могут быть получены в рамках многоступенчатого процесса обучения [7]. В такой ситуации вспо-

могательные признаки на первой стадии обучения нейронной сети не используются. После окончания первого этапа полученная нейронная сеть вычисляет векторное представление для всех лиц в обучающей базе. Оно и используется на следующем этапе обучения в качестве вспомогательного вектора признаков для поиска сложных примеров. Нейронная сеть продолжает своё обучение с промежуточного состояния, но теперь она имеет информацию о том, какие пары лиц для неё являлись сложными на момент окончания первого этапа обучения, благодаря чему может формировать более сложные пары примеров. Описанный процесс повторяется после каждого этапа обучения.

МИНИ-БАТЧИ

Обучение нейронных сетей для конкурса DFW 2018 проходило следующим образом: на каждой итерации обучения в нейронную сеть подавались мини-батчи — небольшие порции обучающих данных, состоящие из 80 фотографий лиц, по 4 фотографии для одного человека. Строились эти мини-батчи так: в первую очередь, определялось, изображения каких людей попадут в очередной мини-батч. Первые несколько человек выбирались случайно, а последующие — по методу поиска двойников, подробно описанному в [8]. Этот метод предполагает поиск для каждого человека в обучающей базе его двойника — наиболее похожего на него другого человека. Выдаваемые нейронной сетью векторные представления лиц таких пар людей обычно располагаются близко в векторном пространстве, что помогает в поиске сложных пар примеров.

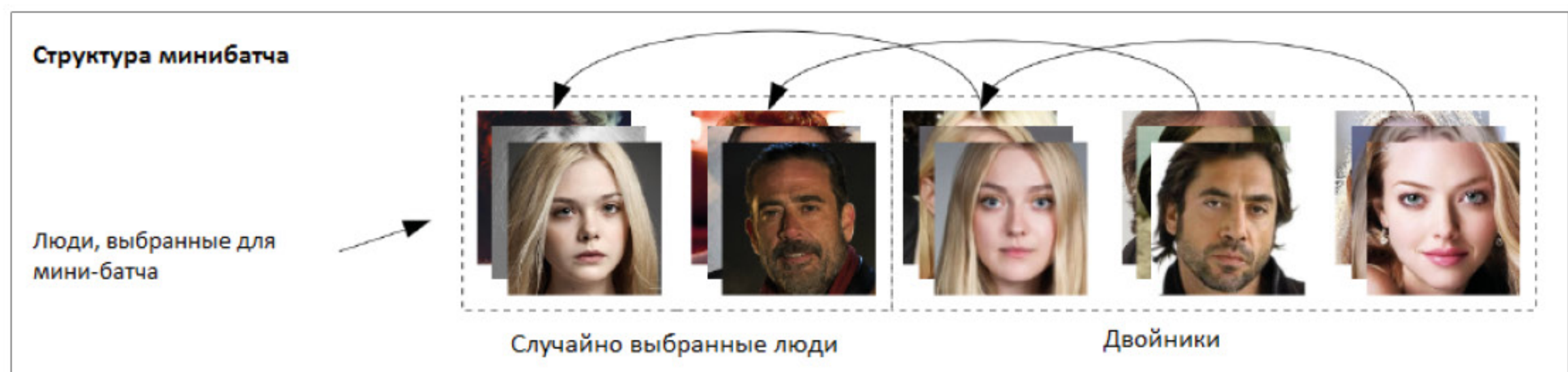


Рисунок 3. Первый этап формирования обучающего мини-батча для нейронной сети: выбор людей

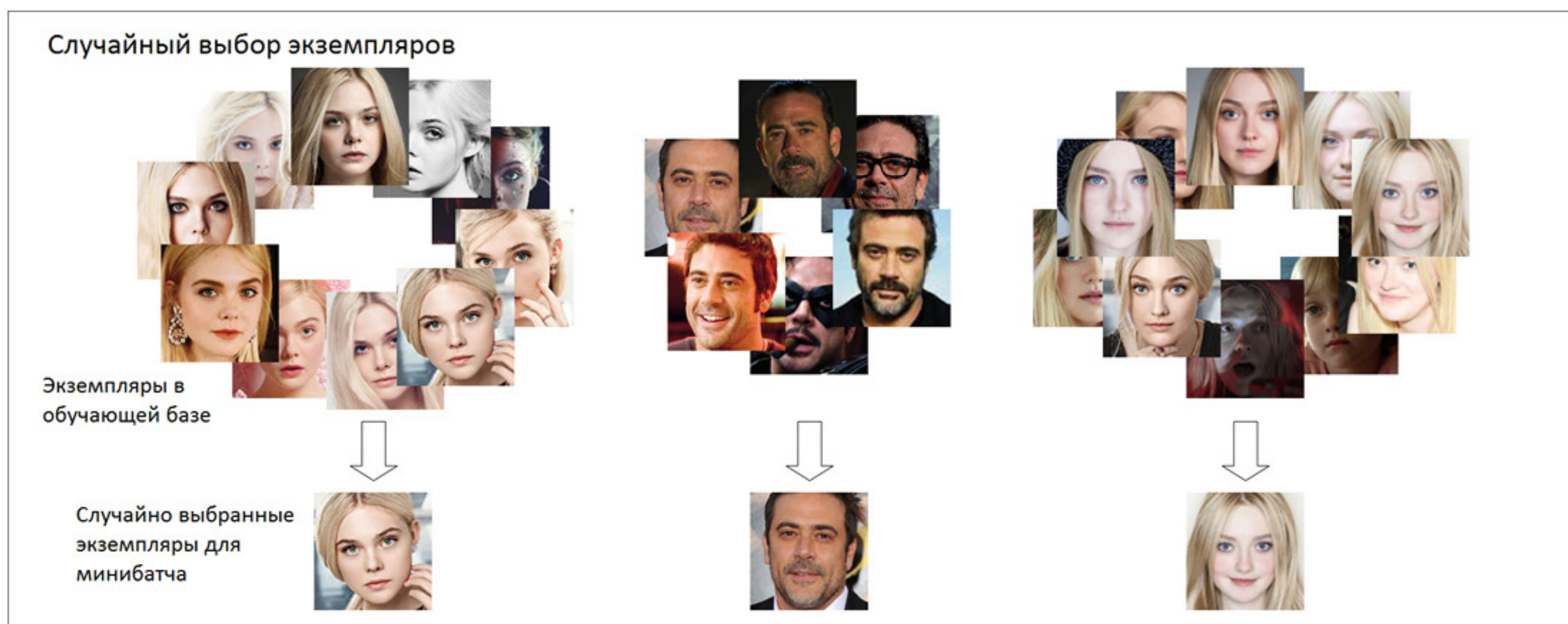


Рисунок 4. Второй этап формирования обучающего мини-батча для нейронной сети: случайный выбор снимков

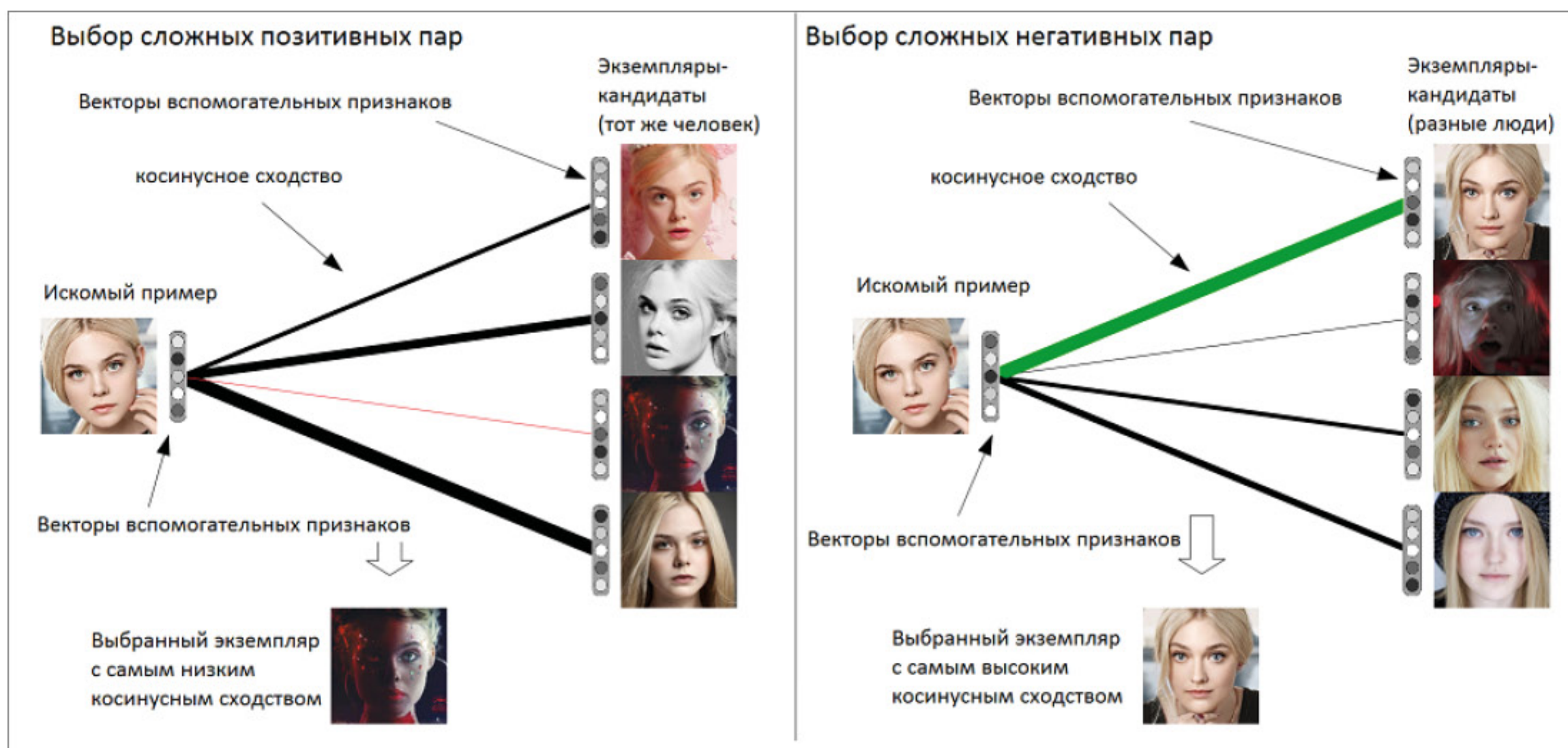


Рисунок 5. Второй этап формирования обучающего мини-батча для нейронной сети: формирование сложных позитивных и сложных негативных пар

На рисунке 3 изображён процесс выбора людей для мини-батча: первые два человека из обучающей базы данных были выбраны случайно, третий подбирался как двойник для первого, четвёртый — как двойник для второго, пятый — как двойник для третьего и т.д.

ВТОРОЙ ЭТАП

Второй этап формирования обучающего мини-батча заключался в том, чтобы выбрать фотографии, которые будут ис-

пользованы в обучении. Для каждого из добавленных в мини-батч людей последовательно выбиралось по несколько фотографий (в решении команды из России — по четыре фотографии на человека). Снимки выбирались одним из следующих способов:

- 1) случайный выбор из всех изображений конкретного человека, имеющих в обучающей базе (см. рисунок 4),
- 2) выбор фотографии, составляющей сложную позитивную пару с одной из

уже помещённых в мини-батч фотографий того же человека,

3) выбор фотографии, составляющей сложную негативную пару с одной из уже помещённых в мини-батч фотографий какого-то другого человека (например, двойника).

Для выбора сложных позитивных и негативных пар использовались вспомогательные векторы признаков. Чтобы найти и добавить в мини-батч сложную позитивную пару, выбиралось одно из уже помещённых в мини-батч изо-

Структура минибатча

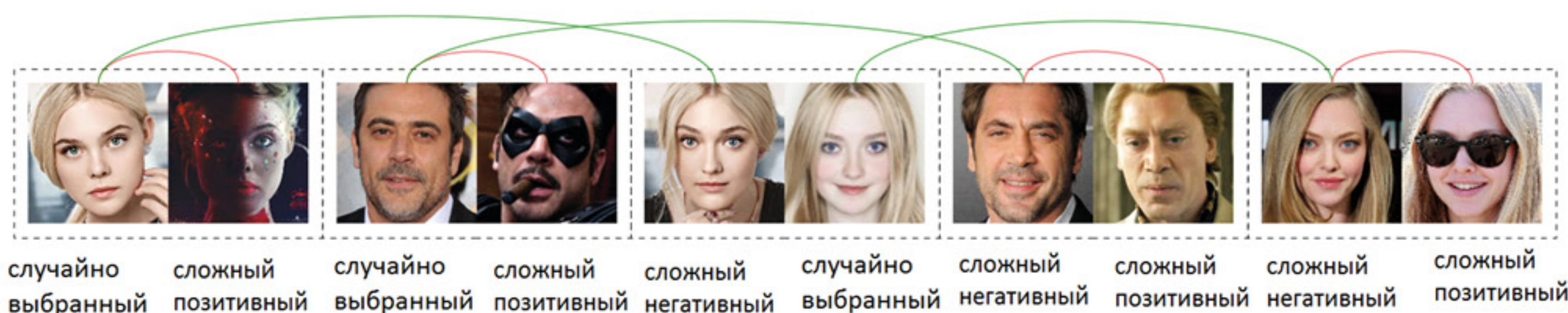


Рисунок 6. Структура обучающего мини-батча

бражений какого-либо человека. Затем подсчитанный для него вектор вспомогательных признаков сравнивался по метрике косинусного сходства с такими же векторами для случайного множества снимков того же человека, находящихся в обучающей базе. Тот снимок, вектор вспомогательных признаков для которого оказывался дальше всех, добавлялся в мини-батч в качестве сложной позитивной пары к уже имеющемуся там изображению (см. рисунок 5).

Чтобы найти и добавить в мини-батч сложную негативную пару, выбирался

один из уже помещённых в мини-батч портретов какого-либо человека, брался рассчитанный для него вектор вспомогательных признаков, а затем сравнивался по косинусной метрике близости с векторами вспомогательных признаков для случайного множества снимков, но теперь уже другого человека из обучающей базы. Тот снимок, вектор вспомогательных признаков для которого оказывался ближе остальных, добавлялся в мини-батч в качестве сложной негативной пары к уже имеющемуся там изображению (см. рисунок 5).

В результате, с помощью вышеуказанных алгоритмов формируются такие обучающие мини-батчи, в которых содержится достаточное количество как сложных позитивных, так и сложных негативных пар (см. рисунок 6).

Например, первая фотография в мини-батче на рисунке 6 составляет со второй фотографией сложную позитивную пару (две фотографии одного человека, непохожие друг на друга) и сложную негативную пару с пятой фотографией (две фотографии разных людей, похожие друг на друга). Третья фотография также имеет свои сложные пары: негативную (седьмое фото) и позитивную (четвёртое фото) и т.д.

Подготовленные описанным способом мини-батчи были использованы для обучения нейронных сетей, представленных российской командой на конкурс. Результатом стали призовые места по всем трём протоколам.

* * *

Данный инновационный метод использования обучающих данных для систем распознавания лиц уже лёг в основу конкретных продуктов для лицевой биометрии, обеспечив высокое качество их работы. Качество это обеспечивает низкий процент ошибок распознавания, даже если в камеру попадает кто-то в очках, с бородой, в шляпе или в гриме. Различные средства маскировки и имперсонации, когда-то способные взломать систему лицевой биометрии, сегодня перестают работать, а значит, у злоумышленников не остаётся шанса выдать себя за другого или спрятаться от системы безопасности.

ЛИТЕРАТУРА

1. Taigman, Y., Yang, M., Ranzato, M., 'aurelio & Wolf, L. DeepFace: Closing the Gap to Human-Level Performance in Face Verification. in 2014 IEEE Conference on Computer Vision and Pattern Recognition (2014). doi:10.1109/cvpr.2014.220
2. Dhamecha, T. I., Singh, R., Vatsa, M. & Kumar, A. Recognizing Disguised Faces: Human and Machine Evaluation. PLoS One 9, e99212 (2014).
3. Ramanathan, N., Chellappa, R. & Chowdhury, A. K. R. Facial similarity across age disguise illumination and pose. in 2004 International Conference on Image Processing, 2004. ICIP '04. doi:10.1109/icip.2004.1421474
4. Righi, G., Peissig, J. J. & Tarr, M. J. Recognizing disguised faces. Vis. cogn. 20, 143–169 (2012).
5. Singh, R., Vatsa, M. & Noore, A. Face recognition with disguise and single gallery images. Image Vis. Comput. 27, 245–257 (2009).
6. Evgeny Smirnov, Aleksandr Melnikov, Andrei Oleinik, Elizaveta Ivanova, Ilya Kalinovskiy, Eugene Luckyanets. Hard Example Mining with Auxiliary Embeddings. Computer Vision and Pattern Recognition Workshops (CVPRW), 2018 IEEE Conference on 37–46 (2018).
7. I. Loshchilov, F. H. Sgdr: stochastic gradient descent with restarts. ICLR (2017).
8. Smirnov, E., Melnikov, A., Novoselov, S., Luckyanets, E. & Lavrentyeva, G. Doppelganger Mining for Face Representation Learning. in 2017 IEEE International Conference on Computer Vision Workshops (ICCVW) (2017). doi:10.1109/iccvw.2017.226



АйТи БАСТИОН

СКДПУ

система контроля
действий
поставщиков
ИТ-услуг



Аутсорсинг:
Выгодно...
НО ОПАСНО!



ФСТЭК РОССИИ
РД НДВ4



МО РФ
РД НДВ2

WWW.IT-BASTION.COM



Александр БОДРИК
обозреватель BIS Journal,
исполнительный директор
ANGARA Professional Assistance (TOP 5-MSSP)

SOC-ФОРУМ 2018

СВЯЗАННЫЕ ОДНОЙ SOC-ЦЕПЬЮ

Четвёртый SOC-Форум выявил неотвратимость реализации функции мониторинга информационной безопасности в организациях. Стало понятно, что другой big idea в информационной безопасности нет, и рынок SOC стал довольно зрелым, чтобы заслужить упоминания куратора крупнейшего SOC страны — руководителя службы ИБ Сбербанка Сергея Лебеда. Его фраза: «На рынке появились услуги мониторинга», — с высоты возможностей Сбербанка означает, что теперь такие услуги есть для всех и каждого — от малого бизнеса до крупнейших корпораций.

ПЛЕНАРНОЕ ЗАСЕДАНИЕ

Форум открылся выступлениями регуляторов — представителей ФСТЭК, ФСБ, ЦБ РФ и Сбербанка. В рамках освещения ситуации с выполнением ФЗ-187 «О безопасности КИИ РФ» заместитель директора ФСТЭК Виталий Лютиков рассказал, что организации пока сосредоточены на этапах инвентаризации и категоризации объектов критической инфраструктуры, в частности, дальше остальных в этом продвинулись организации сектора ТЭК, здравоохранения и ОПК. Есть и отстающие («Например, банки...»), возможно поэтому регулятор подчеркнул, что ФСТЭК будет настаивать на завершении категоризации до

конца 2019 года, окончательный срок определится во втором квартале 2019 г. Интересно и то, что ФСТЭК подходит к процессу категоризации во многом неформально, не педалирует мелкие неточности в формулярах, главное — это добросовестное применение методики и оценка потенциального ущерба. В завершение регулятор пригласил все заинтересованные стороны принимать участие в разработке нормативных документов в сфере обеспечения безопасности КИИ и пообещал выпустить отдельный документ по информационному обмену.

Автор отмечает некое перекрытие темы информационного обмена с зоной ответственности ФСБ — ГосСОПКой,



Виталий Лютиков, заместитель директора ФСТЭК России



Игорь Качалин, заместитель начальника 8-го центра ФСБ России

однако информационный обмен в России ещё редкий (хотя и безусловно положительный) тренд, поэтому документ в любом случае будет полезен для отечественных служб ИБ.

Представитель ФСБ, заместитель начальника 8-го центра ФСБ России, Игорь Качалин рассказал о численных параметрах работы ГосСОПКА: НКЦКИ оказывал практическое содействие в выявлении и реагировании на компьютерные инциденты, направил субъектам ГосСОПКА 700 уведомлений, 18 организаций создали или создают корпоративные центры ГосСОПКА. Руководитель подчеркнул, что НКЦКИ заинтересован в создании корпоративных центров и будет поддерживать этот процесс.

Вместе с тем, автор выступал заказчиком создания корпоративного центра ГосСОПКА, направленного на оказание услуг субъектам КИИ. На практике конкретные сотрудники НКЦКИ

не очень дружелюбны, плюс существует проблема курицы и яйца: нет зоны ответственности (нет договора с субъектом КИИ) — нет статуса корпоративного центра. Отсутствие статуса корпоративного центра не позволяет заключать договора с субъектами КИИ на реализацию функций ГосСОПКА в их интересах. Впрочем, в дальнейшем на SOC-Форуме Роман Кобцев (компания «Перспективный мониторинг»)

предложил свой рецепт: объявить зоной ответственности корпоративного центра ГосСОПКА инфраструктуру корпоративного центра ГосСОПКА и категорировать центр мониторинга как КИИ.

Артём Сычёв, первый заместитель директора Департамента ИБ Банка России, привёл обнадеживающую статистику: год от года наблюдается увеличение количества атак разного типа, однако мы

О SOC-ФОРУМЕ 2018

Организаторы:
ФСБ России, ФСТЭК России

Оргподдержка:
Медиа Группа «Авангард»,
закрытый клуб «SOC в России»

2000+ участников (по сравнению с SOC-Форумом 2017 общее число участников увеличилось **на 20%**)

География участников:
6 стран, **47** городов России

2 дня деловой программы

12 сессионных заседаний

45 докладов

28 стендов ведущих компаний отрасли



Артём Сычёв, первый заместитель директора Департамента информационной безопасности Банка России



Сергей Лебедь, руководитель службы кибербезопасности «Сбербанка»

уже научились работать с ними, поэтому ущерб год от года падает. Возможно, немалую роль в эффективности защиты играет именно процесс остановки несанкционированных платежей, реализованный на базе ФинЦЕРТ. Артём поделился планами: ФинЦЕРТ переходит на работу в режиме 24×7, что должно сократить доходы злоумышленников. Второе магистральное направление развития ИБ от Банка России — стимулировать развитие банками своих систем и практик информационной безопасности. Теперь риски ИБ станут учитываться при расчёте резервов банка как часть операционных рисков.

Впрочем, профильные эксперты в кулуарах сходятся в едином мнении: сейчас в ИБ относительное затишье, гром-

ких атак давно не было, и это вполне может оказаться затишьем перед бурей. Вот когда она грянет, тогда мы и сможем по-настоящему оценить эффективность механизмов ФинЦЕРТ, НКЦКИ и других системных институтов по противодействию киберугрозам в РФ.

Руководитель службы ИБ Сбербанка Сергей Лебедь (напомню, что Сбербанк является Центром компетенции по ИБ программы «Цифровая экономика Российской Федерации») рассказал о содержании раздела ИБ Программы. Кроме того, он сообщил, что на сегодняшний день в Программе числится 141 мероприятие, но есть проблема с финансированием: из запланированных 5 млрд 667 млн рублей выделено всего 363 млн.

Профильные эксперты в кулуарах и по этому поводу оказались едины: с финансированием в 6 процентов от плана говорить о реальной работе по программе не приходится.

СЕКЦИИ

Отраслевая специфика. Кроме пленарной сессии, на Форуме было представлено сорок докладов. Основные темы — отраслевые: SOC в Промышленности и SOC в Финансах. SOC в Промышленности на практике свёлся к целому ряду выступлений, связанных с КИИ и ГосСОПКА. Промышленники неохотно делились реальными кейсами центров мониторинга. Всего выступили три представителя промышленности (ЕВРАЗ, СО ЕЭС и концерн Калаш-





Качественно новым и очень интересным форматом для Форума стали Киберучения

ников), и только один из них рассказывал про SOC (Евгений Акимов, концерн Калашников), да и то про пилот SOC Информзащиты. Остальные пока находятся на стадии развития SIEM или реализации регуляторных требований.

Направление Финансы больше эксплуатировало SOC. Дельтакредит, Ингосстрах, Газпромбанк и Банк Санкт-Петербург поделились опытом развития SOC, создания гибридного SOC и проведения киберучений. Представители Дельтакредит и Ингосстраха подчёркивали важность передачи знаний от сервис-провайдера клиенту, такая возможность была для них одним из решающих факторов при выборе поставщика услуг мониторинга. В том же русле выступил и автор (ANGARA ASSISTANCE), рассказав, как создать гибридный SOC с передачей знаний клиенту и хранением данных у клиента.

Операционная специфика. С точки зрения операционной деятельности SOC ярко проявился тренд увеличения количества сенсоров и поступающих в SOC данных (big data). Представители Инфотекс и ANGARA упомянули об установке агентов на обнаружение вторжений на рабочих станциях и серверах (хостах), представитель Fore-Scout — об инвентаризации сети как ключевом контексте безопасности для SOC, а представители Гарда Технологий и Cross Technologies — о сетевой и хостовой форензике как необходимых

для расследования инцидентов практиках и технологиях.

Одним из ключевых технологических трендов стало активное использование Open source коммерческими центрами мониторинга. Об этом говорилось в докладах Информзащиты, ICL КПО ВС, на стендах Infosecurity и ANGARA. В конце концов open source позволяет более гибко обрабатывать увеличивающийся поток данных.

Однако любые технологии не приносят пользы без преодоления кадрового дефицита, о существовании которого сокрушались представители Ростелеком-Solar, Инфосистем Джет и других. Со своей стороны, рекомендую для преодоления кадрового голода в SOC воспользоваться специально разработанными и проверенными при создании SOC стратегиями, опубликованными автором в последнем выпуске BIS Journal (№ 4/2018).

ДРУГИЕ ФОРМАТЫ

Выставочная часть Форума насчитывала более двух десятков стендов поставщиков услуг и регуляторов. Все три регулятора, активно работающие на Форуме, — ФСБ России, ФСТЭК России и ФинЦЕРТ Банка России — представили свои стенды. Было бы логичным увидеть в будущем и стенд Роскомнадзора.

Качественно новым и очень интересным форматом для Форума стали Киберучения. Эти весьма азартные соревнования позволили проверить

практические навыки по формированию и принятию решений в ИБ шести командах из 29 специалистов. Примеры вопросов: «Что вы будете делать, если сайт вашего банка взломали?», «Стоит ли оповещать клиентов об инциденте?», «Как реагировать на инцидент, связанный с личной техникой председателя правления банка?» и другие. Чтобы победить в Киберучениях, необходимо было учесть технические, управленческие и политические аспекты управления ИБ в крупной организации. Судейство обеспечивали представители ФСБ, ФСТЭК, Банка России и Сбербанка. В итоге первое место, по единогласному решению судей, заняла команда специалистов Сбербанка.

ЗАДЕЛ НА БУДУЩЕЕ

Следующий SOC-Форум, надеюсь, перейдёт в плоскость конкретики оказания услуг. Кто, кого и в каком объёме обслуживает становится важным — лишь практический опыт мониторинга соизмерных инфраструктур позволяет клиенту быть спокойным, что и у него сервис «взлетит» и принесёт пользу. Второй безусловный тренд (машинное обучение) ещё не достиг зрелости и существенно поможет SOCам и их клиентам не ранее 2025 года. Он же поможет справиться и с экспоненциальным ростом объёма данных, благо, продолжающийся кадровый дефицит автоматически понижает планку качества принимаемых аналитиками SOC решений.



OFFZONE 2018

КОНФЕРЕНЦИЯ БЕЗ ПИДЖАКОВ В АТМОСФЕРЕ ПОСТАПОКАЛИПСИСА

Конференция по кибербезопасности OFFZONE 2018 проходила в окрестностях Кремля, в Digital October, «в постапокалиптических интерьерах, интересных, — как сказал зампред Сбербанка Станислав Кузнецов, — молодым ребятам». Идеологом и организатором мероприятия выступила BI.ZONE — дочерняя компания Сбербанка.

СТАВКА НА «МАЛЬЧИШЕЙ»

По сути OFFZONE 2018 оказалась своеобразным коллоквиумом с элементами дня открытых дверей. Станислав Кузнецов так и заявил: «Тут несколько кадровых агентств отслеживают активности и потенциальных кандидатов, которых мы, в том числе, отбираем на работу».

Атмосфера действительно была любопытной. Элементы лагеря повстан-

цев Че Гевары соседствовали с палаткой дореволюционного старьевщика, где счастливицы отоваривали оффкоины — кибервалюту конференции... Плюс толпы юнцов, одетых в соответствии с дресс-кодом «этичного хакера» — всё это напоминало киношную постапокалиптическую общину.

Официально конференция анонсировалась так: «Более 50 уникальных докладов... Понимание, как выявлять уязвимости и устранять их в финансовой сфере, в области интернет-технологий, «железа»... Участвуют больше тысячи человек...». Реальность вполне соответствовала: около 700 участников, уважаемый иностранный гость — посланец DEF CON, в роли звезды матёрый безопасник Дмитрий Скляров, весьма неглупые представите-

Элементы лагеря повстанцев Че Гевары соседствовали с палаткой дореволюционного старьевщика, где счастливицы отоваривали оффкоины — кибервалюту конференции...

ли «Лаборатории Касперского», QIWI, Wallarm, Тинькофф Банка и Сбербанка.

Уместно предположить, что очень скоро лучшими специалистами будут именоваться и участники тех 10 команд из России, Украины, Венгрии, Польши, Китая и Южной Кореи, которые сразились в финале битвы «этичных хакеров» CTFZONE 2018. Эти ристалища проводятся с 2016 года, в них приняли участие больше 2 тыс. команд. В этот раз участие в предварительном этапе приняли более 1 тыс. команд из 95 стран.

НАДО ЗАИНТЕРЕСОВАТЬ

Упомянутый Дмитрий Складов провёл своеобразный экскурс в профессию и дал наставления молодым против всего плохого. Признанный эксперт рассказал «как мир менялся для меня, и почему ИБ — это то, чем имеет смысл заниматься в жизни». Участникам была предложена работа «до седьмого пота», в связи с чем слоганом OFFZONE стало «Никаких пиджаков, никакого бизнеса — только hardcore research!»

Помимо четырёх потоков докладов на площадке развернулись рабочие зоны для исследователей «железа», аналитиков защищённости интернет-приложений, безопасников банков и т.п. За достижения на «семинарах» и «практикумах» на специальную бейдж-карту начислялись оффкоины, которые можно было потратить на «товар» (рюкзак, футболки, перчатки и др.) или в игре «Тотализатор CTFZONE».



Изюминкой конференции стало подчёркнутое внимание к «железу». О низкоуровневых уязвимостях рассказали Максим Горячий и Марк Ермолов (доклад «Intel ME Manufacturing Mode — скрытая угроза»), а представитель BI.ZONE Иннокентий Сенновский выступил с докладом «Проснись, Нео: детектирование виртуализации при помощи спекулятивного исполнения». На площадке HARDWARE.ZONE были сделаны сообщения о таких направлениях, как «программное» радио, перехват и обработка цифровых сигналов, атаки типа faultinjection на микроконтроллеры на основе архитектуры ARM

и многое другое. Для тех, кто интересуется ИБ в кредитно-финансовой сфере в зале FINANCE.ZONE рассказывали о проблемах ИБ современного банка.

В ОБХОД СТАНДАРТОВ

Если исходить из воспоминаний Дмитрия Складова, первая волна кадров для российской ИБ формировалась в 2000-х в ходе самообразования при решении разрозненных задач. «Все мы учились понемногу чему-нибудь и как-нибудь». И в этой фрагментарности была своя сильная сторона.

Сегодня заслоном на пути такого разностороннего самообразования встали Стандарты. В сфере ИБ их 7 (!) профессиональных и 9 (!) образовательных. А если к этому добавить 300+ нормативных документов, регламентирующих ИБ, то пора грустить: не скоро созреют разносторонне образованные кадры, способные на прорыв.

Похоже, спустя 20 лет, мы снова рискуем увидеть, как в родном Отечестве «бьются мальчиши от тёмной ночи до светлой зари». На этот раз — в сражениях с иностранными киберугрозами и зоопарком ИТ-платформ. По крайней мере OFFZONE 2018 — это именно про подобный подход, про ставку на «мальчишей».



КТО ВЫ: ДОКТОР ДЖЕКИЛ ИЛИ МИСТЕР ХАЙД?

ЗАМЕТКИ С КОНФЕРЕНЦИИ «РАБОТА
С ПЕРСОНАЛЬНЫМИ ДАННЫМИ В ЦИФРОВОМ МИРЕ»

Законотворческий процесс придал новый импульс развитию сферы ИБ. В штатах компаний должен появиться («Денег нет, но вы держитесь!») как минимум ещё один «офицер» — ответственный за защиту персональных данных. В связи с этим конференция «Работа с персональными данными в цифровом мире» показала нам актуальной.

О ЧЕМ ШЛА РЕЧЬ

«Персональные данные», «личные данные», «обезличенные персональные данные», «цифровой профиль клиента» и др. терминология вконец запутала бизнес-сообщество. Чтобы его распутать на конференцию пригласили экспертов из МТС, Боинга, М-Видео, ФАС и др. Речь шла, в частности, о системном использовании законов (например, допускается передача персданных в рамках законов о борьбе с терроризмом и преступностью), внимательном анализе буквы закона (различие понятий «частная жизнь» и «работа»), судебной практике и т.д.

ПОКОРНОСТЬ СУДЬБЕ

Конференция продемонстрировала, что общество готово в очередной раз склонить голову перед новыми малопонятными законами. И это при явных в них противоречиях. Например, в текстах судебных актов, размещаемых на официальных ресурсах, кокетливо «запикиваются» ФИО участников процессов, а в картотеке дел на тех же ресурсах эта информация лежит открыто и тоже на вполне себе законных основаниях.

Никто при этом внятно не объяснил, что же нового внесла «цифровизация» в представления о коммерческой ценности персданных, и почему именно эти данные должны храниться на основе особых законов, отличных от уже

известной «нормативки», касающейся конфиденциальной информации.

Да, сбор персональных данных и построение на их основе цифрового профиля клиента (или гражданина) — это новые технологии, которые иногда удешевляют, иногда ускоряют и иногда делают безопаснее процессы в бизнесе и госуправлении. Но! Как возможность использовать статанализ (на основе обработки массивов данных) может повлиять на изменение правил конфиденциальности при хранении и управлении персональными данными? Почему нельзя законодательной поправкой присвоить персональным данным гриф ДСП, и все обязательства государства перед гражданами в части заботы о безопасности этих данных были бы исполнены.

Ну, и ещё упомянуть в этой же поправке об отказе в присвоении грифа ДСП данным о гражданах, которые зарегистрированы в социальных сетях...

ИСТОРИЧЕСКИЙ ВЫЗОВ? ХА!

Чиновничество развлекается. Сначала вводит требование запрашивать разрешение граждан на передачу их персданных на обработку третьим лицам. Потом понимает, что, как минимум, граждане озвереют от количества приходящих им коротких сообщений, а как максимум, необходимо создавать технологию доверенной передачи ответов этих озверевших граждан... В результате появляется законопроект, согласно которому можно передавать данные граждан на обработку третьим лицам... без всякого уведомления.

А ведь этой вознѣй затушѣвается принципиальное обстоятельство: в цифровом мире происходит подмена людей-личностей наборами данных, обрабатываемых в промышленных масштабах. В этих условиях реальные личностные качества могут не получить

должной оценки и уважительного отношения, в результате чего возникнут глобальные кризисы доверия между людьми, между людьми и государственными институтами, между людьми и бизнесом... Этот социокультурный вызов грозит фундаментальным общественным ценностям.

Кроме того, технологии создания цифрового профиля клиента (ЦПК) несут угрозы и ценностям материальным. Говоря о банках, «автоматизированное» доверие к ЦПК, построенное дистанционно и без должного личностного общения с потребителем — это источник рисков. Кто и как может гарантировать соответствие виртуального поведения клиента (слепок его поведения в социальных сетях) поведению в реальных обстоятельствах? Различия между доктором Джекилом и его виртуальным мистером Хайдом способны обесценить самые совершенные технологии оценки кредитных рисков.

И вдобавок, утрата цифровых персданных доктора Джекила может мгновенно превратить его в злодея Хайда, требующего компенсации в суде.

И всё это происходит на фоне не менее интересной ситуации с безопасностью «цифровых предприятий». А она, по словам замдиректора Positive Technologies Бориса Симиса, такова, что «с большой долей вероятности вы уже взломаны...»

И тут, как ни крути, надо признать, что российский закон о персональных данных и европейский GDPR создают новые отличные стимулы для поиска следов взлома. В Европе штрафные санкции — до 20 млн евро или 4% годового оборота компании. Штрафующие обычно выбирают большую сумму.

ВБА-2018

«СИЖУ В ПРЕЗИДИУМЕ, А СЧАСТЬЯ НЕТ...»

Осенью 2018 г. в московском Экспоцентре прошёл V Международный форум «Вся банковская автоматизация — 2018». Добротное мероприятие, десятки стендов, поток докладов в трёх залах разом, интеллект организаторов — эти составляющие привели ВБА к очередному успеху. И всё же, всё же, всё же... Вспоминается знаменитая фраза народного поэта Расула Гамзатова, написанная им на заседании Президиума Верховного Совета СССР: «Сижу в Президиуме, а счастья нет...»

Главные цели форума ранжированы его организаторами так:

- ♦ предоставить финансовому сообществу максимум готовых решений, способных уже сегодня сократить издержки и повысить эффективность банковского бизнеса;

- ♦ способствовать продвижению и внедрению лучших ИТ-решений для банков;

- ♦ ознакомить банки и финансовые компании с практическими кейсами цифровой трансформации.

«Чего в этих щах не хватает?» — всплывает в памяти ещё одна цитата.

Представляется, что в заявленных целях не хватает присутствия в явном виде термина «кибербезопасность». Нет, организаторы ВБА-2018 не забыли об информационной безопасности. Активно прошёл поток докладов, в которых упоминались и «применение национального стандарта безопасности финансовых операций», и «использование прорывных технологий для обеспечения информационной безопасности». Более того, состоялась панельная дискуссия «Выполнение требований 382-П, безопасность ЕБС и другие актуальные вопросы информационной безопасности».

Но, судя по выставочной экспозиции, кибербезопасность пока ещё остаётся незначительной составляющей и цифровой трансформации, и цифровой эволюции в представлении компаний, предлагающих ИТ-решения для банков. Видно, что большинство компаний и основная масса банков во главу угла ставят «сокращение издержек и повышение эффективности банковского бизнеса». Что было бы вполне естественно для стабильных времён.

К сожалению, сегодня мы живём во времена экономических войн. Только разрывы снарядов сменили отказы в

обслуживании со стороны ИТ-инфраструктуры, а вой систем оповещения ПВО — оповещения ФинЦЕРТ. И это заставляет говорить о необходимости мобилизационной банковской экономики, в которой кибербезопасность приобретает тот же вес, что и эффективность банковского бизнеса, а сокращение издержек ассоциируется с чем угодно, только не с расходами на ИБ.

Безусловно, организаторы ВБА-2018 не могут быть святее Папы Римского. И если известная на нынешний момент версия «Цифровой экономики РФ» свободно оперирует понятиями распределённого реестра, искусственного интеллекта, Интернета Вещей и дополненной реальности при отсутствии реального импортозамещения в базовых аппаратно-программных платформах ИТ, то «кто б тогда за всеми не повлёкся»? Тем не менее, отдавая должное напряжённой работе организаторов ВБА-2018, хочется увидеть в 2019 году обновлённый взгляд на банковскую автоматизацию — сквозь призму кибербезопасности и импортозамещения.



ПОДЪЁМ С ГЛУБИНЫ

ДАРКНЕТ — ГЛАВНЫЙ ДРАЙВЕР ОПАСНОСТИ В 2019 ГОДУ

На пресс-конференции «Кибербезопасность 2018–2019: тренды и драйверы» эксперты Positive Technologies подвели итоги 2018 и представили возможные сценарии 2019 года.

В числе ключевых тенденций прошлого года они отметили:

- ♦ Рост рынка ИБ в России составил 10% по сравнению с 2017 годом. Драйвером стал запуск отдельных проектов федерального уровня в области цифровизации (например, перевод городского хозяйства на новые технологии, появление умных городов, транспорта, государственных сервисов), а также активность ряда крупных компаний в сфере ИБ.

- ♦ Средний прирост числа инцидентов за три квартала 2018 года составил 34%. Одна из причин — существенно снизившийся порог входа в киберпреступность: злоумышленнику уже не нужно обладать высоким уровнем знаний в области IT, достаточно купить готовые инструменты и инструкции в дарквебе. Новое поколение универсальных троя-

нов можно использовать как для шпионажа и кражи данных, так и для удалённого управления устройствами.

- ♦ Промышленный шпионаж снова в моде. Всё больше атак направлено на хищение данных (планов стратегического развития, информации ограниченного доступа и т.п.). В течение года эксперты РТ Expert Security Center зафиксировали на территории России и стран СНГ активность 12 различных АРТ-группировок, нацеленных именно на получение информации.

- ♦ Фишинг — основной метод проникновения. Он использовался в 61% атак на банки в первом полугодии 2018 года. Так действуют, например, группы Cobalt и Silence. Наиболее вероятной мишенью преступников в этом случае остаются банки среднего звена, которые не готовы вкладывать сверхбюджеты в обеспечение ИБ.

- ♦ Всё больше уязвимостей в АСУ ТП. Показатели на конец осени 2018 года уже превышали прошлогодние на 10%. Только с помощью экспертов Positive

Technologies было выявлено и устранено 30 уязвимостей, ещё чуть более сотни отправлены вендорам и ожидают соответствующих патчей. В оборудовании и SCADA-системе одного из исследованных производителей обнаружено более 50 уязвимостей нулевого дня.

- ♦ Кража информации как многофункциональный сервис. Пароли и логины от различных «учеток» и данные банковских карт занимают около 80% всей информации, продаваемой в дарквебе. Средняя стоимость данных одной карты с балансом от нескольких сотен долларов составляет всего \$9. Текст SMS-сообщения, содержащего одноразовый код для проведения платежа, можно оперативно получить за \$250.

Среди возможных негативных сценариев 2019 года эксперты отметили:

- ♦ Инциденты с кибероружием. История, начавшаяся со Stuxnet и Industroyer, может получить продолжение. Так, в 2018 году были обнародованы детали атаки с использованием кибероружия Triton, которое заточено под специфи-



Борис Симис, заместитель генерального директора Positive Technologies



Ярослав Бабин, руководитель отдела исследований безопасности банковских систем Positive Technologies



Владимир Назаров, руководитель отдела безопасности промышленных систем управления Positive Technologies

ческое оборудование Schneider Electric. Исходники попали в сеть и в 2019 году, возможно, будут использованы для различных атак.

♦ Банкоматы могут начать взламывать серийно. В даркнете сегодня можно купить не только сам инструмент и инструкцию по эксплуатации, но и техническую поддержку. Стоимость такого ВПО начинается от \$1500. По данным Positive Technologies, до 69% банкоматов уязвимы для атак Black Box, до 85% для атак на сетевом уровне и до 76% — для выхода из режима киоска.

♦ Скрытый майнинг может остановить завод. Пять лет назад продажа доступа к 1 тыс. взломанных ПК приносила злоумышленнику до \$20, теперь, имея доступ к тем же 1 тыс. ПК, он может заработать до \$600 ежемесячно на майнинге криптовалюты — несмотря на падение курса. Страдают даже коммунальные службы: в феврале на серверах некоторых европейских водочистительных сооружений был обнаружен майнер криптовалюты Monero. Такая паразитная нагрузка для промышленных систем чрезмерна и может достаточно быстро нарушить технологический процесс.

♦ Хакеры могут повлиять на курсы акций и валют. Согласно исследованию Positive Technologies, слабая защищенность трейдинговых приложений мо-

жет привести к тому, что атаки на пользователей бирж станут массовыми в ближайшие год-полтора.

♦ Перехват SMS-сообщений продолжает сохранять актуальность. Массовые атаки с использованием уязвимостей мобильной связи начнутся, если кибергруппировки окажутся быстрее операторов мобильной связи, предпринимающих усилия по нейтрализации угроз. В настоящее время уязвимы около 78% сетей, и перехват SMS возможен в 9 из 10 случаев. При этом в даркнете уже можно купить подписку на получение и подделку чужих SMS в реальном времени всего за \$20 в месяц.

♦ Процессоры могут выдать информацию о своих владельцах. Есть области, в которых меры безопасности реализованы максимально жестко, и фишинг не работает, поэтому эксплойты под процессорные уязвимости могут создаваться продвинутыми кибергруппировками уже сейчас. Сделать процессорные атаки массовыми могут либо новый способ их монетизации, либо утечка готового инструментария, как это было в случае с EternalBlue.

♦ Города могут остаться без интернета. Власти Великобритании выпустили руководство по обеспечению защиты интернета вещей от распространенных кибератак, закон об IoT вышел в Калифорнии. Однако сегодня в мире существует множество так называемых

end-of-life-устройств, производство которых завершено, вендор прекратил выпуск обновлений ПО, а значит, обнаруженные позже уязвимости никогда не будут закрыты. В случае с end-of-life-роутерами атакующие могут блокировать доступ к интернету сотням тысяч пользователей, перенаправлять пользователей на поддельные страницы онлайн-банков и интернет-магазинов для перехвата паролей.

♦ Многим придется отключить Bluetooth. В сентябре 2018 года во всем мире оставалось около 2 млрд устройств, подверженных уязвимостям BlueBorne, которые позволяют красть данные на устройствах, заражать их вирусами-вымогателями или создавать ботнеты. Уязвимы 734 млн устройств на базе Android 5.1 и более ранних версий, свыше 260 млн устройств на Android 6.0 и 50 млн iOS-устройств на базе версий 9.3.5 и ниже.

♦ Тайные АРТ могут стать явными. По итогам 2017 года эксперты компании отметили, что так или иначе с целевыми атаками столкнулась практически каждая вторая организация. В 2018 году ситуация сохранилась. Благодаря давлению регуляторов в 2019 году объекты КИИ обратят внимание на собственную инфраструктуру и с большой долей вероятности увидят, что уже были атакованы какое-то время назад.

**Александр КОЛОДЗЕЙ**

кандидат физико-математических наук,
доцент кафедры ИУ-10 МВТУ
им. Н.Э. Баумана, генеральный директор
ООО «Вычислительные решения»

КЛЮЧ К ПАУТИНЕ

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ БЛОКЧЕЙН-ТЕХНОЛОГИЙ В ЦИФРОВОМ ГОСУДАРСТВЕ

Технологии блокчейн исполнилось 10 лет — 3 января 2009 года был сгенерирован первый генезис-блок блокчейна Bitcoin (Биткоин, обозначение валюты — BTC) [1]. Цифровые валюты, сохраняющие приватность пользователя, появились значительно раньше — тестовые платежи в системе eCash прошли ещё в 1994 году [2]. Цифровая валюта eCash была централизованной и требовала участия банков.

Чтобы избавиться от посредника, участникам необходимо открыто публиковать транзакции, а также уметь приходить к согласию относительно единого порядка их следования. Предполагается, что система находится в безопасности, пока самая крупная часть её вычислительных ресурсов находится под совокупным контролем честных участников [3]. Блокчейн (blockchain, цепочка блоков) — это опубликованная база транзакций, в котором транзакции объединены в блоки. Заголовок

блока включает хэш данного блока и хэш предыдущего блока. За формирование блока полагается вознаграждение. Это эмиссия (конечная или неограниченная) и/или комиссии от включённых в блок транзакций.

Блокчейн-технология не есть нечто однозначно определённое. Это живой, бурно развивающийся мир, в котором много жёстко конкурирующих между собой самых разных решений. На основе открытых исходных кодов Bitcoin появился целый ряд так называемых

альтернативных криптовалют, общее число которых превысило несколько тысяч. На пике в январе 2018 года общая стоимость рынка криптовалют оценивалась в 814 миллиардов долларов, курс BTC приблизился к отметке \$20 тыс. Затем случился резкий откат. К декабрю 2018 год общая капитализация упала примерно до 100 миллиардов, а курс биткоина откатился к уровню лета 2017 года — \$3 тыс. за 1 BTC.

Среди наиболее значимых альтернативных криптовалют следует отметить Ethereum (Эфириум, обозначение валюты — ETH). Основное отличие Ethereum от Bitcoin заключается в наличии децентрализованной виртуальной машины (Ethereum Virtual Machine, EVM). Ethereum создавался не как валюта для переводов, а как платформа для выполнения приложений с оплатой теми самими ETH [4], [5].

На данном этапе развития технологии распределённого реестра из трёх характеристик — децентрализованность, безопасность, масштабируемость — одновременно можно обеспечить только две и принести в жертву что-то одно [6]. В [7] были сформулированы следующие условия применимости блокчейн-технологий:

1. Информация может быть организована в виде базы данных.
2. Множество авторов имеют право порождать транзакции.
3. Авторы не доверяют друг другу.
4. Нет возможности или неэффективно использовать доверенного посредника.
5. Транзакции, созданные разными авторами, зависят друг от друга.

Если не выполнено хотя бы одно из этих условий, блокчейн использовать не стоит. Могут подойти, например, обычное файловое хранилище; централизованная база данных; реплицированная (master-slave) база данных; несколько баз данных с механизмом подписки для пользователей.

Если указанные требования выполнены, требуется чётко понимать:

- ♦ правила валидации транзакций;
- ♦ кому доверяется роль валидатора и какой используется механизм консенсуса;
- ♦ кто обеспечивает эти активы, контролируемые распределённым реестром,

как решаются те или иные юридические вопросы.

Только после решения всех этих вопросов можно говорить о реализации блокчейн-проекта.

К ключевым параметрам блокчейна можно отнести:

- ♦ способ подтверждения блока и достижения консенсуса;
- ♦ язык скриптов в транзакциях;
- ♦ среднее время генерации и максимальный размер одного блока;
- ♦ используемые криптографические алгоритмы хэширования и цифровой подписи.

МЕХАНИЗМЫ КОНСЕНСУСА

В блокчейн-системах используются различные механизмы консенсуса и подтверждения блоков. Схемы типа «один кошелек — один голос», «один IP-адрес — один голос» легко могут быть скомпрометированы действиями злоумышленников. Механизм консенсуса должен опираться на ресурс, который трудно подделать. Сатоши Накамото в [3] предложил принцип «один процессор — один голос».

При алгоритме «доказательство работы» (Proof-of-Work, PoW) в блокчейн включается первый найденный блок, удовлетворяющий некоторой трудно решаемой, но легко проверяемой задаче. В качестве такой задачи обычно выбирается попадание в требуемый диапазон значения хэша блока, зависящего от метки времени и некоторого произвольного параметра. Чем меньше этот диапазон, тем выше сложность задачи. Найденный блок-претендент рассылается по сети. Если остальные участники признают этот блок, то они начинают строить цепь дальше уже относительно него. Считается, что с большей вероятностью наиболее длинная цепочка состоит из блоков, признаваемых большинством участников.

Сложность динамически меняется в зависимости от текущей вычислительной мощности системы так, чтобы средняя скорость генерации новых блоков оставалась примерно постоянной. В Bitcoin пересмотр сложности происходит через каждые 2016 блоков, примерно раз в 2 недели. В ряде альтернативных криптовалют сложность пересматривается чаще, иногда даже после каждого блока. Обладатели крупных вычислительных ресурсов могут манипулировать устанавливаемой в системе сложностью в своих интересах, например, переключаясь с одной криптовалюты на другую [8].

Вероятность получить вознаграждение за генерацию нового блока определяется отношением мощности используемого ресурса к общей мощности системы. Майнеры вкладываются в приобретение нового оборудования, мощность системы растёт, и сделанные вложения обесцениваются. На один блок, записанный в блокчейн, может приходиться 100–1000 блоков-претендентов [9]. Чтобы минимизировать время синхронизации цепи все эти блоки-претенденты должны как можно быстрее доходить до всех участников, что порождает соответствующую нагрузку на сетевую инфраструктуру. Проводимые при генерации блоков вычисления не нужны ни для чего, кроме как для самой блокчейн-системы. Всё это порождает справедливые упреки в крайней неэффективности таких блокчейн-систем. Криптовалюты при объёме капитализации в несколько сот миллиардов долларов и примерно 5 млн активных участников потребляют объём энергии, сравнимый со всем мировым финансовым рынком с капитализацией 300 трлн долларов и 5 млрд участников [10].

Были предложены концепции консенсуса, ориентированные не на использование процессора, а другой вы-

На данном этапе развития технологии распределённого реестра из трёх характеристик — децентрализованность, безопасность, масштабируемость — одновременно можно обеспечить только две и принести в жертву что-то одно

Кардинальное повышение производительности блокчейн-систем до уровня классических платёжных систем возможно за счёт использования так называемых вторичных сетей

числительный ресурс — например, ёмкости дисковых накопителей, алгоритмы Proof-of-Capacity или Proof of Storage. При этом блокчейн, по сути, является инструментом создания децентрализованного облачного хранилища [11], [12].

Вариацией Proof-of-Work является Proof-of-Research (PoR). В проекте Primecoin [13] Proof-of-Work основан на востребованной задаче поиска простых чисел. Другие криптовалюты, такие как Gridcoin [14] и Curecoin [15], пытаются улучшить этот подход, объединив работу майнеров с научными вычислительными задачами открытой платформы BOINC [16] под эгидой американского университета Беркли.

Другой алгоритм — доказательство владением, буквально — подтверждение доли (Proof-of-Stake, PoS). Вероятность того, что система предоставит участнику право сформировать очередной блок и получить за это вознаграждение, будет определяться суммой его депозита. Кроме механизмов поощрения могут быть предусмотрены штрафы за недобросовестное поведение. Случайность выбора очередного победителя может обеспечиваться за счёт использования VDF-функций (Variable Delay Function) [17]. Эти функции отличаются тем, что их вычисление не распараллеливается, а проверка правильности вычисления может быть выполнена существенно быстрее, чем само вычисление — алгоритм Proofs-of-Delay. Предполагается, что валидирующие узлы для ускорения вычисления VDF-функций будут использовать специальные ASIC. Уже стартовал соответствующий open-source-проект. Блокчейн на Proof-of-Stake существенно энергоэффективнее блокчейна на Proof-of-Work.

Венесуэльская криптовалюта El Petro (петро) взяла за основу криптовалюту NEM (New Economy Movement).

Формирование блокчейна в NEM происходит с использованием алгоритма доказательства важности (Proof-of-Importance, PoI) [18]. Он учитывает три характеристики аккаунта:

- ♦ баланс кошелька;
- ♦ количество совершённых аккаунтом транзакций, то есть его «активность» в сети;
- ♦ время нахождения аккаунта в сети.

Интересно отметить, что изменение в Белой книге El Petro с изначального Ethereum на NEM произошло за сутки до начала продаж [19].

В централизованных системах, где есть доверие одному участнику достаточно цепочки подписей (Proof-of-Signature, PoSign).

SMART-КОНТРАКТЫ

Язык скриптов большинства современных блокчейнов, включая биткоин, позволяет программировать условные транзакции — простейшие алгоритмы «if-then-else», но не обладает полнотой по Тьюрингу — возможностью решения любой вычислимой задачи. Поэтому «контракты» представляют собой относительно простые конструкции, такие как «мультиподпись» или «транзакции с отложенным исполнением».

Биткоин мог бы расширить свой функционал, став тьюринг-полным, но отказ от этой характеристики — его принципиальная позиция. По мнению Максвелла, одного из разработчиков ядра биткоина, для системы важна лишь верификация подлинности входящей информации, а не сами вычисления. Вычисления внутри блокчейна серьёзно затрудняют масштабирование.

Язык смарт-контрактов Ethereum тьюринг-полный. Главное отличие в том, что смарт-контракты Ethereum способны хранить состояние в блокчейне (stateful), воспринимать каждую транзакцию как часть большой картины. Bitcoin же использует контракты

без хранения состояния (stateless), его блокчейн обрабатывает каждую транзакцию как абсолютно независимое событие. Тьюринг-полнота Ethereum является всего лишь следствием [20].

ПРОИЗВОДИТЕЛЬНОСТЬ БЛОКЧЕЙН-СИСТЕМ

Размер блоков и среднее время их генерации ограничивают максимальную пропускную способность системы. Так в Bitcoin при размере блока 1 мегабайт и среднем времени генерации одного блока 10 минут пропускная способность ограничена величиной 3–7 транзакций в секунду. Для сравнения, платёжные системы типа Visa рутинно обрабатывают 2 тыс. транзакций в секунду, потенциально Visa может обрабатывать до 56 тыс. транзакций в секунду.

При увеличении размера блока вырастает нагрузка на сеть, увеличивается себестоимость работы узлов, меньше людей оказываются в состоянии продолжать этим заниматься — система становится всё более и более централизованной. Разработчикам Bitcoin это показалось неприемлемым. Вместо увеличения размера блока в Bitcoin была реализована технология SegWit (Segregated Witness, отделённый свидетель), когда подписи транзакций не входят в сам блок, а могут запрашиваться дополнительно. Это примерно вдвое увеличивает максимальное количество транзакций, которые могут быть размещены в одном блоке без увеличения его размера.

Кардинальное повышение производительности блокчейн-систем до уровня классических платёжных систем возможно за счёт использования так называемых вторичных сетей. В таких сетях для проведения большого количества транзакций между двумя или более участниками в блокчейн записываются только транзакции о создании каналов обмена, а потом их закрытии. При открытии канала происходит блокирование средств в размере установленных лимитов. При закрытии канала стороны договариваются о подведении баланса в расчётах. Все остальные транзакции между ними осуществляются, минуя блокчейн — транзакции генерируются, но в блокчейн не записываются, остаются в статусе неподтверждённых.

Криптографические протоколы гарантируют, что в случае недобросовестного поведения одного участника, второй участник может забрать первоначально замороженные средства себе. Технология SegWit обезопасила от мошенничества с неподтверждёнными транзакциями, чем существенно облегчила реализацию вторичных сетей [21].

Радикальным редизайном Bitcoin является Bitcoin NG. В нем раз в 10 минут генерируются ключевые блоки, которые включают в себя только доказательство PoW, ссылку на предыдущий блок, единственную транзакцию — вознаграждение за генерацию блока и публичный ключ майнера. При помощи приватного ключа майнер будет подписывать последующие микроблоки, содержащие транзакции, пока не будет сгенерирован следующий ключевой блок. Микроблоки в исходной версии Bitcoin NG создаются уже раз в 10 секунд и не требуют PoW. Майнер может подписывать противоречивые транзакции, допускать двойное расходование. Если сеть заметит это, создаётся «токсичная» транзакция, которая задним числом уничтожает прибыли недобросовестного майнера [22].

Отечественная платформа Vostok [23], развивающаяся в сотрудничестве с Госкорпорацией Ростех, основывается на технологической базе и технологических заделах Waves — самом быстром публичном блокчейне в мире, обрабатывающем 1 тыс. транзакций в секунду. Блокчейн Waves сочетает идеи Bitcoin NG с Proof-of-Stake.

Создатели Ethereum решение задачи масштабирования при сохранении децентрализации и безопасности видят в технологии партиципирования, которая давно известна в распределённых базах данных. Транзакции делятся на «осколки» (на английском «shard»). Каждый узел обрабатывает не весь блок, а его составляющие. При этом происходит дробление вычислительной мощности системы, поэтому вместе с внедрением этой технологии будет происходить переход с Proof-of-Work на Proof-of-Stake.

Стратегии на основе каналов и типа Bitcoin NG могут масштабировать количество транзакций, что достаточно для stateless-блокчейнов, но не могут

масштабировать хранилище состояний и подвержены DDos-атакам. Партиципирование (шардинг) и масштабирование оффчейн через каналы, возможно, могут дополнять друг друга [24].

КРИПТОГРАФИЧЕСКИЕ ФУНКЦИИ

В Bitcoin используются комбинации хэш-функций SHA-256, RIPEMD-160 и алгоритм подписи на эллиптической кривой secp256k1: $y^2 = x^3 + 7$ (Elliptic Curve Digital Signature Algorithm, ECDSA). Инвариант этой кривой равен 0, то есть ГОСТ Р 34.10–2012 не рекомендует её к использованию [25]. Обоснования выбора в Bitcoin эллиптической кривой secp256k1 никогда публично не обсуждались.

В алгоритме ECDSA при выработке каждой очередной цифровой подписи происходит выбор некоторого целого числа. Если хотя бы для одной подписи это число становится известным злоумышленнику (навязано при помощи программной закладки, снято со слабого генератора случайных чисел и пр.), то компрометируется и сам секретный ключ цифровой подписи. Поэтому некоторые пользователи после каждой транзакции остаток средств каждый раз пересылают на новый адрес, что не всегда удобно.

В основе развиваемой под эгидой ЦБ РФ платформы Мастерчейн лежит протокол платформы Ethereum с адаптацией под возможность применения стандартов шифрования в соответствии с российским законодательством и в части идентификации пользователей, и валидирующих узлов [26]. В платформе Vostok также используются криптографические алгоритмы, соответствующие требованиям ГОСТ, и квалифицированные электронные подписи [23].

БЕЗОПАСНОСТЬ БЛОКЧЕЙН

Транзакции Bitcoin никак не шифруются, хранятся и пересылаются по сети в открытом виде. Это позволяет осущест-

влять атаки на сетевую инфраструктуру, блокировать распространение тех или иных транзакций или блоков-претендентов.

Говорить об анонимности блокчейна можно лишь условно. Отследить, с какого IP-адреса была отправлена транзакция с тем или иным адресом Bitcoin — дело техники. Не случайно был случай, когда что-то за деньгами, отправленными на биткоин-кошелёк очередного вируса-вымогателя, обратиться никто так и не рискнул.

В качестве криптовалюты, обеспечивающей анонимность, популярность набрала криптовалюта Monero (Монеро, обозначение валюты — XMR) [27]. В ней используются одноразовые адреса, скрывающие информацию о счёте и его владельце, а также система кольцевых подписей, исключающая идентификацию участников цепочки. В 2017 году в Monero была добавлена технология RingCT (Кольцевые конфиденциальные транзакции), которая позволяет скрывать суммы транзакций. В разработке находится проект Kovri — I2P-маршрутизатор на языке C++, который должен позволить пользователям Monero скрывать свои IP-адреса во время отправки транзакций.

Анонимность переводов в Monero всё равно не имеет 100 % гарантии. Из-за выявленных уязвимостей до обновления в начале 2017 года можно было вычислить реальную монету более чем в 90 % случаев, сводя на нет все гарантии безопасности. Сейчас реальную монету можно вычислить в 45 % случаев. Транзакции Monero остаются потенциально отслеживаемыми, небольшие фрагменты информации могут накапливаться и в сочетании с другими источниками данных со временем образовывать вполне твердую доказательную базу. На примере Monero видна фундаментальная проблема конфиденциальности криптовалют. Любая уязвимость, обнаруженная в будущем, может быть задним числом

Говорить об анонимности блокчейна можно лишь условно. Отследить, с какого IP-адреса была отправлена транзакция с тем или иным адресом Bitcoin — дело техники

По некоторым оценкам, в коде смарт-контрактов Ethereum в среднем 100 ошибок на 1000 строк кода; в то время как в коде Microsoft их в среднем 15 на 1000 строк, в коде NASA — около нуля на 500 000 строк

использована на имеющихся данных, позволяя заинтересованному наблюдателю извлечь из блокчейна любые старые скелеты [28].

УЯЗВИМОСТИ СМАРТ-КОНТРАКТОВ

По некоторым оценкам, в коде смарт-контрактов Ethereum в среднем 100 ошибок на 1000 строк кода; в то время как в коде Microsoft их в среднем 15 на 1000 строк, в коде NASA — около нуля на 500 000 строк [10]. Проанализировав около миллиона смарт-контрактов, исследователи обнаружили, что в 34 200 из них содержались критические уязвимости. Они проверили свои предположения на 3000 смарт-контрактах и в 89 % случаев смогли вызвать на своей копии блокчейна Ethereum самые нежелательные последствия, что позволило бы им украсть \$ 6 млн [29]. В большинстве случаев, как отмечают ученые, баги случались из-за трудности восприятия смарт-контрактов, которые сейчас, в основном, написаны на языке программирования Solidity. Главная претензия, что к этому языку невозможно применить аппарат автоматической проверки теорем [30].

ВЕТВЛЕНИЯ БЛОКЧЕЙНОВ И АТАКА 51 ПРОЦЕНТОВ

Широко распространено мнение, что злоумышленнику для того, чтобы вмешаться в работу блокчейна необходимо контролировать более 50 % ресурсов сети — вычислительной мощности, монет и пр. На самом деле, речь идет о том, если злоумышленник контролирует менее 50 % ресурсов, вероятность того, что ему удастся сгенерировать n блоков подряд, экспоненциально убывает с ростом n . Но эта вероятность всё равно остаётся больше 0. Так, например, контролируя 30 % мощности, злоумышленник может сгенерировать 5 блоков подряд с вероятностью 18 %.

Основная проблема заключается в том, что решения, какие транзакции или блоки принимаются, а какие — отвергаются системой, делаются на уровне программного обеспечения. Разработчики могут выпускать его всё новые и новые версии, в том числе противоречащие друг другу. Изначально единый блокчейн может расходиться на разные ветки, признаваемые разными версиями программ — так называемый форк (fork). И уже сам пользователь должен принимать решение, какой версией программ пользоваться, чему он должен доверять. Характерный пример. В одном из смарт-контрактов, размещенных в блокчейне Ethereum, была обнаружена уязвимость, из-за которой деньги утекали и продолжали утекать. Встал вопрос, что делать дальше. Одни выступили за то, чтобы откатить историю и вместо ошибочного контракта разместить правильный. Другие из философских соображений стояли на том, что блокчейн должен быть нерушим. Договориться так и не удалось, в результате Ethereum разделился на криптовалюты Ethereum и Ethereum Classic (обозначение валюты ETC). В одной пошли одним путем, в другой — другим, получилось две параллельные реальности. Различные ветвления — частные явления в мире криптовалют. Появление всё новых и новых форков обесценивает ограниченность эмиссии каждой конкретной криптовалюты.

5 января 2019 года была замечена глубокая реорганизация блокчейна Ethereum Classic, в результате которой осуществлялись двойные траты. Биржа Coinbase моментально остановила движение этих средств, после чего зафиксировала еще восемь дополнительных случаев реорганизации цепи. Общая сумма попавших под атаку 51 % средств, по оценке биржи, составила 88 500 ETC (около \$ 460 000) [31].

Биткоин-биржа Gate.io сообщила, что предположительный организатор атаки 51 % на сеть криптовалюты Ethereum Classic вернул ей \$ 100 000 из 40 000 ETC (примерно \$ 200 000) которые ее пользователи потеряли ранее. Причины, по которым ей вернули средства, биржа также не знает. «Если организатор атаки не стремился к получению выгоды, то это может быть белый хакер, который хотел напомнить людям о рисках, которые присущи консенсусам блокчейнов, и о безопасности, которую обеспечивает вычислительная мощность», — говорится в сообщении биржи [32].

РОЛЬ И МЕСТО БЛОКЧЕЙН-ТЕХНОЛОГИЙ

Известный экономист Нуриэль Рубини в своём выступлении в Сенате США подверг технологии блокчейн жестокой критике, назвав криптовалюты самым серьёзным в истории лопнувшим пузырьком, а блокчейн — самой переоцененной технологией, которая в реальности не лучше, чем таблица Excel или обычная база данных. Реальная революция в сфере денежного обращения, по его словам, это ФинТех, основанный на искусственном интеллекте (ИИ), бигдате и интернете вещей, а не криптовалюты и не блокчейн [10].

Следует четко понимать условия и границы применимости блокчейн-технологий. Так, Минфин РФ допускает появление единой цифровой валюты в Евразийском экономическом союзе (ЕАЭС) в 2020–2021 годах. Но, как сообщил журналистам замглавы Минфина Алексей Моисеев, реализовываться данный проект цифровой валюты будет, скорее всего, без использования технологии блокчейн [33].

Внутри одного ведомства блокчейн не нужен. Взаимодействие разных ведомств может быть организовано с использованием блокчейн-технологий, но при этом возникают вопросы о порядке финансирования получившейся системы и ответственности за её функционирование.

Основной областью применения блокчейн-технологий является ведение распределенного реестра в децентрализованных системах в условиях взаимного недоверия.

В числе основных сервисов, которые могут предоставляться блокчейн-платформам, можно перечислить:

- ♦ авторизация пользователей в различных сервисах, в том числе с выполнением требований закона о защите персональных данных;
- ♦ цифровой нотариат;
- ♦ клиринговые системы, в том числе международные расчеты в условиях санкций;
- ♦ ведение реестров акционеров;
- ♦ ведение истории сделок с объектами недвижимости;
- ♦ ведение истории автотранспортных средств, авиатехники и пр.
- ♦ страховые истории;
- ♦ кредитные истории;
- ♦ отслеживание грузов;
- ♦ контроль качества товаров при движении сырья и комплектующих по производственным цепочкам;
- ♦ фиксация основных транзакций с объектами интеллектуальной собственности и правами на них, организация

хранилища оцифрованных объектов и предоставление доступ к объектам с использованием коллекций «умных» контрактов;

- ♦ безопасное обновление программного обеспечения в интернете вещей, системах видеонаблюдения и пр.

ПОДВОДЯ ИТОГИ

Всплеск интереса к блокчейн-технологиям и криптовалютам дал серьёзный импульс развитию «гражданской криптографии», обеспечению информационной безопасности самых различных цифровых сервисов, позволил сделать значительные шаги в создании цифрового государства, цифровой экономики.

Технологии распределённого реестра имеют самые широкие области применения в цифровых сервисах, цифровой экономике, цифровом государстве. При этом блокчейн-технологии имеют условия применимости, при невыполнении которых их внедрение нецелесообразно.

При всех своих достоинствах существующие блокчейн-технологии имеют ряд принципиальных недостатков и ограничений, требуют дальнейшего развития.

Широкое распространение блокчейн-технологий в России, наряду с совершенствованием правовой базы, потребует решения вопросов как производительности и масштабируемости, так обеспечения информационной безопасности. В качестве варианта решения может быть предложено использование доверенных, сертифицированных аппаратных блокчейн-клиентов и создание, по образцу операторов фискальных данных, сети независимых доверенных блокчейн-центров. Должны решаться вопросы импортозамещения, разработки собственных программных и аппаратных решений, а также их сертификации. Важную роль должно сыграть развитие экосистемы разработки, анализа и внедрения блокчейна и других криптографических технологий.

ЛИТЕРАТУРА

1. «10 лет назад в сети биткойна был добыт генезис-блок», <https://forklog.com/10-let-nazad-v-seti-bitkoina-byt-dobyt-genezis-blok/>
2. «Взлёт и падение проекта DigiCash, который изменил мир», <http://chainmedia.ru/articles/where-it-all-began/>
3. Satoshi Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System», <https://bitcoin.org/bitcoin.pdf>. Русский перевод: «Биткойн: система цифровой пиринговой наличности», https://bitcoin.org/files/bitcoin-paper/bitcoin_ru.pdf
4. «Ethereum Project», <https://www.ethereum.org/>
5. «Что такое криптовалюта Ethereum простыми словами», <https://cryptonisation.ru/ethereum-cto-eto-i-kak-zarabotat/>
6. «Дорожная карта Эфириума на 2018–2019 г. или в ожидании Virtuoso», <https://1ethereum.ru/dorozhnaya-karta-efiriuma-na-2018-2019-goda-ili-v-ozhidanii-virtuoso/>
7. «Как избежать бессмысленных блокчейн-проектов», <https://bitnovosti.com/2015/12/22/avoiding-pointless-blockchain-project/comment-page-1/>
8. «Как майнеры манипулируют сложностью майнинга Bitcoin Cash, и что в этом плохого», <https://ttrcoin.com/kak-maynery-manipuliruyut-slojnostyu-mayninga-bitcoin-cash-i-cto-v-etom-plohogo.714/>
9. «Блеск и нищета Bitcoin (а ещё про blocknet)», <https://habr.com/post/408627/>
10. «Криптовалюты — самый большой (и уже лопнувший) пузырь в истории», <https://andreimovchan.whotrades.com/blog/43773660029>
11. Sia. Fully decentralized cloud storage, <https://sia.tech/>
12. ThreeFold Grid, <https://threefold.io/grid/>
13. Primecoin, <http://primecoin.io/>
14. Gridcoin, <https://www.gridcoin.us/>
15. CureCoin, <https://curecoin.net/>
16. BOINC, <https://boinc.berkeley.edu/>
17. VDF Research Effort, <https://vdfresearch.org/>
18. «NEM — технология экономики будущего», <https://cryptostate.ru/kriptovalyuty/nem>
19. «О венесуэльской государственной криптовалюте», https://pikabu.ru/story/o_venesuyelskoy_gosudarstvennoy_kriptovalyute_5973972
20. «Концепции развития умных контрактов: биткойн vs Ethereum», <https://forklog.com/smart-contracts-concepts/>
21. «Спор о масштабируемости Биткойна: контекст, решения и будущее», <https://bitnovosti.com/2018/07/12/spor-o-masshtabiruemosti-bitkojna-kontekst-resheniya-i-budushhee/>
22. «Учёные считают, что Биткойну требуются радикальные изменения», <https://bitnovosti.com/2015/11/23/bitcoin-ng/>
23. «Платформа Vostok», <http://www.vostokplatform.org/>
24. «Шардинг в Ethereum: полный FAQ от команды проекта», <https://crypto-fox.ru/faq/sharding-ethereum/>
25. ГОСТ Р 34.10-2012. «Процессы формирования и проверки электронной цифровой подписи», <http://docs.cntd.ru/document/gost-r-34-10-2012>
26. «Что умеет Мастерчейн?», <https://www.if24.ru/cto-umeet-masterchejn/>
27. Monero, <https://monero.org/>
28. «Никакой анонимности: Почему Monero не скроет ваши транзакции.» <https://ru.ihodl.com/analytics/2018-03-29/nikakoj-anonimnosti-pochemu-monero-ne-skroet-vashi-tranzakcii/>
29. «В смарт-контрактах на блокчейне Ethereum обнаружено свыше 34 тысяч уязвимостей» <https://forklog.com/v-smart-kontraktah-na-blokcheyne-ethereum-obnaruzheno-svyshe-34-tysyach-uyazvimostej/>
30. «Why Solidity isn't solid», <https://medium.com/@Hibryda/why-solidity-isnt-solid-3341af77fc1c>
31. «На сеть Ethereum Classic осуществлена атака 51%», <https://forklog.com/na-set-ethereum-classic-osushhestvlena-ataka-51/>
32. «Организатор атаки 51% на Ethereum Classic вернул \$100 000 бирже Gate.io», <https://forklog.com/organizator-ataki-51-na-ethereum-classic-vernul-100-000-birzhe-gate-io/>
33. Минфин России допустил ввод единой цифровой валюты ЕАЭС в 2020-2021 годах», <https://tass.ru/ekonomika/5941194>

АРГУМЕНТЫ ПРОТИВ ФАКТОВ

УДАЧНЫЙ МАРКЕТИНГОВЫЙ ХОД ИЛИ ЭКОНОМИЧЕСКИ
УСПЕШНАЯ СТРАТЕГИЯ?¹

ВОЛНА ПРАВЕДНОГО ГНЕВА

Эксперты Агентства США по международному развитию (USAID) не нашли никаких доказательств успеха технологии blockchain. Как пишет сайт The Register, несмотря на отлично спланированную рекламную кампанию по продвижению технологии, пресс-релизы, официальные документы и убедительные статьи, проведенное аналитиками Агентства исследование 43 решений на основе blockchain не обнаружило фактов успешного использования этой технологии.

«Мы не получили ответов, когда обратились к фирмам-производителям напрямую — по электронной почте, по телефону и лично. Никто не хотел делиться данными о результатах программы, процессах MERL или адаптивным управлением для потенциального масштабирования. Несмотря на всю шумиху о прозрачности технологии blockchain и возможности ее применения в процессах и операциях в средах с низким уровнем доверия, индустрия blockchain сама по себе непрозрачна», — заявил недавний поклонник технологии, один из экспертов Агентства Джон Бург. И сделал вывод: «Blockchain был отлично подан и продан, но в его основе лежит база данных с проблемами производительности и масштабируемости».

Принятие Blockchain широкими массами, далёкими от техники и технологий, —

это хорошо построенная рекламная кампания, основанная на вере в технический прогресс, — считают эксперты. Они сравнивают blockchain с мыльным пузырьком, похожим на тюльпаноманию или калифорнийскую золотую лихорадку. Большинство инвесторов теряет свои состояния, в то время как доходы советников и маркетологов растут. Например, Fujitsu предлагает услуги ускоренного консалтинга по цене от 9 900 фунтов стерлингов, чтобы оценить возможность использования технологии blockchain в проекте любого заказчика.

Потому возникают вопросы о необходимости жёсткой регламентации консалтинга и маркетинга в области технологий, как это происходит в области финансовых услуг, которая контролируется Комиссией США по ценным бумагам и биржам.

ПРИМЕР № 1

Но BIS Journal все же отыскал пару солидных примеров успешного применения blockchain. Летом 2018 г. торговая площадка We.trade, построенная на основе blockchain, провела первые живые торги. За пять дней десять компаний из пяти стран выполнили семь сделок через четыре международных банка. Эти сделки стали первыми коммерчески жизнеспособными сделками с открытым счетом, использующим технологию blockchain.

Решение We.trade, построенное на платформе IBM Blockchain, оснащено Hyperledger Fabric, предлагает клиентам доступ к простому интерфейсу и использует инновационные смарт-контракты. «Проведённые торги доказывают, что We.trade — надёжное и выгодное предложение, удобное при международной торговле», — заявил главный операционный директор We.trade Роберто Манконе. Его коллега, глава отдела торговли в KBC и председатель совета директоров We.trade, Хуберт Беноут пояснил, что «живая торговля является масштабным достижением для всех участников. Мало того, что We.trade построил техническое решение, ему также удалось создать реальное сотрудничество между несколькими банками и увеличить связность торговой экосистемы. Это сотрудничество в лучшем виде».

We.trade называет себя дружелюбной цифровой платформой, дающей безопасное, эффективное и инновационное решение для банков. Платформа была создана группой банков — Deutsche Bank, HSBC, KBC Bank NV, Natixis, Nordea, Rabobank, Santander, Societe Generale и UniCredit — для упрощения трансграничной торговли и удовлетворения ожиданий клиентов. Консорциуму удалось выполнить требования каждого банка к внутреннему управлению и процедурам, чтобы сделать инновацию реальностью. В настоящее время We.trade доступен в одиннадцати европейских странах — Бельгии, Дании, Финляндии, Франции, Германии, Италии, Нидерландах, Норвегии, Испании, Швеции и Великобритании, — и рассчитывает на расширение числа участников в Европе и мире.

Принятие Blockchain широкими массами, далёкими от техники и технологий, — это хорошо построенная рекламная кампания, основанная на вере в технический прогресс, — считают эксперты

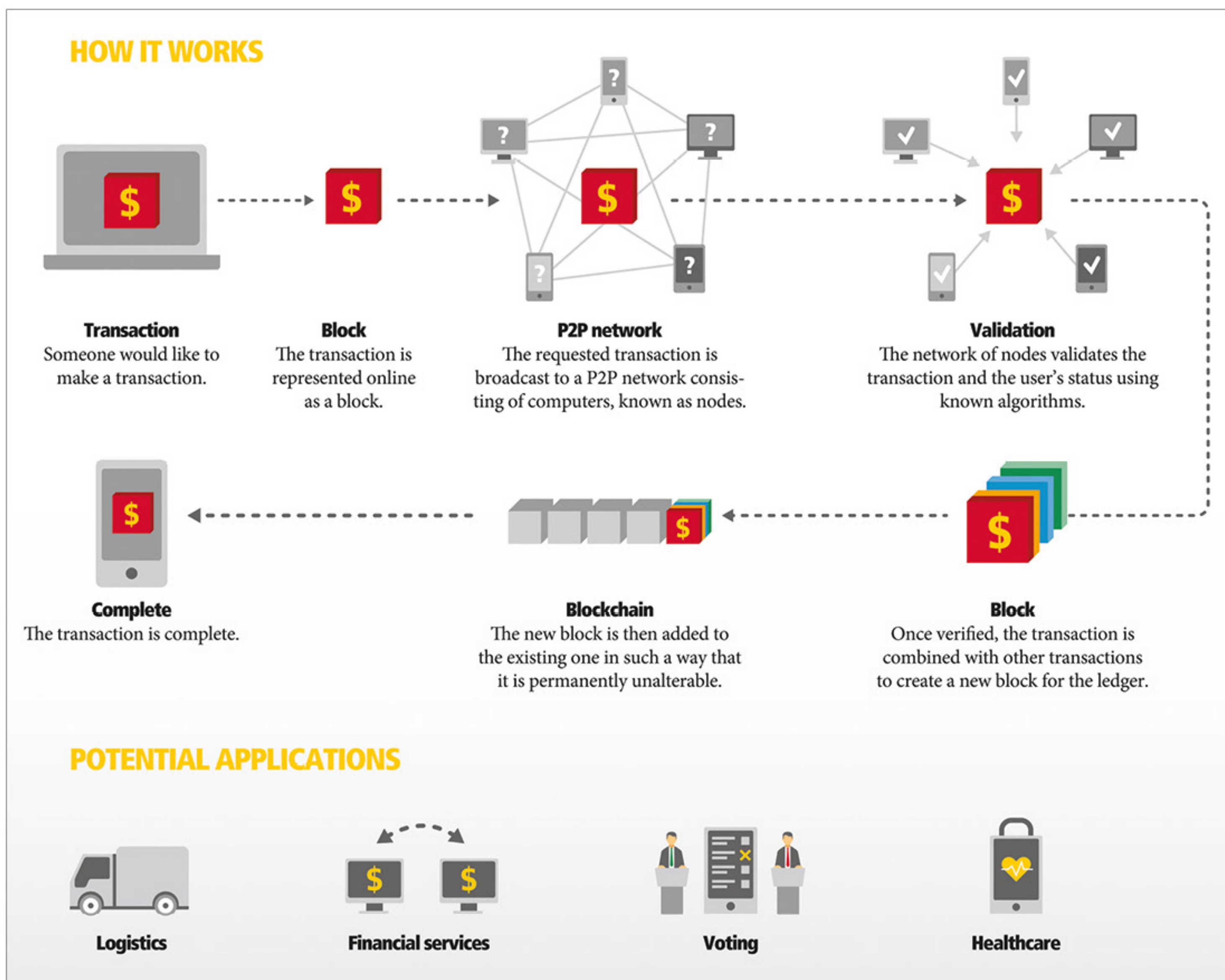


Схема реализации технологии блокчейн в финансовой структуре компании DHL

ПРИМЕР № 2

Ещё один пример применения технологии blockchain для бизнеса — компания DHL, мировой лидер в области логистики. Весной 2018 г. DHL запустила в эксплуатацию платформу ShipChain, которая помогла устранить ряд застарелых проблем и повысить качество работы компании. Благодаря использованию ShipChain, технология blockchain отлично вписалась в технологическую цепь поставок и логистики, повысив эффективность всех процессов. Компания DHL планирует и дальше развивать процесс обновления своих технологий с использованием blockchain.

Второе направление, где DHL использует blockchain, — финансовое. Управление платежами отнимает много времени, что затрудняет взаимодей-

ствие между компаниями и их торговыми партнёрами. Для решения этой задачи DHL создала первую в мире программу торгового финансирования на основе blockchain на базе Платформы от TradeIX при участии банка Standard Chartered и страховой компании AIG. Все детали счёта и имеющейся застрахованной суммы зафиксированы в бухгалтерской книге, построенной на основе blockchain. Такое финансовое описание счёта позволяет DHL активно взаимодействовать с контрагентами, отслеживать и продлевать сроки оплаты, поддерживая дебиторскую задолженность в актуальном состоянии.

В конечном итоге DHL реализовал на основе технологии blockchain информационную систему для своего бизнеса по доставке товаров. В системе,

помимо сотрудников компании, работают:

- ♦ банки, кредитующие её клиентов;
- ♦ страховые компании, страхующие грузы и кредиты банков;
- ♦ клиенты компании DHL.

За счёт реализации доверенной среды для всех участников и прозрачности бизнес-процессов, банки и страховые компании понизили ставки. От этого выиграли клиенты DHL. Как следствие, в результате формирования лучших рыночных условий для клиентов, компания нарастила свой бизнес.

¹ Редакция благодарит члена редколлегии BIS Journal А. Филипчука за предоставленную информацию

ПОБОЧНЫЕ «ЗАРАБОТКИ» ИБ

ЕЩЁ ОДИН ВЗГЛЯД НА ЦЕННОСТЬ DLP-СИСТЕМ

Приятный сюрприз: DLP-система, собирающая коммуникационные метрики внутри компании, при надлежащем использовании становится источником Больших Данных для предиктивной аналитики «социальных» и деловых процессов в компании. В таком контексте DLP-система превращается в источник «добавленной стоимости».

В НУЖНОЕ ВРЕМЯ В НУЖНОМ МЕСТЕ

В сфере управления персоналом при принятии решений традиционно используются чутьё, интуиция и субъективные выводы сотрудников кадровых служб. Видимость объективности им придаёт анализ ограниченных данных (кадровые анкеты, материалы психологического тестирования и т.п.). Технологии анализа Больших Данных (БД) позволяют перейти к управлению «HR-ресурсами» на основе «объективной» обработки цифровых профилей людей.

Кавычки в слове «объективный» призваны обратить внимание, что и технологиям БД присущ субъективизм. Он кроется в ограниченной точности моделей для расчётов или процессов «машинного обучения». Тем не менее инструменты предиктивной аналитики позволяют руководителям фокусироваться точно на проблеме и принимать обоснованные решения «в нужный момент в нужном месте».

О ЧЁМ РЕЧЬ?

По словам Андрея Арефьева, руководителя отдела развития продуктов компании InfoWatch, использование таких технологий как Scikit-learn и TensorFlow (программные библиотеки для машинного обучения), Pandas (библиотека для обработки и анализа данных), SQLAlchemy (библиотека для работы с базами данных при помощи язы-

ка SQL) позволило DLP-системе InfoWatch научиться решать задачи по прогнозированию ИБ-рисков, связанных с увольнением сотрудников.

Поясним, что результаты анализа информации DLP-системой могут быть представлены в виде своеобразного светофора. При появлении проблемных мест в конкретных рабочих кабинетах на интерфейсе оргструктуры компании появится «тревожная» подсветка, характерная для того или иного нежелательного процесса.

Пример. Модуль предиктивной аналитики указал на готовность сотрудника расстаться с организацией. Особенностью происходящего явилось то обстоятельство, что после прихода нового начальника отдела уволиться были готовы сразу несколько специалистов, к работе которых раньше никаких претензий не было. С учётом того, что потери от ухода квалифицированного работника оцениваются в сумму, равную его годовой зарплате, у руководства были все основания для детального анализа ситуации. В результате решение об увольнении было принято, но расстаться пришлось лишь с начальником отдела, создавшим условия для возникновения группы риска («с точки зрения» предиктивного модуля DLP-системы).

На графике вероятности увольнения видно (Рис. 1), как оценка сотрудников отдела с августа растёт вверх, в «тревожный» рейтинг (снижается рабочая активность, скорость реакции на письма и др. показатели), а в ноябре, с момента ухода начальника отдела, вероятность увольнения сотрудников резко снижается. Тревожные показатели устремились к нулю.

Другая ситуация. Опираясь на данные из DLP, служба безопасности выявила нарушения кадровой службы при приёме людей на работу. Само по себе это обстоятельство не содержало криминала, но регулярное нарушение кадровых процедур привело к приёму гораздо менее квалифицированных специалистов, чем того требовали стандарты. В результате работу кадровой службы тщательно исследовали и внесли важные коррективы.

«InfoWatch стоял у истоков создания DLP-рынка, и вот уже 15 лет внимательно следит за трендами угроз информационной безопасности. А они всё больше сосредотачиваются не столько вокруг компьютерных систем, сколько вокруг человеческого фактора. Ландшафт средств безопасности меняется, границы между ними стираются, уступая место комплексным решениям, объединяющим все ИТ-си-



Рисунок 1. График вероятности увольнения

системы, с которыми соприкасается сотрудник предприятия», — считает Андрей Арефьев.

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ КАДРОВОЙ СЛУЖБЫ

До недавнего времени использование Больших данных в управлении кадрами считалось надуманным. Исключением было проведение в 2008 году компанией Google проекта Oxygen, оценивавшего качество управленческого персонала. Но масштабы Google — это около 40 тыс. сотрудников, 5 тыс. менеджеров, тысяча директоров и около сотни вице-президентов. Можно говорить о статистике. Для большинства же компаний речь шла лишь об анализе на основе моделей не более сложных, чем те, что использовались демографическими службами по опросам общественного мнения.

Тем не менее, рынок периодически предлагал бизнесу те или иные средства автоматизации работы кадровых служб. Например, приложение IBM Kenexa для поддержки процессов поиска и закрепления на работе наиболее квалифицированных сотрудников. Для аналогичных целей предлагались и пакеты Crunchr и Talentsoft Analytics.

BigData прописались в отделах кадров с развитием социальных сетей, когда миллионы людей стали выкладывать на всеобщее обозрение не только персональные данные, но и информацию о своём окружении и поведенческих характеристиках.

На одной из конференций по ИБ в 2018 году демонстрировались дополнительные возможности контроля благонадёжности сотрудников. Оказалось, что при определённых обстоятельствах негативной метрикой может оказаться «более 20 подтверждений взаимного общения между сотрудниками различных банков». При всей спорности данной метрики, упомянутый мастер-класс в целом дал примеры того, как Большие Данные из социальных сетей используются службами кадров.

ИСТОЧНИКИ BIGDATA ДЛЯ КАДРОВОГО МЕНЕДЖМЕНТА

Социальные сети стали «золотым дном» для BigData-аналитики в интересах служб безопасности и отделов

При определённых обстоятельствах негативной метрикой может оказаться «более 20 подтверждений взаимного общения между сотрудниками различных банков»

кадров. Очень быстро появился инструментарий, позволяющий давать детальные характеристики целевым аудиториям. Например, на конференции по digital-маркетингу FiNPLACE представители компаний «МедиаЛогия», «Brand Analytics», социальной сети «ВКонтакте» раскрыли в цифрах и графиках если не все, то многие характеристики разных сегментов отечественных социальных сетей. На всеобщее обозрение были выставлены гендерные, возрастные, культурные и т.д. особенности виртуальных сообществ России.

Однако использование данных соцсетей может стать предметом и судебного спора. Почти два года продолжается тяжба между компанией-администратором социальной сети и компанией, разработавшей оригинальные методики и алгоритмы для поиска, хранения и анализа социальных данных в Интернете. Последняя извлекала из соцсетей данные и оценивала для своих клиентов риски от взаимодействия с теми или иными людьми. На момент написания этого материала судебный иск прошёл первый круг слушаний в нескольких инстанциях и вернулся в городской арбитражный суд.

Но вернёмся к DLP-системе. В контексте вышеописанной ситуации, она, как источник данных о людях, интересующих кадровую службу, не обладает недостатками социальной сети. К этим недостаткам, помимо юридических рисков, следует отнести возможное отличие поведенческого профиля персоны в публичной соцсети от её же поведенческого профиля в закрытом коммуникационном пространстве компании. При этом даже в небольшой компании рынка СМБ DLP-система генерирует массивы данных, которые с полным правом можно отнести к классу BigData по таким критериям, как объём собираемых материалов, темпы сбора, актуальность, разнообразие и т.д.

ПРОЦЕСС ПОШЁЛ

Отметим, что термины «технологии BigData», «машинное обучение», «предиктивная аналитика» являются в понимании многих синонимами термина «Искусственный Интеллект» или частью того, что включает в себя этот «зонтичный бренд». С учётом этого обстоятельства следует оценивать следующую информацию:

Если в 2015 году по мировым оценкам лишь 24 % работодателей намеревались использовать предиктивную аналитику в сфере работы с персоналом, то через год эта цифра составила уже 32 %. Стартапы в этой области собирают инвестиции в десятки миллионов долларов.

Один из стартапов, использующий технологию анализа BigData в интересах управления персоналом, создан Дэвидом Яном, входящим в TOP-200 российских миллиардеров. Известная российская компания IBS также уже более 2 лет ведёт исследования в области предиктивной HR-аналитики на основе Больших данных.

* * *

В этом контексте ГК InfoWatch предлагает решение для предиктивной аналитики класса UEBA (User and Entity Behavior Analytics), позволяющее прогнозировать вероятность увольнения сотрудника с точностью 80 % за 25 дней до факта ухода. При этом используется более 15 метрик для анализа структуры коммуникаций в каналах. Это адресаты сообщений, рабочая активность сотрудника в определённые часы, время реакций на рабочую почту и другие. По мнению экспертов InfoWatch, решение целесообразно использовать в компаниях с численностью 800 и более человек. В маленьких компаниях, как правило, все сотрудники и взаимоотношения внутри коллектива на виду.

ЕЩЁ ОДИН ХОМО. КУДА ЕГО?

КРУГЛЫЙ СТОЛ ОБ ОБРАЗОВАНИИ НА ФОРУМЕ
FINOROLIS-2018 ОБОЗНАЧИЛ НАПРАВЛЕНИЯ

Разговор об образовании в цифровую эпоху так и не дал ответа на поставленный в программе Финополиса-2018 вопрос «Homo technologicus. Какой он?». Собственно и разговор пошёл совсем не об этом, но шёл он активно, и в результате достаточно самобытно представил картину нынешней ситуации. Пусть эта картина получилась не столько реалистической, сколько элитарно-концептуальной, но тем не менее... Концептуальный подход применительно к цифровой экономике пока ещё в тренде.

МЕТАНАВЫКИ. БОЛЬШОЙ ВОПРОС

Сергей Мясоедов, модератор, директор Института бизнеса и делового администрирования РАНХиГС: Homo technologicus — это новая волна технологических людей. А помните предыдущую волну, когда в 1920–30-е и послевоенные годы в массовом порядке и весьма успешно готовили инженерную интеллигенцию? Это было время индустриализации и НТР. Сегодня настала пора цифровой экономики. В программе «Цифровая экономика РФ» указано, что в области IT необходимо подготовить 80 тыс. на первом и 120 тыс. специалистов на втором этапах. И тут возникают вопросы: к чему ещё надо готовить этих людей, кроме IT и цифр? Что представляет собой homo technologicus?

В книге Марти Ньюмейера «Метанавыки: пять навыков в эпоху робо-

тизации» описываются скилы (англ. *skill* — умение, мастерство — ред.), необходимые в нашу эпоху: 1. эмпатия и интуиция; 2. видение и системное мышление; 3. умение мечтать, посмотреть на систему извне; 4. талант к реализации, практике; 5. обучаемость. И ничего не сказано об углублении профессиональных компетенций. Это что — провокация? Автор не видит, что мы живём в эпоху цифровых технологий? Или мы упускаем что-то в фокусе подготовки современных специалистов?

ВШЭ. МЕЖДУ ДВУХ ОГНЕЙ

Иван Аржанцев, декан факультета компьютерных наук НИУ ВШЭ: Мне близка тема как учить тому, что постоянно меняется. Эту задачу мы решаем на нашем факультете с момента его создания в 2014 г. Это совместный проект ВШЭ и компании Яндекс. В 2018 г. мы приняли 500 человек на первый курс бакалавриата и 200 в магистратуру. Среди первокурсников 39 победителей и призёров Всероссийской олимпиады по математике, информатике и физике. И мы обязаны учить их хорошо, поскольку это лучшие абитуриенты страны.

А вот как и чему учить... Есть две крайности. Первая — консервативная, когда университет учит одному и тому же последние сто лет и по-другому учить не может. Это тупик. Другая крайность — предельная ориентированность на практику, когда обучение идёт согласно потребностям опрошенных компаний. Но пока студенты окон-

чат обучение, потребности компаний изменятся. Тоже плохо. Нужен компромисс. Мы, например, в первые годы обучения предлагаем базовые курсы, когда студентов учат математике, языкам программирования, алгоритмам и структурам данных, а дальше структура обязательных курсов разветвляется, становится подвижной, практичной, хотя фундаментальная основа тоже остаётся.

Пример из практики. Читаю первокурсникам первую лекцию по математическим основам в защите информации. Рассказываю, с одной стороны, классические, с другой, весьма прикладные вещи. После лекции студенты спрашивают: «А какие навыки мы получим в результате этого курса?». И я задумался. Такой вопрос, оказалось, часто задают преподавателям математики... Поэтому, безусловно, на старших курсах должна быть обязательная вариативность программ, наполненность практико-ориентированными занятиями. Хотя для тех, кто готов к специализации с первого курса, мы предлагаем мини-курсы, факультативы, но при условии выполнения обязательной программы.

Следующий этап — магистратура. У нас она работает по-настоящему, то есть даёт студентам знания в конкретной предметной области. Например, есть магистерская программа, разработанная совместно со Сбербанком, — «Финансовые технологии и анализ данных», есть программа по биоинформатике «Анализ данных в биологии и медицине» и т.д.



КОМИТЕТ
ОБЩЕСТВЕННЫХ СВЯЗЕЙ
И МОЛОДЕЖНОЙ ПОЛИТИКИ
ГОРОДА МОСКВЫ

Публикация подготовлена в рамках проекта «Безопасность цифровой экономики Москвы: Новое поколение», поддержанного грантом Мэра Москвы №085-МГ/18



Сергей Мясоедов, модератор, директор Института бизнеса и делового администрирования РАНХиГС

Отдельный вопрос — учебные центры компаний. Их возникновение объясняют крахом системы высшего образования, тем, что университеты не справляются с обучением. Иногда это так. Когда университеты дают неактуальные знания, компании вынуждены включаться в учебный процесс. Но в целом это обычная практика привлечения старшекурсников и обучение с учётом специфики организации. Например, наша магистерская программа «Науки о данных» создана совместно со Школой анализа данных Яндекса. Школа Яндекса — корпоративный проект, не связанный напрямую с университетами, его задача — формирование среды в области computer science. Но одно другому не мешает, и вот уже несколько выпускников Школы стали нашими преподавателями.

ЯНДЕКС. ВЫСШЕЕ ОБРАЗОВАНИЕ НЕ ОБЯЗАТЕЛЬНО

Илья Залесский, руководитель образовательных сервисов Яндекса: Как Яндекс пришёл к самостоятельной подготовке кадров? Очень просто: всех знакомых наняли, стали приглашать незнакомых, а их, оказалось, надо обучать. Нашей компании сложно нанимать людей извне, важно, чтобы человек не только обладал технологическими навыками, но ещё и мог к нам присое-

диниться, а значит, умел делать свой продукт и умел разбираться в соседних областях. Яндекс — большая экосистема, где продукты создаются на стыке разных технологий. Например, каршеринг «Яндекс.Драйв» использует принципиально разные продукты «Яндекс.Карты» и «Яндекс.Авто».

Погрузиться сразу в несколько продуктов ни у кого быстро не получается. Этому нужно учиться, поэтому мы идём в университеты и работаем со студентами. Мы это делаем через Школу анализа данных. Она существует 11 лет, курс обучения занимает два года. В него входят теория и практика. Практика выполняется совместно с сотрудниками Яндекса. Это очень глубокое погружение, и многие выпускники Школы сегодня работают в ключевых проектах Яндекса.

Мне кажется, что homo technologicus, которому посвящён круглый стол, — это глубокое погружение в корпоративную культуру. Невозможно воспитать человека одновременно для Яндекса и для какой-то другой компании. Он так или иначе будет подходить только одной организации.

И ещё одна мысль мне кажется важной: индивидуализация образования. По данным академика Евгения Ямбурга только 12% школьников считаются, с точки зрения образовательной системы, здоровыми. У них нет особенностей, которые нужно учитывать в процессе об-

учения. А у остальных они есть, и всем им требуется индивидуальный подход.

88% — эту цифру нельзя забывать, но о ней просто не хотят знать. И речь не только о средней школе. Говоря о подготовке кадров, нужно понимать, что и тут индивидуализация — абсолютная неизбежность. Преподаватель в стенах или вне стен вуза обязан учитывать интересы, потребности и особенности учащихся.

Не так давно мы запустили проект «Яндекс.Учебник». Это новое поколение пособий — цифровые учебники для школ, которые построены на идее индивидуализации. Над этой темой работают многие, основная сложность — никто не знает, как правильно. Учит не технология, учит учитель — и так будет ещё много лет. Необходимо найти стык, в котором есть и преподаватель, и технология, и вместе они создают синергию. Это сложно, и именно эту проблему мы со своей стороны пытаемся решить.

Нужно ли сегодня высшее образование? При отборе в нашу компанию оно не является обязательным критерием. Все кандидаты проходят вступительные испытания, которые позволяют отбирать сильные кадры. Безусловно, чтобы заниматься сложными продуктами, высшее образование полезно, и сотрудников с дипломами университетов у нас много, а те, кому образования не хватает, стараются его получить.

ПРО ОНЛАЙН-ОБРАЗОВАНИЕ

Можно ли получить образование, в том числе и высшее, онлайн? Считается, что многие на это способны. Учит онлайн можно всех, и это будет правильно, и безусловно повысит общее качество образования. Но есть элементы мотивации, топовые лекторы в ведущих вузах, которые сильны как личности, взаимодействие с которыми само по себе ценно. Не менее важны семинарские занятия. Поэтому популярные стартапы, например, Minerva, существуют в партнёрстве с вузами. Хотя изначально они начинали как самостоятельные онлайн-структуры. Но позже они пришли к пониманию, что взаимодействие важно.

Высшее образование, повторюсь, полезно, но когда я слышу цифры, что не-



обходимо подготовить 120 тыс. человек, мне не понятны цели. Если мы говорим про инженеров, решающих задачи высшего порядка, то это спорт высоких достижений, и массовостью такие задачи не решаются. Если речь о программах, то их нужно гораздо больше, и их можно готовить быстрее — не в вузах, а через онлайн-образование. Тем более, что в России есть коммерческие игроки, которые это уже делают. В ближайшие годы рынок онлайн-образования будет расти, и имеет смысл его поддерживать, в том числе и государству.

ЗА СЧЁТ ШИРИНЫ ВОРОНКИ

Вопрос из зала: Вы говорили об особенностях корпоративной культуре Яндекса. Но как может кандидат на работу в Яндексе, прошедший только онлайн-обучение, соответствовать этой культуре?

Илья Залесский: Риск нивелируется тем, что в онлайн-образовании гораз-

до шире воронка. Мы можем учить на входе не 30, а 30 тыс. человек. И даже если будет огромный отсев, выбор всё равно останется большим. За счёт ширины воронки онлайн-обучение на выходе даст нам не меньше специалистов, чем при очном обучении. В Школе Яндекса есть заочный факультет. До конца учёбы доходит немного слушателей, процент выпускников ниже, чем при очном образовании, но он не нулевой. Важно дать людям, которые не могут посещать очные занятия, возможность учиться дистанционно.

Другой опыт. Яндекс.Лицей — это проект для школьников 8–9-х классов по обучению программированию. Там есть очные кружки, а есть заочные. На очные — огромный конкурс: 500 школьников на 15 мест, а онлайн-кружки дают шанс всем. Отсев оказался очень невысоким, т.к. мотивация настолько велика, что дети — сами

или с помощью родителей — доходят до конца. Много, конечно, зависит от программы, от способов отбора, но в любом случае онлайн расширяет возможности и решает часть проблем.

Вопрос из зала: ВШЭ заявила, что уходит от очных курсов профессоров. Теперь студенты будут слушать видеолекции, а профессора сосредоточатся на исследованиях, научной работе. Так ли это?

Иван Аржанцев: Это эксперимент. Насколько он будет успешным, не знаю. Но если получится, вероятно, его можно будет тиражировать.

Илья Залесский: Предложение революционное, работа идёт уже несколько лет. ВШЭ является лидером среди российских университетов по числу записанных онлайн-курсов. Часть есть на платформе Coursera. Наш факультет, помимо одиночных курсов, сделал три больших англоязычных специализации

в партнёрстве с Яндексом и Университетом Сан-Диего. В среднем студенты оценивают онлайн-курсы не ниже, чем живые лекции.

Процесс перехода на видеолекции будет проходить поэтапно. Посмотрим, что получится.

Модератор: Перенос лекций в онлайн имеет ещё одну грань. Высвобожденное время преподаватели должны будут тратить на внеклассную проектную работу со студентами, ибо индивидуализация образования — это не только возможность брать нужные онлайн-курсы, но и проработка их через проекты в постоянном контакте с экспертом-преподавателем. Но не все преподаватели к этому готовы.

СУММА ТЕХНОЛОГИЙ: ФАНАЗИЯ ИЛИ ПАНАЦЕЯ?

Константин Козлов, генеральный директор Национального центра электронного образования, руководитель проекта электронного образования аппарата директора по особым поручениям ГК «Ростех»: Проект «Современная цифровая образовательная среда» был создан в ВШЭ и является национальной платформой открытого образования. Была поставлена задача интегрировать всевозможные онлайн-курсы в программы различных вузов. Процесс идёт крайне неоднозначно. Например, практика показывает, что онлайн — это, при разной степени эффективности, часто потеря студентов. Существует проблема сохранения связи студента, обучающегося дистанционно, и коллектива, совместной деятельности.

Другой вопрос — вопрос идентификации Иванова, который прошёл онлайн-обучение, с Ивановым, который пришёл устраиваться на работу. Это задача биометрической идентификации, которая позволит получить доступ к сведениям о порядке изучения студентом материала внутри курса. Такие подходы разрабатывались Министерством образования и науки, но пока это — массив ни о чём не говорящих данных.

И нельзя забывать о главном, иначе мы выплеснем с водой ребёнка. В образовании важен субъект и его интерес, а не технологии сами по себе. Если уча-



Антон Арнаутов, директор НКО «Финтех Лаб»

щемуся тема неинтересна в принципе, результат обучения, независимо от технологий, будет крайне низким. Поэтому важен комплекс технологий, каждая из которых отвечает за определённый аспект, этап. Например, сначала адаптивные технологии должны выявить интересы человека, его предрасположенность, особенности восприятия, пробелы в его образовании, достоинства, недостатки... И только потом, исходя из этого, с помощью уже других технологий точно, шаг за шагом достигать результата.

Инструментом такого комплексного воздействия могут стать государственные информационные системы. Сейчас создаются национальные проекты по формированию цифровой образовательной среды для школ. Перетекание информации, накопление цифрового портфолио и умение с ним работать, введение интересных для поколения Z предметов — нужны такие решения. Цифра, которая приходит в образование, не исключает преподавателей, но она меняет роль участников в образовательном процессе. Раньше учитель — носитель знаний, теперь — старший наставник, который учит работать с материалом и находить ответы на вопросы.

Google и Apple работают именно по этой схеме, собирая данные из разных сфер. Задача образовательного трека —

обеспечить единую платформу сбора данных, к которым имели бы доступ все. Это обеспечит и поиск талантов, и их индивидуализацию.

ИТОГ ЭКСПЕРИМЕНТА: СТУДЕНТОВ НАДО «ПЕРЕУПАКОВАТЬ»

Модератор: Три года успешной работы в нашей магистратуре по совместной со Сбербанком программе Fintech показали, что молодые специалисты, обладающие блестящим техническим образованием и языковой подготовкой, не имеют базовых коммуникативных навыков. Плюс нестандартное мышление. Схожая ситуация в бакалавриате: первые два курса доминируют победители всероссийских олимпиад и отличники по ЕГЭ, а на третьем курсе занятия переводятся в проектный режим, когда надо принимать решения, работать в команде. И тут из тени выходят середнячки и отстающие, оттесняют отличников и занимают первые позиции. Антон, как вы учите новое поколение мыслить нестандартно и адекватно одновременно?

Антон Арнаутов, директор НКО «Финтех Лаб»: Я присутствую здесь в двух качествах: как директор компании «Финтех Лаб» и как советник по работе с банками образовательного центра «Сириус». И есть замкнутый круг, который мы пытаемся разорвать.



Руслан Вестеровский, заместитель Председателя Банка России

Год назад я участвовал в такой же дискуссии, и тогда мне казалось, что у меня есть ответы на вопросы о причинах разрыва между потребностями работодателя и тем, что делают вузы. Как любому стартаперу мне казалось, что я вот-вот переверну мир. Мы придумали идею группового проектного обучения, когда финансовая организация ставит практическую задачу, а группа студентов работает над её решением и в процессе учится именно тому, что сегодня актуально для банка. По сути мы учим студентов за три месяца «запилить пилот» для банка.

Мы запустили девять таких пилотов в разных городах. До финиша добрались два: студенты из Томска сделали проект для QIWI Blockchain Technologies, а студенты из Таганрога — для «Центр-Инвеста». Остальные проекты застопорились. С одной стороны, банкам оказалось некогда заниматься какими-то там групповыми проектами с обучением. С другой, ребята, столкнувшись с таким отношением, потеряли мотивацию. И всё само собой рассосалось. Соответственно моё представление о том, как всё очень просто, тоже изменилось.

Ещё одно направление, которым мы занимаемся, — пытаемся устроить на стажировку талантливых студентов, победителей олимпиад. Вы знаете, сколь-

ко студентов я — специалист по продажам с многолетним стажем — устроил в банки за год? Одного — в банк «Открытие»! Полный провал, из которого надо делать выводы.

Почему банки не хотят выращивать для себя кадры? Банкиры уверяют, что у них нет нужных специалистов, а вузы учат не тому, и приходится переучивать. И в то же время они абсолютно не готовы прилагать усилия в этом направлении и отвлекаться от основной деятельности. Банки якобы перегружены текущими задачами, зарабатыванием денег. Им не до кадров.

Из этого опыта я сделал такой вывод: и университетам, и банкам надо пересмотреть отношение и идти навстречу друг к другу. Для того, чтобы финансовые и нефинансовые компании брали к себе студентов и занимались их развитием, молодёжь надо «переупаковывать».

Потенциальный работодатель заинтересован в решении производственной проблемы здесь и сейчас. И бессмысленно предлагать ему студентов просто на практику или обучение. Чтобы бизнес взял студентов, надо знать его потребности. Например, если разрабатывается мобильный банк, надо искать студентов для выполнения рутинных задач именно по этой разработке. И таких студентов возьмут на практику

или стажировку, начнут учить и адаптировать на новом месте.

Вопрос из зала: Банк ВТБ. У вас интересная инициатива. Но как вы считаете, если человек не имеет опыта и знаний, не умеет социализироваться в организации со своей внутренней бюрократией, может ли банк доверить ему аналитические или прикладные IT задачи, от решения которых многое зависит?

Антон Арнаут: Вопрос отлично демонстрирует барьер между банками и студентами. В рамках Молодёжного дня на Финополисе студенты решали кейсы для банков. На многих участников форума уровень этих решений произвёл сильное впечатление, что подтверждает: у молодежи есть и образование, и силы, и потенциал. Но общего языка с банками мы пока не находим.

Реплика из зала: Волговяское главное управление Банка России. С удовольствием берём студентов на практику. Уровень их подготовки, конечно, часто вызывает вопросы, но все они быстро погружаются в нашу среду и работают, приносят пользу. Мы — за студентов.

БАНК РОССИИ. ПОЗИЦИЯ РАБОТОДАТЕЛЯ

Руслан Вестеровский, заместитель Председателя Банка России: Мы позиционируем ЦБ как высокотехнологичного регулятора и соответственно развиваем свои технологии и кадры. Структура Банка России трансформируется — становится компактной, число сотрудников, с одной стороны, сокращается, с другой, требования к ним изменяются, с третьей, появляются запросы на новые профессии и команды. Мы практически заново комплектуем экономические подразделения во всех главных управлениях по стране, запускаем новые хабы, центры разработки. Теперь нам нужны чуть другие по профилю сотрудники. Мы, безусловно, заинтересованы в талантливых выпускниках, но ставку всё же делаем на обучение и развитие тех, кто уже работает в ЦБ. Вкладываем в это большие средства. В этом году мы открыли университет, практически это самостоятельный департамент, работаю-

щий и внутри банка, и для внешнего контура. Там разработаны дистанционные программы по разным направлениям, охватывающим тысячи человек. Многие сформированы на основе спроса самих сотрудников. Например, программа «Ступени лидерства». Через эту комплексную переподготовку пройдут 1300 руководителей. Чему их будут учить? Системные решения, принятие решений в ситуации неопределённости, большой пакет софт скилс¹, технических навыков, знаний в области кибербезопасности и т.д. Зачем, спросите вы, опытному руководите-

¹ Софт скилс (англ. *soft skills*) — «мягкие навыки» или «гибкие навыки», позволяют быть успешным независимо от специфики деятельности и направления, в котором работает человек.

Хард скилс (англ. *hard skills*) — технические навыки или навыки, которые можно наглядно продемонстрировать. К этой категории относятся например знание технологий, гостей и стандартов, ремонт оборудования и т.д.

лю все эти примочки? Поделюсь собственным опытом. Мне сейчас 38 лет, и всё, что я сегодня делаю, я узнал за последние шесть лет. Прошлые знания не актуальны. Чтобы работать в изменяющейся среде, нужно быть в тонусе, постоянно поддерживать свой профессиональный уровень. При формировании новых подразделений мы с удовольствием смотрим новых потенциальных работников. В этом смысле ЦБ является интересным работодателем. К нам приходят, потому что у нас основательно, надёжно, безопасно. Но хочется, чтобы нас выбирали потому, что у нас интересно, много разных проектов и хорошая корпоративная культура. Хочу пожелать участникам сессии, чтобы компании правильно выстраивали свои стратегии в области управления персоналом, чтобы была возможность привлекать достойных сотрудников, в том числе и из среды выпускников. Но не стоит ждать, что

вузы закроют все бреши в образовании, нужно создавать условия для развития людей внутри компании. Вложенные средства вернутся.

Вопрос из зала: Екатерина Мельникова, Сбербанк. Все обращают внимание, что у молодого поколения отсутствует или на минимальном уровне софт скилс. Как вы считаете, надо вменить развитие этих навыков вузам, поручить компаниям или с развитием технологий общение станет несущественным для бизнеса?

Руслан Вестеровский: Надо идти от клиентов. Меньше общения — меньше продаж. Я думаю, вузы могут взять на себя часть обучения, за 4 + 2 лет в университете вполне можно развить и эти навыки. Для корпоративных университетов также есть простор для деятельности. Но есть и третий сценарий, когда человек сам в себя инвестирует: ходит на программы, тренинги, читает, общается — занимается саморазвитием.

ИТ-ОТРАСЛЬ И КАДРОВЫЙ АПОКАЛИПСИС

В конце прошлого года состоялось заседание Комитета АПКИТ¹ по образованию. По оценке отчетного доклада Б. Нуралиева сегодня в России насчитывается порядка миллиона ИТ-специалистов, что составляет менее 1,5 % от трудоспособного населения России. Один из ключевых выводов доклада: в стране наблюдается хронический некомплект кадров ИТ-профиля.

Для сравнения, доля работников сферы ИТ в России в 4 раза меньше, чем в Великобритании — стране в контексте ИТ-лидерства достаточно периферийной. Развитие же экономики России на основе программы «Цифровая эко-

номика РФ» неизбежно повысит спрос на ИТ-кадры со стороны предприятий за пределами ИТ-отрасли. Неизбежная конкуренция между ИТ-компаниями и ИТ-отделами предприятий других отраслей позволяет предположить апокалиптический сценарий, ведущий к падению конкурентоспособности ИТ-отрасли России.

Вынесенный на обсуждение Б. Нуралиевым сценарий эволюционного реформирования системы профподготовки ИТ-специалистов включает отказ от уравнилельных принципов распределения финансирования на образование и переход на приоритетное финансирование ИТ-образования, увеличение квот на обучение ИТ-специалистов за счёт бюджета, сокращение сроков высшего образования до 5 лет.

Представители вузов в свою очередь отметили, что препятствием для бы-

строого увеличения выпуска специалистов ИТ-профиля, в частности, является дефицит педагогических кадров. Обсуждалось влияние увеличения бюджетных квот на финансовую самостоятельность образовательных учреждений. Декан факультета ИТ Новосибирского государственного университета М. Лаврентьев отметил, что факультет при содействии государства смог бы увеличить набор студентов на 30 % без потери качества их подготовки.

На заседании был также рассмотрен вопрос о подготовке ежегодной конференции «Преподавание ИТ в России», которая пройдёт в 2019 году в мае в Новосибирске, и проведении в ее рамках хакатона АПКИТ для молодежных команд с участием преподавателей.

В заключение состоялось обсуждение шести проектов профстандартов, актуализированных АПКИТ.

¹ Ассоциация предприятий компьютерных и информационных технологий, главный смысл членства в которой — формирование ИТ-рынка вместе с ведущими игроками, обеспечение будущего для ИТ-бизнеса

**Екатерина ЗОБОВА**сотрудник Фонда содействия развитию
безопасных информационных технологий
(ФСРБИТ)

ЦЕЛЕВОЙ НАБОР

В 2019 ГОДУ КОНКУРС ВЫРАСТЕТ¹

Поступить в высшее учебное заведение на специальность, связанную с информационной безопасностью, задача для многих выпускников школ невыполнимая. Проходной балл общего конкурса по трём экзаменам в некоторые московские институты достигает 298 (!), а конкурс в среднем составляет 20 человек на бюджетное место.

В такой ситуации разумные абитуриенты ищут альтернативные варианты поступления — помочь могут олимпиады и целевой набор. И если про олимпиады школьникам всё хорошо известно, то целевой набор, хоть и существует не один год, всё-таки явление для современных абитуриентов новое, пусть и пришедшее к нам из СССР.

ОСОБЕННОСТЬ

Особенность целевого набора в том, что абитуриент приходит в вуз не только с результатами ЕГЭ, но и с соответствующим направлением от какого-либо органа государственной власти или госу-

дарственного предприятия. При этом, в случае успешного прохождения отдельного конкурса, он зачисляется на выбранную им специальность, обучается там, а после окончания вуза идёт работать в то место, откуда его направили.

ПЛЮСЫ

Плюсы для абитуриента очевидны. Во-первых, конкурс по целевому набору несколько ниже. В Минобрнауки РФ отмечают, что он не превышает двух человек на место. А число студентов по программам целевого обучения составляет 13 % от общего набора.

Во-вторых, для целевиков проводится отдельный конкурс. Он проходит раньше, чем общий приём. Таким образом, если студент не поступает по целевому набору, он может претендовать на бюджетные места на общих основаниях.

Кроме того, при поступлении студент будет получать дополнительные «бонусы» от предприятия в виде повышенной стипендии, помощи при подготовке практических заданий и т.д.

МИНУСЫ

Впрочем, у целевого набора есть и минусы. Целевик обязуется не менее трёх лет отработать на предприятии, от ко-

торого поступает в вуз. Кроме того, с 2019 года в договоре заказчик может указать свои собственные требования к результатам обучения. Скажем, он может захотеть, чтобы ваш диплом был без «троек», а то и вовсе красный. И если вы нарушите этот договор, придётся вернуть деньги, потраченные на обучение. Заплатить придётся и в том случае, если студент вдруг решит не отрабатывать на предприятии минимум три года.

Но санкции устанавливаются и в отношении самих компаний. Не трудоустроили выпускника на обещанное место — платите ему штраф в размере трёх средних месячных зарплат по своему региону.

КВОТЫ

Количество мест для целевиков с 2019 года ограничивается специальными квотами. Теперь правительство будет рассчитывать их отдельно для каждой специальности с учётом потребностей экономики. Если мы посмотрим на направление «информационная безопасность», то квота целевых мест от общего числа бюджетных в 2019 году составляет 10%. И если в 2018 году в Высшей школе экономики по специальности «Компьютерная безопасность» на 30 бюджетных мест было семь целевых, то теперь только три.

ОБЗОР

Российские вузы сотрудничают с многими государственными компаниями. Например, в 2018 году МГТУ им. Баумана осуществляло целевой набор на

Если про олимпиады школьникам всё хорошо известно, то целевой набор, хоть и существует не один год, всё-таки явление для российских абитуриентов новое, пусть и пришедшее к нам из СССР

¹ Публикация подготовлена в рамках проекта «Безопасность цифровой экономики Москвы: Новое поколение», поддержанного грантом Мэра Москвы №085-МГ/18



В 2018 году МГТУ им. Баумана осуществляло целевой набор для ФГБУ «ЦЭКИ»



РТУ МИРЭА принимает студентов от НИИ ТП

специальность «компьютерная безопасность» для Федерального государственного бюджетного учреждения «Центр экспертизы и координации информатизации» (ФГБУ «ЦЭКИ»), подведомственной структуры Министерства цифрового развития, связи и массовых коммуникаций РФ. Также вуз ведёт работу с организациями ОПК, подведомственными Министерству промышленности и торговли, «Роскосмосу» и «Росатому».

МАИ подписал договор о целевом наборе на специальность «информационная безопасность» с АО «Россий-

ская самолётостроительная корпорация «МиГ», АО «Уфимское агрегатное предприятие «Гидравлика».

Московский государственный университет геодезии и картографии предлагает целевой набор на специальность «информационная безопасность» от АО «Головное производственно-техническое предприятие «Гранит».

РТУ МИРЭА принимает студентов на специальность «информационная безопасность телекоммуникационных систем» (10.05.02) от НИИ ТП.

МФТИ сотрудничал с ИТЭБ РАН, Министерством образования и науки

Республики Ингушетия, Правительством Республики Северная Осетия-Алания. Целевой набор в ВШЭ который год осуществляют Сбербанк, Управление по контролю за оборотом наркотиков, корпорация «Энергия» и многие другие предприятия.

В МГУ на ВМК в 2018 году поступило 7 человек — от Министерства обороны Республик Калмыкии, Адыгеи, Тыва, Пензенской области, от Правительства Ханты-Мансийского автономного округа-Югры.

337-ФЗ

Впрочем, это совсем не значит, что абитуриент, который хочет поступать по целевому набору, должен подписывать договор с одной из вышеперечисленных компаний. В прошлом году был принят Федеральный закон от 03.08.2018 N 337-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части совершенствования целевого обучения». «Установлено, что гражданин, поступающий на обучение по образовательной программе среднего профессионального или высшего образования либо обучающийся по соответствующей образовательной программе, вправе заключить договор о целевом обучении с федеральным государственным органом, органом государственной власти субъекта РФ, органом местного самоуправления, юридическим лицом или ИП».

Таким образом, любая компания, испытывающая дефицит в специалистах, сможет отправить своих абитуриентов на обучение. Нужно лишь заключить соглашение с соответствующим вузом. Конкурс по целевому набору по специальности «информационная безопасность» в 2019 году однозначно будет выше.

* * *

Однако проблемы с нехваткой специалистов по ИБ сохраняются. По данным Минобрнауки, в России потребность в новых специалистах по ИБ до 2020 г. составит 21 тыс. человек в год. Отечественные вузы выпускают по 5000 человек в год. И эта цифра в последнее время, если и растёт, то незначительно.

ОБРАТНАЯ СТОРОНА ЗОЛОТОЙ МЕДАЛИ

ПОТЕРИ НА ПУТИ ОТ ПЕРВОКУРСНИКА
ДО МОЛОДОГО СПЕЦИАЛИСТА
СОСТАВЛЯЮТ ОТ 40 ДО 80%!¹



Марина БРОДСКАЯ
обозреватель
BIS Journal

ОБЫЧНЫЕ НОВОСТИ

К 2024 г. Россия должна стать одним из мировых лидеров в области информационной безопасности, — прописано в национальной программе «Цифровая экономика РФ». В то же время, как было отмечено в ноябре на SOCFORUM-2018, задержка в выполнении программы по разделу ИБ составляет один год, государственное финансирование формально открыто, но денег до исполнителей доведено ноль рублей.

По мнению экспертов Фонда развития интернет-инициатив, в России в ближайшие 10 лет потребуется 2 млн IT-специалистов. Нехватка разработчиков усугубляется перекосом в сторону разного рода администраторов, тестировщиков, консультантов и специалистов по безопасности. По оценкам этих экспертов, вузам необходимо набирать ежегодно не менее 100 тыс. человек при одновременном повышении качества обучения и целевого трудоустройства выпускников. Только таким образом можно воспитать новое поколение, которое через 10 лет будет конкурировать с IT-отраслями других стран.

О том же говорили и на заседании комитета Ассоциация предприятий компьютерных и информационных технологий, посвящённом образованию. Директор компании «1С» Борис Нуралиев сообщил, что сегодня в стране насчитывается порядка миллиона IT-специалистов, что составляет менее 1,5% от трудоспособного населения России. Ключевой вывод: в стране наблюдается хронический некомплект кадров IT-профиля. Среди решений про-

блемы — увеличение квот на обучение IT-специалистов за счёт бюджета. Собравшиеся отметили, что ряд университетов может увеличить набор студентов на треть без потери качества их подготовки, но только при содействии государства.

Порой кажется, что атака на «отсталое» фундаментальное образование идёт по итогам опроса рынка. Так, по данным российского отделения компании SAP, по профилю, указанному в дипломе, сегодня работают 41% опрошенных айтишников, многим пришлось повышать квалификацию и учиться дополнительно (38%), а есть и те, кто не имеет классического профильного образования (21%). Конечно, программист с дипломом повара, не может не вызывать вопросов у службы кадров, однако таких «историй успеха» немало. При этом эксперты неумолимы: таким «умельцам» не хватает фундаментальных знаний для аналитической работы, в первую очередь в сфере кибербезопасности.

Да, сфера ИБ не столь популярна у поваров и кондитеров, так как требует профильного или близкого к нему образования. И в мире мы тут далеко не первые. По оценкам аналитиков компании IBM, к 2020 г. в мире ожидается 1,8 млн вакансий для специалистов по ИБ, которых некому будет заполнить. Frost & Sullivan даёт близкую цифру — 1,5 млн вакансий в сфере ИБ к 2020 г. Сегодня уже более 70% компаний испытывают сложности при найме безопасников.

ПРО БАНКОВСКУЮ БЕЗОПАСНОСТЬ

В феврале 2018 г., на X Уральском форуме «Информационная безопасность

финансовой сферы», заместитель председателя ЦБ Руслан Вестеровский заявил со ссылкой на Министерство образования, что до 2020 г. организациям в стране потребуется 21 тыс. новых специалистов по ИБ. При этом ежегодно вузы выпускают 6 тыс. человек. Р. Вестеровский вполне ожидаемо предложил увеличивать квоты для студентов, поступающих на специальности по направлению ИБ.

По оценкам BIS Journal, который уже несколько лет проводит анализ вступительных кампаний, в 2018 г. в некоторых университетах действительно выросло число мест для абитуриентов, поступающих в вуз на коммерческой основе, однако существенного изменения с бюджетными местами не произошло. Конкурс на бюджетные и платные места был большим, проходные баллы выросли, чем успели похвастаться большинство ректоров, существенно вырос и размер оплаты... Однако...

ПОСТУПИЛИ. ЧТО ДАЛЬШЕ?

Как в любой сказке, история будущих студентов заканчивается в момент «свадьбы», то бишь зачисления в вуз. А вот долго ли и счастливо учатся вчерашние абитуриенты, все ли доходят до выпуска — нам не ведомо. Ректоры не спешат делиться успехами вчерашних победителей и призёров олимпиад, что уж там говорить об обычных выпускниках школ.

Первый и, кажется, последний раз о количестве отчисленных в процессе учёбы представители университетов серьёзно говорили в 2012 г. Примерно 15% студентов МГУ не сдают курсовые работы, зачёты и экзамены, ещё 15% имеют хвосты по итогам сессии. Об этом говорил ректор МГУ Виктор

¹ Публикация подготовлена в рамках проекта «Безопасность цифровой экономики Москвы: Новое поколение», поддержанного грантом Мэра Москвы №085-МГ/18

Садовничий. В среднем 5% студентов ежегодно не справляются с программой и их отчисляют. Таким образом, примерно четверть учащихся отсеивается в процессе учёбы и не оканчивает МГУ.

Осенью 2012 г. тема отчислений была продолжена на пресс-конференции, устроенной в редакции «Комсомольской правды». По словам Бориса Падалкина, проректора по учебной работе МГТУ им. Н.Э. Баумана, 12% студентов покидают стены Училища в течение первого курса. «У нас говорят, что с 1-го курса вылетают те, кто не хочет учиться, со 2-го, — кто учиться не может, а дальше — кто неправильно распределил свои время, силы и возможности», — говорил тогда проректор.

Отчисленных после первого курса в ВШЭ оказалось ещё больше — 15–20%, — рассказал тогда Григорий Канторович, проректор ВШЭ.

ВШЭ продолжила изучение вопроса и позднее подготовила «Эмпирические исследования. «Изучение отчислений студентов в бакалавриате/специалитете НИУ ВШЭ» (автор Е. Колотова, аналитик Центра внутреннего мониторинга). Согласно приведённым в работе данным, «наибольшая доля студентов, не окончивших вуз, фиксируется в США (54%), наименьшая — в Дании (16%) и Корее (15%). В России на 2008 г. уровень отчислений составлял 21%. По данным на 2008 г. 23% россиян в возрасте до 25 лет имели неполное высшее образование. Среди населения России всех возрастов эта доля составляла 15%».

ОБРАТНАЯ СТОРОНА ЗОЛОТОЙ МЕДАЛИ

Сегодня представители ВШЭ радуются качеству абитуриентов. Так, по словам декана факультета компьютерных наук ВШЭ Ивана Аржанцева, в 2018 г. на факультет поступило рекордное число победителей всероссийских олимпиад по математике, информатике и физике. Согласно данным приёмной комиссии, конкурс на специальности по ИБ превысил 20 человек на бюджетное место, проходной балл — не ниже 280.

Однако стремление учить лучших часто приводит к обратному эффек-

Факт остаётся фактом: в классическом подходе к образованию ситуация выглядит намного печальнее, чем кажется изначально

ту. Как показал опрос преподавателей различных дисциплин, призёры олимпиад и отличники по ЕГЭ уже при поступлении знают предметную область на уровне первого-второго курса и быстро теряют интерес к учёбе. В силу личностных причин многим представителям поколения Z (родившиеся после 1995 г.) часто неинтересны другие предметы. И потому всё чаще со стороны представителей ВШЭ и близких к ней по духу организаций звучит призыв отказаться от традиционного для отечественной высшей школы классического образования. Об этом много говорили на «круглом столе», посвящённом проблемам талантливых студентов, на Форуме инновационных финансовых технологий Finopolis в Сочи.

Какой выход предложили новаторы? Отказ от классической школы, от традиционной системы передачи информации в виде живых лекций преподавателей, переход на проектную деятельность и индивидуальный подход к каждому студенту с учётом его особенностей. А также обучение навыкам коммуникации и презентации, ораторскому искусству и всему прочему, что поможет продать себя и свои разработки работодателю или заказчику. Хорошо ли это? Не знаю, но факт остаётся фактом: в классическом подходе к образованию ситуация выглядит намного печальнее, чем кажется изначально.

ОТСТУПЛЕНИЕ ПРО ПОКОЛЕНИЕ Z

Тут стоит отклониться от темы и вспомнить не о достоинствах, а о проблемах поколения Z. Как отмечают психологи, многие его представители не воспринимают прочитанное, школьные педагоги говорят о росте числа детей с дислексией и дисграфией. Чтение художественных книг для многих — не увлекательное занятие, а непосильная работа. В моду вошли твиты и корот-

кие заметки, текст на 2–5 тыс. знаков (или 2–3 экрана компьютера) стал называться лонгридом (англ. long — длинный и read — читать). Что уж тут говорить о толстых книгах? Связаны ли эти тенденции с физиологическими причинами или с развитием медийных технологий, приучающих с пелёнок к иной, более простой подаче информации, или просто с обилием информации, которую человеческий мозг не желает воспринимать в полном объёме, — неизвестно.

ТЕМ ВРЕМЕНЕМ В ОБЩЕЙ МАСШЕ

Что до представителей многочисленных столичных и региональных университетов, то они везде и всюду рассказывают о соответствии программ обучения Федеральным государственным образовательным стандартам (ФГОС), которые опираются на классический подход. Тот самый, который многие новаторы, да и работодатели, считают устаревшим со всех точек зрения.

Фундаментальная программа включает изучение ряда дисциплин: математики, физики, программирования, основ информационной безопасности, программно-аппаратных средств защиты информации, криптографических методов защиты информации, организационного и правового обеспечения информационной безопасности, технической защиты информации, основ управления информационной безопасностью. Из гуманитарных дисциплин технари традиционно учат философию, историю, иностранный язык. Да, ещё физкультура. Эти предметы входят в базовый блок и обязательны к изучению. Также стандартами предусмотрен набор дисциплин и практик, относящихся к вариативной части программы. Этот набор определяется университетом самостоятельно, дисциплины предлагаются студенту на выбор и становятся обязательными для изучения после решения учащегося.

Кроме того, ФГОС ВО определяет требования к материально-техническому оснащению лабораторий и специализированных кабинетов, которые должны быть оснащены, если не по последнему слову, то на уровне, достаточном для изучения всех процессов на практике. Отдельно стоит отметить, что проблемы коммуникации и презентаций, о которых говорят эксперты ВШЭ, госстандарты не отражают.

На бумаге всё выглядит в общем-то правильно. На практике — проблемы. Многие студенты не понимают, чему и зачем их учат. Кто-то представлял себе будущего специалиста по ИБ как «белого» хакера, а не инженера с кучей рутинных дел, да ещё со знанием нормативной базы. Кого-то привлекла перспектива высокой зарплаты в будущем, а часть выбрала направление ИБ по совету родителей. Чаще всего о том, что учиться в техническом вузе сложно, а по IT и ИБ специальностям вдвойне тяжело, большинство первокурсников не догадывалось.

УДРУЧАЮЩАЯ СТАТИСТИКА

По данным статистики, порядка 40% студентов бросают учёбу в университете, поскольку разочаровались в своём выборе. Кто-то переходит на другую специальность, кто-то полностью меняет профиль. Пятая часть досрочно покинувших студенческую скамью решает, что высшее образование ему не требуется. 10% отчисленных не ожидали, что учиться будет так сложно. Каждый пятый не ожидал, что учёба станет единственным занятием в этот период жизни, не оставив времени на отдых и развлечения. А кто-то, наоборот, не смог совмещать работу и учёбу, таких среди отчисленных те же 20%.

Среди прочих причин отчисления, около 20% бывших студентов называют конфликты с преподавателями и соучениками. Одна из частых причин отчисления — проблемы со здоровьем, а вот материальные проблемы называют всего 7% бросивших учёбу. Согласно аналитическим данным Фонда развития интернет-инициатив, 39% выпускников вузов работают не по своей специальности.

О ПРЕПОДАВАТЕЛЯХ

Ситуация с другой стороны кафедры так же не выглядит оптимистично: не всегда курсы лекций и семинары ведут квалифицированные кадры, нередко случаи, когда преподаватель учит программирование вместе со студентами, пользуясь при этом услугами поисковых систем. Часто причиной значительного отставания от современных достижений в области IT является возраст преподавателей и их заработная плата — прибавка к пенсии. О соответствии учебных программ требованиям времени и об их оперативном обновлении в последние годы говорили многие, однако воз и ныне там...

ПРОСТОЕ РАССЛЕДОВАНИЕ

Поскольку в открытом доступе университеты не приводят статистику отчислений, мы попробовали сами оценить убыль студентов, основываясь на количестве зачисленных на первый курс по конкретной специальности и числе вакантных бюджетных мест по состоянию на 1 сентября 2018 г. Данные приведены по факту, без учёта внутренней миграции студентов с платных на бюджетные места.

Как показывают данные по МИРЭА, где открыты почти все специальности по ИБ, число вакантных мест не столь велико, как можно представить, основываясь на среднестатистических данных. Единственный «провал» — направление специалитета «Компьютерная безопасность», куда в 2015 г. было принято 70 человек на бюджетные места и 41 — на платные. А вот отчислены были 27% учащихся — 19 человек. Ещё больший процент оставивших учёбу к 5 курсу у поступивших в 2014 г. Из 60 бюджетников и 28 платных студентов до пятого курса не «дожили» как минимум 27 человек, или 45% от числа поступивших на бюджет.

Тех, кто окончил бакалавриат (на 2019/2020 учебный год приём составил 40 человек на бюджет и 230 — на коммерческой основе), в магистратуре не очень-то и ждут. На следующий учебный год открыты 30 мест (11 бюджетных и 19 платных), это всего 11% от числа принимаемых в бакалавриат. Утверждения университетов, что мо-

лодой бакалавр по уровню подготовки соответствует дипломированному специалисту старых времён, вызывает горькие усмешки работодателей.

Другой пример — РГГУ, где направление безопасности в части делопроизводства было открыто ещё в 1985 г., а с развитием IT к бумажной безопасности добавилась ещё и компьютерная. Анализ вакантных мест показывает, что при высоком конкурсе среди желающих поступить на специальности сферы ИБ, до окончания бакалавриата дотягивают 70–75% студентов. И, как отмечают окончившие университет в разные годы, по выбранному направлению идут работать единицы. Магистратура по направлению ИБ в РГГУ не открыта.

ТРЕВОЖНЫЕ ВЫВОДЫ

Профессионалы в области ИБ отмечают, что высококлассных специалистов по кибербезопасности в России можно сосчитать по пальцам и они все на виду: являются спикерами на профильных конференциях или публикуют статьи в отраслевых журналах. Компании продолжают переманивать специалистов друг у друга, и с годами (и это на фоне постоянных громких заявлений ректоров университетов и представителей ФУМО о росте числа мест на ИБ в вузах и техникумах, о стремительно растущем конкурсе среди абитуриентов) ситуация только ухудшается. Потому что конечные потери на пути от первокурсника до молодого специалиста, как показывают исследования, составляют от 40 до 80%. То есть вместо заявленных 6–7 тыс. студентов в год, обучающихся по профилю ИБ, до рабочих мест дойдут чуть более одной тысячи. Остальные потеряются в процессе учёбы или пойдут работать по другим направлениям.

Решат ли эти — выстоявшие до выпуска — молодые специалисты задачи, поставленные в программе «Цифровая экономика РФ», и станет ли Россия в 2024 г. одним из мировых лидеров в области информационной безопасности, как заложено в документе? Есть большие сомнения.



Валерия МЕЩЕРЯКОВА
студентка факультета журналистики МГУ им. М. В. Ломоносова

«В РОССИИ НЕТ ПОНИМАНИЯ ПРОФЕССИИ БЕЗОПАСНИКА»

ОТЕЦ И ДОЧЬ БЕСЕДУЮТ О ПРОБЛЕМАХ ОБРАЗОВАНИЯ В СФЕРЕ ИБ¹

В прошлых выпусках я говорила со студентами-безопасниками из разных городов России (BIS Journal №№ 3–4/2018). Узнавала, как дела у сферы студенчества, есть ли, с одной стороны, спрос среди абитуриентов на учёбу, развитие и работу в ИБ, с другой, предложение среди работодателей. В связи с этими исследованиями появилось много вопросов, главный из которых: что происходит с образованием в сфере ИБ?

По случаю новогодних и околопраздников мне удалось поговорить с профессором Романом Валерьевичем Мещеряковым, заведующим Лабораторией 80 ИПУ РАН. Этот разговор интересен для меня, и, надеюсь, для вас: дочь-студентка журфака, некогда собиравшаяся в сферу ИБ, и папа-безопасник, известный своими проектами, говорят об образовании и приобразовательных темах. Правда, споры о физиках и лириках в этот раз остались между строк.

— В чём проблема современного образования в сфере ИБ?

— Я не хотел бы ограничиваться только сферой информационной безопасности. Проблемы образования кроются глубже — в недрах будущего. У нас сейчас немного мест, где готовят разработчиков новых технологий, как это было раньше, а больше тех,

кто будет эксплуатировать существующие решения.

— Когда-то было наоборот?

— Да, после войны: тогда нужно было заново строить страну и вводили всеобщее университетское образование. Так выявляли и «отлавливали» таланты. А когда понадобилось создавать ядерные и космические технологии, образование было направлено на поиск талантов и создание прорывов.

— Так, погоди. А образование в принципе есть в России?

— Есть конечно. И у нас — самое лучшее! А иностранцы, которые говорят обратное, просто завидуют.

— Думаешь? Я вот заметила, сменив кучу школ, что некоторые учителя у нас особенно отличаются неразумностью своих высказываний. Всем что-то не нравится, обвиняют во всех грехах своих «учеников». Это особенность школы или образования в принципе?

— Я бы сказал, что это особенность отдельно взятого учителя или преподавателя. Знаю и таких, кто при каждом удобном случае не преминет любому показать свое превосходство, а студента непременно унижить. Ну и чему такой человек может научить, какому отношению к работе и к жизни? Всё



Профессор Р. В. Мещеряков (в центре) с сотрудниками лаборатории

¹ Публикация подготовлена в рамках проекта «Безопасность цифровой экономики Москвы: Новое поколение», поддержанного грантом Мэра Москвы №085-МГ/18

время ворчать — не дело, только собственным примером и отношением к делу человек может воспитать это чувство в другом.

— Помню, про тебя ещё в Томске шутка ходила: гадание на сдачу экзамена у РВ. Если подбросишь монетку и выпадет орёл — поставит 4, если решка — значит 3. А если монетка повиснет в воздухе, то мооожет быть будет пятерка. Кстати, я таких, кто заставляет думать, встречала только пару человек. Ладно, вернёмся. Как дела у университетов сегодня?

— Сегодня в образовании тяжело: появилось много новых требований. Много говорится об университетах 3.0, 4.0 и так далее. Чтобы пережить этот сложный период, нужно вернуться к истокам. Университет должен быть центром культуры, образования и науки. Без этих трёх составляющих это уже не университет, а какое-то другое место, воспитание личности — неотъемлемая часть учебного процесса. Технические специальности стоит сегодня строить по-новому — как технологические корпоративные университеты. Так они будут целенаправленно обеспечивать потребности предприятий в кадрах для наукоемких производств. Тем более, если мы говорим об университетах как градообразующих предприятиях региона. В общем, знания плюс практика — всё просто (отдавая дань моде и ФГОСам, стоит упомянуть про сформированность компетенции как основного результата обучения).

— Какое должно быть образование ИБ в будущем?

— Сейчас в небольшом количестве университетов учат современному подходу к информационной безопасности. Я имею в виду, что текущий профессорско-преподавательский состав в

силу своего возраста и опыта учит тому, что знает. Это не плохо и не хорошо — это так есть.

Вообще ИБ должно, я думаю, развиваться в трёх направлениях: повышение обороноспособности России (первый рубеж обороны и это разговор для отдельной статьи), обеспечение защиты информации в государственных организациях, коммерческих структурах и т.д. (защита коммерческой тайны, персональных данных, врачебной тайны и других видов тайн) и гуманитарное направление (философские вопросы, этические принципы защиты информации).

Сегодня насущные проблемы, требующие решения, например, обитают в Internet of Things (интернет вещей), Big Data (обработке больших данных, поступающих с сенсоров, поставщиков информации). Большое внимание стоит уделить изучению и пониманию работы с биометрическими данными. На днях прошла новость: уже сделали универсальный отпечаток пальцев, который подойдёт в 70 % случаев. И ещё куча проблем! Случаи подделки речи, изображения лица на фото и видео. На прошлой неделе оппонировал диссертацию, посвящённую противодействию атакам на голос человека. Ещё одна весёлая ситуация произошла в Америке: известной ведущей пришёл штраф за переход дороги в неположенном месте, а в итоге оказалось, что камеры засекли не её саму, а её изображение на автобусе. Таким образом, вопросы идентификации и аутентификации до сих пор не решены (надеюсь, в 2019 году защитится одна докторская диссертация по этому направлению, и будет больше научного базиса).

Сегодня сама атака на систему приспособляется к алгоритмам и методам защиты, и работать в первую очередь надо непосредственно над

техническими каналами утечки информации. И всё это реальность — сегодняшний день, а вот специалист по информационной безопасности должен жить завтрашним днём, чтобы наши с тобой данные были защищены. Это как врач — он должен стремиться не допустить болезни.

— Несколько месяцев я разговариваю с молодыми безопасниками со всей страны. Так вот, те, кто учатся именно на «безопасности», говорят, что после выпуска в эту сферу работать они вряд ли пойдут, ибо работу по профилю найти трудно, особенно в регионах. Что скажешь? Недостаточный спрос, однако, на безопасников или молодёжь сдаёт?

— Нужен мотивированный заказчик на выпускника, а понимание информационной безопасности в обществе, к сожалению, пока не сформировано. Поэтому функции безопасника дают кому-то еще: безопасник в одном случае и юрист, которому одновременно поручают подготовить комнату для переговоров, и та же бабушка на вахте, которая пропуска проверит, или (это если повезёт!) инженер или системный администратор. В первую очередь преследуются экономические интересы — безопасник не производит продукции, он является обслуживающим персоналом и его роль ярко видна, только когда произойдёт инцидент — утекут коммерческие данные. Наиболее распространённый пример, когда функции по информационной безопасности возлагаются на администратора сети. Он и политику настраивает, и сам себя проверяет. Таким образом получается, что он сам себе и закон, и исполнитель, и контролёр. Хорошо, если человек надёжный и морально устойчивый, а если слаб духом? Понятно, что фрилансить и получать сразу большие деньги можно без обучения. С другой стороны, есть и у нашей молодёжи недостаток — маленький опыт.

Безопасники не востребованы не потому что недооценены, а потому что полностью не сформирован запрос общества на их деятельность.

— Думают, что всё произойдёт само собой?

— Именно. Однако, если говорить о заокеанских партнёрах, то за грани-

Университет должен быть центром культуры, образования и науки. Без этих трёх составляющих это уже не университет, а какое-то другое место, а воспитание личности — неотъемлемая часть учебного процесса



Профессор Р. В. Мещеряков (справа)

цей security, safety & privacy — это вообще другое направление, так что сравнить сложно. У наших безопасников узкая специализация, т.к. она формируется профессорско-преподавательским составом и материально-технической базой, на которой проходят обучение и практика. Ситуация, конечно, меняется в лучшую сторону, но всё же... Что-то я повторяюсь начинаю. К сожалению, само собой ничего не произойдёт, нужно целенаправленно работать по изменению ситуации.

— А почему многие даже не доучиваются?

— В мире очевидный дефицит талантов, растёт общество потребления. Не всем дано понять, что такое ИБ: нужно быть безопасником в душе. Скажу непопулярную вещь — не все могут доучиться из-за проблем с базовыми знаниями.

— И какой выход?

— Учить нормально студентов! Чтобы они по выпуску обладали квалификацией (компетенциями по-модному), превышающей «бывалых» сотрудников.

Наработка опыта, с одной стороны, задача самого студента. А университет, со своей стороны, должен быть практикоориентированным, чтобы материально-техническая база позволяла научить школяра в соответствии с требованиями современного мира и перспективой завтрашнего дня. Эти вопросы обсужда-

ются и в Совете Безопасности России, и на пленумах Федерального учебно-методического объединения в системе высшего образования по УГСНП «Информационная безопасность».

— Это все так говорят. А что по сути? Где брать деньги и время молодому студенту на образование вкупе с работой?

— Раз, практика всегда должна быть оплачиваемой. Два, нужно уметь успевать всё, а для этого правильно расставлять приоритеты. Когда ко мне приходили студенты сдавать экзамен или зачёт и плакались, что работают, то я предлагал отчислиться, чтобы учёба не мешала работе. Да и денег всегда не хватает.

— Утром учиться, по вечерам работать в одном месте, в выходные — в другом? Дай совет молодым, что делать, чтобы стать суперпродуктивным.

— Роль личности в истории ещё никто не отменял. Нужно найти нормально-го руководителя (учителя, преподавателя, начальника — называй как хочешь). Расшифровываю, адекватный руководитель — тот, который:

- ◆ может предложить оплачиваемую работу (значит, он заинтересован в своих студентах на перспективу);
- ◆ относится к студентам по-человечески (принимает студента как равного);

◆ увлечён своей работой (горят глаза).

А вообще, самому ставить цели и прилагать усилия для их достижения. Идеально работать в месте, где ты учишься (например, в лаборатории или в центре при университете), тогда и преподаватели будут тебя знать, и опыт хороший заработаешь. И должен быть интерес — без него скучно, мысли должны летать...

Успех любого университета определяется успехом его выпускников. Для правильного преподавателя — радость, когда ученик становится выше своего учителя. У меня много таких, которые достигли больше меня, и я рад, что они есть, ведь они встали на плечи предков. Кстати, я посчитал — преподавал примерно более чем у двух тысяч студентов.

— Бывали случаи, когда к тебе просились в аспирантуру или на диплом, а ты отказывал?

— Конечно. В основном, когда мне неинтересно, чем студент хочет заниматься. Или вижу, что человек не хочет работать. Хотя это редкость, ко мне такие не идут — повезло. И тяжело у меня, жестоким я и требовательный...

Помнится, один из первых дипломников был со средним баллом 3,0. Я был новенький на кафедре и отказаться, понятно, было нельзя. Он три года до этого не мог защититься, но мы победили, в смысле, он защитил диплом. Оценка — это критерий успешности, но только один из них, и нельзя по нему оценивать человека, да и вообще, оценивать человека нельзя, только поступки. Все люди хорошие.

— А где берёшь время на всех своих подопечных?

— Распределяю время. Встречались по вечерам, выходным. Я своих подопечных люблю и уважаю: интересно пообщаться с умными людьми, с теми, которые чего-то хотят, а время — это тот ресурс, который дан нам в ограниченном объёме, его всегда не хватает.

— А дальше что?

— Хочу пожелать всем быть самими собой. А дальше надо жить, радоваться и заниматься любимым делом, несмотря на все трудности, которые нас окружают. Поэтому сейчас работаю над интересными проектами, которые, надеюсь, изменят будущее.



Дмитрий ЛАРИН
историк
криптографии,
кандидат
технических наук

ВЕЛИКАЯ КРИПТОГРАФИЧЕСКАЯ БИТВА

ПОСВЯЩАЕТСЯ 75-ЛЕТИЮ ПОЛНОГО
СНЯТИЯ БЛОКАДЫ ЛЕНИНГРАДА (08.09.1941–
27.01.1944)

СВЯЗЬ ПРЕВЫШЕ ВСЕГО

Когда в конце 1941 г. Ленинград был блокирован немцами, остро встал вопрос о ВЧ связи города с Ленинградским фронтом и Ставкой. Народный комиссариат (НК) связи организовал связь по радио. Воспользоваться ею в полной мере не получилось из-за недостатка шифровальной аппаратуры. Нужна была проводная линия. НК связи и НК обороны приняли решение в экстренном порядке проложить кабель по единственному возможному направлению — по дну Ладожского озера. Прокладка велась уже под обстрелом противника. В результате была организована непрерывная проводная связь по воздушной линии через Вологду на Тихвин, далее по кабелю до Всеволожской, затем опять по «воздушке» до Ленинграда. Таким образом Ставка всю войну имела с Ленинградом устойчивую ВЧ связь [1].

ПРОТИВ ВОЗДУШНОГО ВРАГА

В битве за Ленинград, пожалуй, наибольших успехов радиоразведка добилась в борьбе с немецкой авиацией и дальнобойной артиллерией. Выход немецких войск на ближайшие подступы к городу лишил нашу ПВО возможности своевременно предупреждать истребительную авиацию, зенитную артиллерию и население о подходе вражеских бомбардировщиков. Командующий Ленинградским фронтом — в то время генерал армии Г. К. Жуков — по-

требовал от разведки обнаруживать немецкие самолёты с момента их взлёта с аэродромов. Это оказалось возможным.

Ленинградские радиоразведчики первыми обнаружили радиосвязь немецкой авиации в УКВ-диапазоне. Пионером на этом направлении был инженер К. И. Дроздов. С 1942 г. на ленинградском заводе им. Козицкого стали производить разведывательные УКВ-радиоприемники для нужд всех фронтов. На Ленинградском фронте действовали 472-й, 345-й и 623-й отдельные радиодивизионы (орд) ОСНАЗ, а также 41-я отдельная радиостанция ОСНАЗ.

Сразу после начала войны радиоразведчики и криптоаналитики активно включились в работу. Уже в 1941 г. они наладили перехват метеорологических сводок, которые передавали шведские радиостанции. Эти сводки очень помогали нашей дальней авиации.

Наши специалисты работали в очень трудных условиях. Сначала сложность состояла в большой удалённости средств радиоразведки от источников информации. После начала блокады — наоборот, стабильность фронта позволила немцам и финнам свести к минимуму применение радиосвязи в войсках. Они стали пользоваться проводной связью.

472-Й ОРД ОСНАЗ

Тяжёлые условия заставили радиоразведчиков искать новые источники информации, повышать эффективность

разведки. Ведущее положение тут занимала старейшая радиочасть Красной армии, бывший 1-й дивизион ОСНАЗ, теперь ставший 472-м. Руководил им опытный радиоразведчик, участник испанских событий Л. Сазыкин. Дивизион был хорошо оснащён техническими средствами и укомплектован грамотными специалистами. Важным фактором эффективности стало и то, что почти все военнослужащие участвовали в советско-финской войне. С одной стороны, противник был хорошо знаком, с другой, радиоразведчикам не пришлось тратить время на боевое слаживание.

Первый серьёзный успех был достигнут уже 24 июня 1941 г. В разведотделе фронта отработали карту аэродромов Финляндии и Северной Норвегии с указанием координат и числом базирующихся там самолётов. В этот основополагающий документ вошли и данные от радиоразведчиков и криптоаналитиков. 25 июня вся эта армада фашистских бомбардировщиков должна была нанести удар по Ленинграду. Пользуясь разведанными, авиация Северного фронта и Балтийского флота нанесла упреждающий удар по аэродромам. Было уничтожено 130 вражеских самолётов.

11 июля, несмотря на большое удаление дивизиона от линии фронта, радиоразведчикам удалось вскрыть дислокацию и маршруты движения дивизий



**ФОНД
ПРЕЗИДЕНТСКИХ
ГРАНТОВ**

Публикация подготовлена с использованием средств гранта Президента Российской Федерации на развитие гражданского общества №18-2-012576, представленного Фондом президентских грантов.



Расчет звукоулавливателя ЗТ-5 на крыше бастиона Петропавловской крепости в Ленинграде

немецкой 4-й танковой армии. Захватив Псков и пытаясь развить успех, немецкое командование отдало приказ войскам взять Ленинград сходу. Но предупреждённое радиоразведкой советское командование приняло меры, и враг был остановлен под городом Лугой. Потерпев неудачу, немцы решили скрытно обойти Лугу с запада, нанести удар по Кингисеппу, выйти на Копорское плато и через Красное село войти в Ленинград. Но и этим планам не удалось сбыться, специалисты 472-го орд ОСНАЗ вновь предупредили командование, и их данные подтвердили воздушная и войсковая разведки.

СМЕНА ВЕКТОРА

Немцы не оставляли попыток взять Ленинград штурмом, но все их попытки провалились. Было принято решение о блокаде — удушении города голодом, систематическими артиллерийскими обстрелами и авиационной бомбардировкой. В этих условиях изменились

задачи радиоразведки. Главным стало добывание данных об авиации и артиллерии противника, чтобы противодействовать авианалетам и артобстрелам.

6 сентября 1941 г. Ленинград подвергся первой бомбардировке. Обстановка для борьбы с авиацией сложилась крайне неблагоприятная. Посты ВНОС (воздушного наблюдения, оповещения и связи) оказались в пределах города. Фашистским самолётам требовалось несколько минут, чтобы долететь от линии фронта до жилых домов Ленинграда. Противовоздушная оборона лишилась возможности своевременно предупреждать нашу истребительную авиацию, зенитную артиллерию и население города о приближении бомбардировщиков.

Тут на помощь и пришли радиоразведчики и дешифровальщики. Они прослушивали радиообмен в районе вражеских аэродромов, засекали время старта бомбардировщиков, устанавли-

вали их курс и следили за ними во время полёта, чтобы наши истребители могли встретить их на подлёте.

РАДИОБИТВА

Наши радиоразведчики начали с тщательного изучения особенностей радиосвязи в немецкой авиации, установили сигналы скрытого управления при боевых вылетах, выявили признаки, указывающие на подготовку самолётов к взлёту и подъём в воздух, организовали обнаружение бортовых радиостанций бомбардировщиков в средневолновом и коротковолновом диапазонах. По характеру радиообмена ведущего самолёта определялось число машин в группе и их тип. Благодаря всему этому немецкие самолёты засекались ещё в 150–190 км от города. Предупреждение о подлёте вражеской авиации передавалось на главный пост ВНОС ПВО за 25–30 мин.

Немцы, в свою очередь, тоже были не лыком шиты, они предпринимали меры по противодействию нашей ради-



Батарея 85-мм зенитных орудий обр. 1939 (52-к) на Университетской набережной в блокадном Ленинграде

оразведке. Сокращалось время сеансов связи самолётов с наземными службами. Это заставило наших специалистов изыскивать новые тактические приёмы. Были созданы специальные группы поиска и наведения в приёмных центрах дивизионов, на радиопеленгаторных пунктах.

Талантливый инженер старший лейтенант К. Дроздов с помощью трофейного ультракоротковолнового приёмника, снятого со сбитого немецкого самолёта, обнаружил радиосвязь немецких самолётов в УКВ диапазоне. Данные, добытые Дроздовым, оказались настолько важны для определения действий вражеской авиации и дальнбойной артиллерии, что новому источнику разведки было уделено особое внимание. Срочно сформировали спецподразделение под руководством того же Дроздова, которое занималось авиаразведкой в УКВ диапазоне, и с весны 1942 г. до снятия блокады не было случая, чтобы радиоразведчики не отследили групповой вылет вражеских самолётов.

«ЛЕДОВЫЙ УДАР»

Особое значение придавалось радиоразведке переговоров люфтваффе, связанных с авианалётами на «Дорогу жизни». Зимой 1941–1942 гг. орд ОСНАЗ предупредили ПВО о более 2 тыс. вылетов. Весной 1942 г. активность враже-

ских бомбардировщиков заметно возросла. Немцы готовились к операции «Ледовый удар» с целью уничтожить наши боевые корабли на Неве и другие важнейшие объекты. Первый массированный налёт люфтваффе провели 4 апреля 1942 г. В воздух поднялось около 150 бомбардировщиков. Однако ПВО Ленинграда была вовремя предупреждена и «Ледовый удар» не принёс немцам ожидаемого результата. В тот день они потеряли больше 60 самолётов.

С открытием навигации на Ладожском озере задачи радиоразведки усложнились. Теперь командование фронтом требовало не только предупреждать о подъёме авиации, но и выявлять потенциальные цели, такие как причалы, станции погрузки и разгрузки. Подсчитано, что за время навигации немецкие самолёты появлялись над Ладожским озером более 5 тыс. раз.

К концу 1942 г. нашими специалистами была полностью выявлена сосредоточенная вокруг Ленинграда группировка противника. Удалось определить число соединений Германии и Финляндии, места их дислокации, аэродромы финских ВВС и частей люфтваффе в Финляндии, Норвегии, а также в полосе действия войск Ленинградского фронта. Специалисты дивизиона своевременно сообщали о налётах вражеской авиации [3].

АРТОБСТРЕЛЫ

Постоянные налёты вражеской авиации, бомбардировки и обстрелы с воздуха — это лишь часть проблем, с которыми столкнулся блокадный Ленинград. Ещё одним «бичом» стали обстрелы дальнбойной артиллерии. 4 сентября 1941 г. в 11.00 начался первый артобстрел Ленинграда. Он продолжался до 18.00. Именно в этот день появились первые убитые и раненые, первые разрушения.

Основную тяжесть борьбы с вражеской артиллерией несли на себе советские лётчики и артиллеристы. Артиллерийская разведка добилась заметных успехов в определении координат фашистских батарей. В результате нашего огня немцы несли большие потери, и чтобы избежать этого они стали часто менять позиции, отводя пушки всё дальше в тыл, что снижало эффективность огня.

К концу 1942 г. немцы изменили тактику. Ставка была сделана на использование дальнбойной артиллерии. Её огневые позиции находились в 20–25 километрах от города. Таким образом, она оказалась вне зоны досягаемости артиллерийской разведки. Определение координат вражеских пушек осложнялось и тем, что немецкие орудия были смонтированы на железнодорожных платформах и выдвигались на позиции не раньше, чем за сутки, а после

обстрела быстро уходили в тыл. Для обнаружения их с воздуха времени почти не оставалось.

Надежда была только на радиоразведку. Основная нагрузка легла на уже знакомый нам 472-й орд ОСНАЗ. Вот что вспоминает об этих событиях фронтовой радиоразведчик Глеб Лопаков: «В 472-м радиодивизионе... были обнаружены две радиосети управления огнём дальноточной артиллерии, работающие в коротковолновом и средневолновом диапазонах. В этих радиосетях передавались какие-то условные сокращения и кодовые величины, понять которые было невозможно. Офицеры Ю. Буштуев, И. Дьяков, переводчица лейтенант М. Дикман обстоятельно изучили наставления по управлению артиллерийским огнём и, сопоставив теорию с упоминавшимися выше кодированными величинами, смогли их расшифровать» [2].

ПЕРЕЛОМ

С 12 по 30 января 1943 г. силами Ленинградского и Волховского фронтов была проведена операция «Искра», её результатом стал прорыв блокады Ленинграда. Положение жителей города и его защитников значительно улучшилось, но до полной победы было ещё далеко.

Если раньше радиоразведка Ленинградского фронта отслеживала в основном действия авиации и артиллерии противника, то теперь от неё требовалась работа и по сухопутным войскам. Её силы были направлены на вскрытие расположения вражеских частей, их систему огня, инженерных заграждений. В первую очередь нас интересовала финская «линия Маннергейма». В 1941 г. финны вновь заняли этот район, восстановили оборонительные сооружения, и в 1944 г. советским войскам предстояло штурмовать его ещё раз.

Начальник разведки фронта, оценивая работу частей ОСНАЗ, отметил: «Обычно разведывательный отдел фронта, благодаря радиоразведке, был всегда в курсе последних событий и очень часто информировал оперативный отдел штаба фронта и штабы армий о характере действий наших войск и войск противника в самую последнюю минуту» [2].

Действительно, в ходе проведения операции по полному снятию блокады Ленинграда радиоразведка обнаружила отход стрелнинской группировки противника на левом фланге 18 армии. Это случилось 17 и 18 января 1944 г. 19 и 20 января 472-й орд зафиксировал отвод в глубину обороны командных пунктов 50-го армейского корпуса, 9-й и 215-й пехотных дивизий и выход на рубеж южнее Гатчины 11-й пехотной дивизии немцев. 23 и 24 января радиоразведчики засекли передислокацию командных пунктов 26-го армейского корпуса из Тосно в Вырицу и 56-го армейского корпуса из Сиверской в Лугу. Это говорило о спешном отходе немецких войск на юг и юго-запад.

За две недели наступления советские войска полностью освободили Ленинград от блокады. Однако городу всё ещё угрожали финские войска, нависающие с севера. Чтобы обезопасить город от финнов, командование провело операцию в Карелии и на Карельском перешейке. В ней принимали участие 623-й и 398-й орд ОСНАЗ. Радиоразведчики хорошо изучили противника, но теперь всё пришло в движение, а командованию требовались срочные данные по изменению обстановки. 623-й орд удалось установить, что перед фронтом наших войск находятся только финские части. Немецких соединений не обнаружили [2].

К концу июля 1944 г. наши войска достигли советско-финской границы. Финляндия прекратила боевые дей-

ствия и вышла из войны. 472-й орд ОСНАЗ был удостоен ордена Красного Знамени.

БОЕВОЙ КРИПТОАНАЛИЗ

В тесном контакте с радиоразведчиками работали криптоаналитики, так как многие, а с 1943 г. практически все немецкие сообщения зашифровывались. Нашим специалистам удавалось вскрывать и немецкие и финские шифры. Ценную информацию получали и из зашифрованных сообщений нейтральной Швеции.

В качестве примера приведём результаты работы дешифровальщиков Краснознамённого Балтийского флота. Только за период 1941–1943 гг. «было раскрыто 256 шифров и кодов Германии (направление возглавлял капитан-лейтенант Семёнов) и Финляндии, благодаря чему прочитано 87362 криптограммы, а это около 100 сообщений в день. Чтение переписки береговых постов немецкой, финской и шведской служб наблюдения позволяло получать ценнейшие сведения о фарватерах, свободных для плавания, о минной, гидрографической и метеообстановке на Балтийском море, об интенсивности движения судов и системе их защиты, что представляло первостепенный интерес для командования флота при планировании боевой деятельности подводных лодок и морской авиации» [6]. Имелись существенные результаты и у дешифровальщиков органов государственной безопасности и армейских криптографов.

ЛИТЕРАТУРА

1. Астрахан В. И., Павлов В. В., Чернега В. Г., Чернявский Б. Г. Правительственная электросвязь в истории России. Часть I (1917–1945). М., Наука, 2001.
2. Болтунов М. Е. «Золотое ухо» военной разведки. М.: Вече 2011.
3. Бурнусов И. Мэтр радиоэлектронной разведки // Независимое военное обозрение № 35, 2009, с. 15.
4. Бутырский Л. С., Ларин Д. А., Шанкин Г. П. Криптографический фронт Великой Отечественной. Монография. М.: Гелиос АРВ, 2017.
5. Дадуков Н. С., Репин Г. А., Скачков М. М., Филин Ю. П. Советская шифровальная техника. Ленинградский период: 1935–1941. Часть 1–6. // Защита информации. INSIDE. № 1–6, 2006.
6. Куличенко В. Русские против «Энигмы» // Независимое военное обозрение № 40, 2004, с. 7.

ШИФРЫ ДВУХ ОКЕАНОВ

ДЕШИФРОВАЛЬНАЯ СЛУЖБА ВОЕННО-МОРСКОГО ФЛОТА В ГОДЫ ВЕЛИКОЙ ОТЕЧЕСТВЕННОЙ ВОЙНЫ¹

Заслуживает интереса деятельность дешифровально-разведывательной службы (ДРС) Главного морского штаба в годы Великой Отечественной войны. В образованном 30 декабря 1937 г. Наркомате ВМФ в Управлении разведки было создано 7-е отделение (в дальнейшем 11-й отдел), в задачу которого входила организация и руководство дешифровальной работой. Подготовка флотских криптоаналитиков осуществлялась на криптографических курсах, организованных при Академии Генштаба РККА. В мае 1939 г. и феврале 1941 г. на флот было направлено больше 40 специалистов, которые стали ядром ДРС во время ВОВ. Весьма незначительная по численному составу, не превышающая 150 человек, ДРС ВМФ СССР показала высокую эффективность. Эта служба непрерывно выдавала достоверные разведданные самого разного содержания, в том числе и стратегического значения.

ДИСПОЗИЦИЯ

Советским морякам-криптоаналитикам противостояла очень сильная шифровальная служба ВМС Германии, обладавшая легендарной роторной шифровальной машиной «Энигма», которой были оснащены крупные корабли, подводные лодки, флагманские корабли соединений лёгких сил, штабы морских и воздушных баз. Широко применялись также различные ручные шифры и коды.

Особенности боевой деятельности немецких ВМС (тенденция к сохранению больших кораблей, что привело, с одной стороны, к отсутствию крупных морских операций с участием линейных сил, а с другой, к широкому привле-

чению против нашего флота авиации, лёгких и вспомогательных сил, управление которыми осуществлялось в низовом звене и практически полностью контролировалось с нашей стороны) в какой-то мере компенсировали недоступность информации, закрытой машинным шифром, для анализа которого просто не было ни сил, ни времени, ни условий. В подобной ситуации даже тот факт, что наши криптографы не читали переписки, закрытой машиной «Энигма», не оказал отрицательного влияния на освещение обстановки на море [Куличенко, 2004].

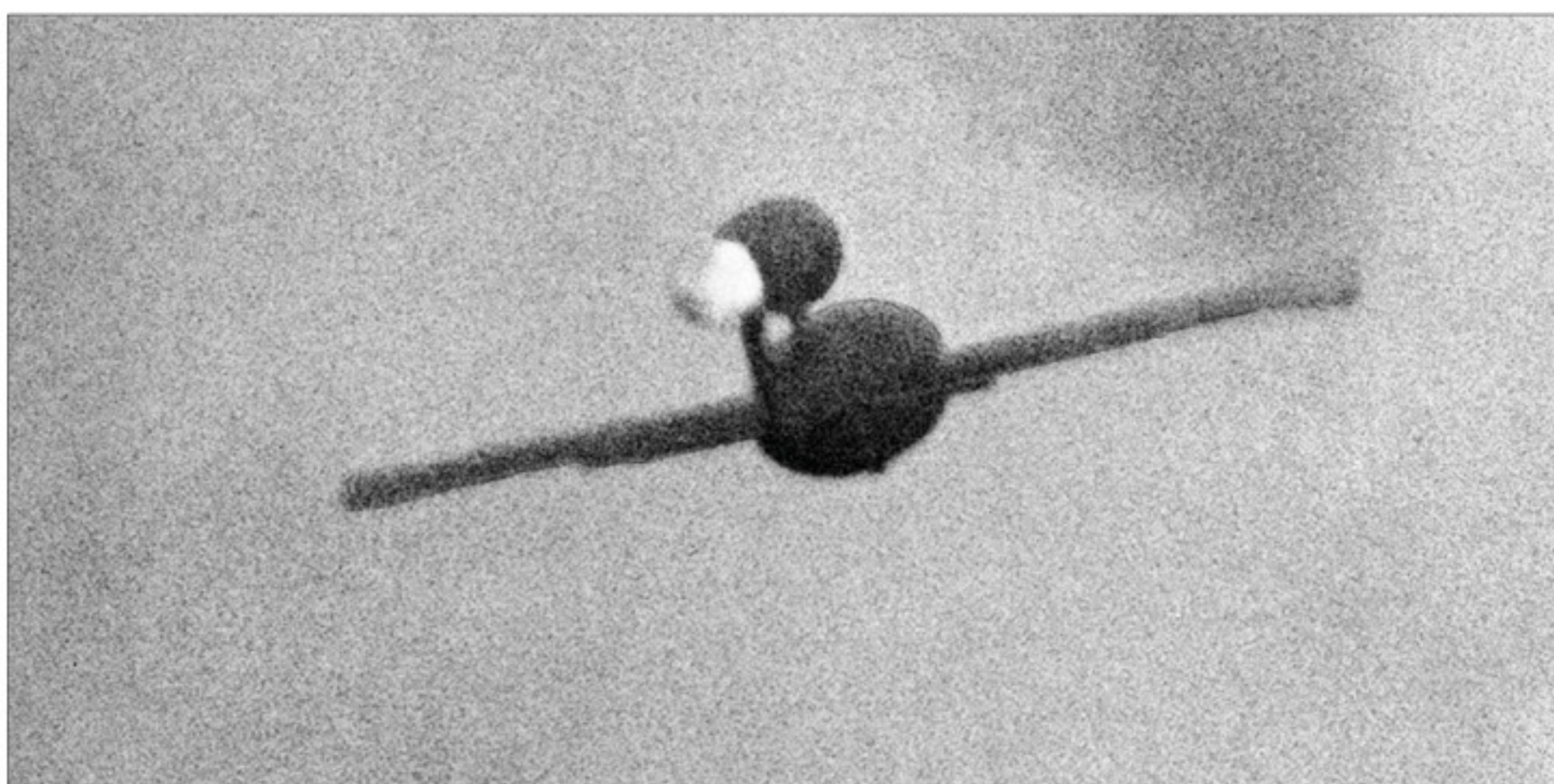
Объектами морской разведки стали не только собственно морские силы Германии и её союзников, но также и приморские группировки сухопутных войск, и в первую очередь авиации — главной ударной силы немцев в войне против СССР. Всего морскими дешифровальщиками было вскрыто более 300 кодов и шифров Германии, её союзников и нейтральных государств и прочитано несколько сот тысяч радиogramм.

Повторюсь, управление немецкой авиацией и лёгкими силами немецкого флота практически полностью контролировалось нашими криптоаналитиками. Очень помогала болтливость союзников Германии, «оповещающих» своё командование о стратегических

планах, тщательно скрываемых самими немцами. А также феномен ведомственности, когда сохраняется «своя» тайна, а «чужими» секретами пренебрегают. Так, из переписки авиации подчас становилось известно о предстоящих операциях сухопутных войск, для обеспечения которых предпринимались те или иные акции ВВС. Успешному раскрытию любых шифрсистем сопутствовал не только каждодневный упорный труд, но и аналитическое осмысливание происходящих изменений и их динамики, что позволяло в ряде случаев добиваться успеха там, где это, с точки зрения теории, казалось невозможным [Куличенко, 2004].

ДВАЖДЫ КРАСНОЗНАМЁННАЯ БАЛТИКА

Специалистами ДРС Краснознамённого Балтийского флота (КБФ) только за период 1941–1943 годов «было раскрыто 256 шифров и кодов Германии и Финляндии, благодаря чему прочитано 87362 криптограммы, а это около 100 сообщений в день. Чтение переписки береговых постов немецкой, финской и шведской служб наблюдения позволяло получать ценнейшие сведения о фарватерах, свободных для плавания, о минной, гидрографической и метео-



Немецкая крылатая ракета Фау-1 (V-1) в полёте

¹ Публикация подготовлена с использованием средств гранта Президента Российской Федерации на развитие гражданского общества №18-2-012576, представленного Фондом президентских грантов.

обстановке на Балтийском море, об интенсивности движения судов и системе их защиты, что представляло перво-степенный интерес для командования флота при планировании боевой деятельности подводных лодок и морской авиации» [Куличенко, 2004].

Криптоаналитики КБФ работали достаточно эффективно, при этом необходимо учесть, что находились они в блокадном Ленинграде. Шло накопление опыта, со временем появилась возможность глубокого анализа шифров и кодов противников, исследование которых ранее не велось из-за недостатка сил и средств [Куличенко, 2004].

Вот что вспоминает В.А. Круглов [Круглов, 1983], служивший в 1942–1945 гг. в 1 морском радиоотряде особого назначения КБФ: «Наш отряд вёл работу, связанную с радиоперехватами, поиском вражеских каналов связи, их центров, объектов особой секретности и т.п. Своими средствами мы должны были искать и находить врага всюду: на суше, в воздухе и на море. В нашу обязанность входило прослушивание эфира на огромном театре действий, на всех доступных нам радиоволнах. Нашему разведрадиопункту пришлось побывать в составе нескольких фронтов: Ленинградского, 2-го и 3-го Прибалтийских. С 1944 г. мы входили в состав 2-й ударной армии и принимали активное участие в обеспечении командования важными радиосведениями, способствовавшими планированию боевых операций».

Весьма ценные сведения специалисты 1 отряда ОСНАЗ КБФ получили при освобождении Прибалтики. «Нам, радистам-осназовцам, было известно, что наступление Ленинградского и Волховского фронтов перепутало все карты немецкой группы армий «Север». Уже с 14 января 1944 г. в эфире звучали (пока ещё шифрованные) её радиосигналы бедствия. По данным нашего радиоперехвата, командующий группой армий «Север» фельдмаршал фон Кюхлер поспешил 22 января на доклад к Гитлеру, который, однако, не дал ему разрешения отойти на Лужские рубежи и к озеру Ильмень. Кюхлер был отстранён от командования, вместо него вступил в должность генерал-полковник В. Модель. Модель, как сообщали

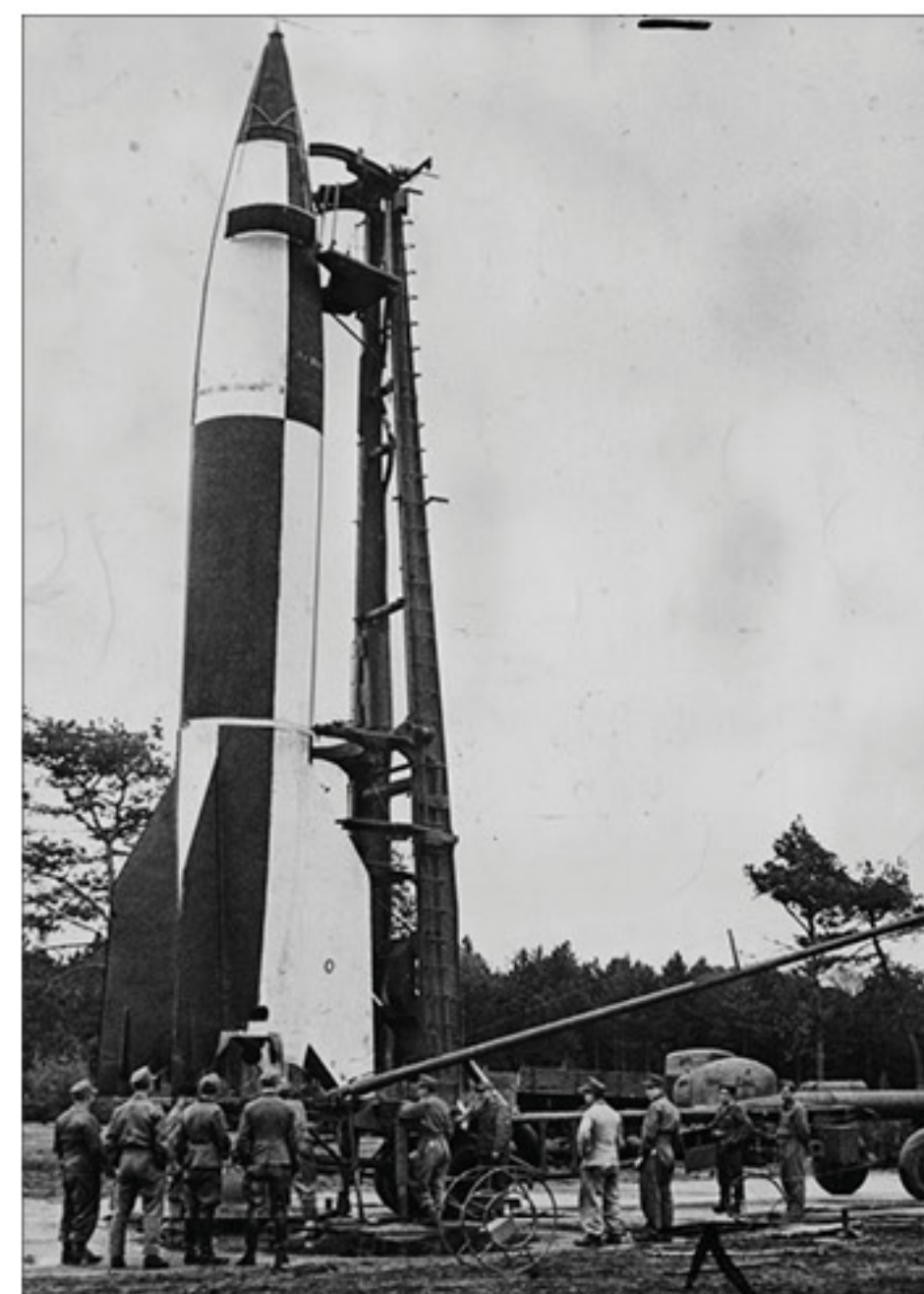
радиоразведчики, без разрешения фюрера всё-таки отвёл свои войска к реке Луга. Таким образом наступление 2-й ударной армии на правом крыле Ленинградского фронта отбросило левое крыло группы армий «Север» к Луге, что позволило нашей 42-й армии выйти к восточному берегу Чудского озера, а 67-й армии Ленфронта вместе с 54-й армией Волховского фронта освободить от врага окрестности Пскова» [Круглов, 1983].

Одним из существенных успехов радиоразведчиков КБФ стало обнаружение и уничтожение полигонов для запуска крылатых ракет ФАУ-1 и баллистических ФАУ-2 в Пенемюнде и Близене. «Полигоны для ФАУ создавались в обстановке строгой секретности. Фашисты надеялись, что успеют опробовать это оружие. В апреле 1945 года, за месяц до окончания войны, Гитлер пытался запугать своих противников этим новым оружием, при помощи которого он хотел уничтожить сначала Англию, а затем отрезать советские войска от Берлина и повернуть вспять колесо войны. Оперативные действия радиоразведки, в том числе и наших разведчиков-радистов в содружестве с польскими группами Сопротивления, помогли вовремя обнаружить полигоны, и они были взорваны» [Круглов, 1983].

НА ЧЁРНОМ МОРЕ

До начала войны Германия не имела флота и морских баз на Чёрном море. Поэтому основные усилия радиоразведки были направлены на Румынию и Турцию — тут и были достигнуты наиболее существенные результаты. «Главной задачей, поставленной перед ДРС Краснознамённого Черноморского флота (КЧФ), являлось добывание разведанных в интересах обеспечения обороны приморских баз и проведения противоблокадных действий, что имело исключительно важное значение для общего положения фланга армии и наших морских коммуникаций» [Куличенко, 2004].

22 июня 1941 г. произошла смена большинства шифрсистем и ключей почти на всех контролируемых до этого каналах связи противника. Но героическая работа советских дешифровальщиков дала свои результаты, уже 25 июня



Подготовка немецкой баллистической ракеты Фау-2 (V-2) к запуску

советские специалисты вскрыли новые шифры противника. Наиболее ценным источником информации явилась шифропереписка румынского Генерального штаба со своей миссией связи при командующем группировкой немецких вооружённых сил на юге СССР фельдмаршале Манштейне.

«В результате чтения переписки командование ЧФ имело исчерпывающую информацию не только о текущей боевой обстановке, но и о некоторых стратегических замыслах врага. Вот несколько примеров полученной информации от криптографов ЧФ:

- ◆ боевые приказы о штурме Одессы, Севастополя, Новороссийска;
- ◆ планировавшееся направление главного удара в районе Курска в предстоящей летней кампании 1943 г.;
- ◆ подготовка покушения на глав правительств союзных держав во время предстоящей Тегеранской конференции;
- ◆ условия, при которых Турция вступит в войну с Советским Союзом;
- ◆ план увода (или уничтожения) румынского флота, разработанный немцами в связи с наступлением советских войск» [Куличенко, 2004].

Полученная дешифровальщиками КЧФ информация была высоко оценена руководством страны. Летом 1942 г. Верховный главнокомандующий



Советская батарея береговой обороны Севастополя, успешно отражавшая огневые налёты немцев на город и нанёсшая серьёзные потери немецкой артиллерии

И. В. Сталин высоко оценил работу ДРС КЧФ, заявив: «Если бы не было разведки Черноморского флота, я не знал бы обстановки на Юге» [Куличенко, 2004].

При этом стоит отметить, что ДРС КЧФ не имела на вооружении даже элементарного оборудования для механизации трудоёмких криптоаналитических процессов. Советские специалисты работали в прифронтовой полосе при постоянном боевом воздействии противника, в сложных бытовых условиях. Вот что вспоминает криптоаналитик Зайцев: «Устроились в недостроенном туннеле для аварийного спасения, пробитом между штольнями, отгородившись от внешнего мира брезентом; брезентовая же занавесь отделяла нас от Уманского (радист-перехватчик — В.К.), первоклассного специалиста, не пропустившего ни одного донесения в Генштаб командующего румынским горно-стрелковым корпусом, вместе с немцами штурмовавшего город. (Севастополь, июнь 1942 г.)» [Куличенко, 2004].

СЕВЕРНЫЙ ФЛОТ

Советская радиоразведка активно работала в Заполярье. Радиоперехват вели специальные береговые радиостанции, морские суда, в том числе и гражданские, полярные станции. Боевые задачи, поставленные перед дешифро-

вально-разведывательной службой Северного флота (СФ), определялись целями, преследуемыми силами флота. Кроме активной борьбы с противником, приходилось осуществлять и защиту наших внешних морских путей, по которым доставлялись грузы из Англии и США.

Самое малочисленное — по сравнению с другими флотами — подразделение криптографов-североморцев (за всю войну через службу прошли всего 15 человек) в целом справилось со всеми задачами. Всего за годы войны вскрыто 9 кодов и 575 их вариантов, прочитано свыше 55000 криптограмм, исходящих от самолётов и авиабаз, что позволило контролировать закрытую переписку ВВС Германии. Также было раскрыто 26 шифров и 13 кодов, ис-

пользуемых силами береговой обороны, аварийно-спасательной, маячной и радионавигационной службами, и прочитано около 3 тыс. криптограмм. При этом у криптологов Северного флота, похоже, не было никаких подручных электромеханических и компьютерных средств, имевшихся в изобилии у их коллег по антигитлеровской коалиции. Только мозговые усилия... И огромное желание внести посильный вклад в разгром Третьего рейха.

Особое внимание уделялось радиообмену немецких подводных лодок. Неоднократно фиксировались сеансы связи немецких подлодок и радиостанций, находящихся на территории СССР. Обнаруживали следы работы немцев в советском Заполярье и после окончания войны. Например, во время осмотра брошенного немецкого наблюдательного пункта на острове Вардропер были найдены радиодетали и кусок антенны [Гольев, 2006], [Гольев, 2008], [Ковалёв, 2006], [Куличенко, 2004], [Лещенко, 2010].

Немецкие подводники использовали для связи различные средства: радио, свет, звук. В конце лета 1943 г. в районе мыса Желания (архипелаг Новая Земля) акустикам тральщика, входившего в советский конвой, с помощью гидрофона «удалось выявить признаки сразу четырёх ПЛ противника, которые, находясь в проливе, обменивались между собой четырёхзначными текстами по звукоподводной связи» [Ковалёв, 2006]. Очевидно речь идёт о каких-либо шумовых эффектах, например, ударах о металлические предметы, которые гидроакустик другой лодки мог слышать на довольно значительных расстояниях. Во второй половине войны немец-

Расположение лодки	Дистанция от «Голиафа»	Глубина антенны
Северный бассейн	1000 км	14–24 м
Средиземноморский бассейн	2300 км	12–17 м
Бискайский залив	—	≤30 м
Индийский океан	6000–8000 км	7–14 м

Таблица 1. Возможности радиостанции «Голиаф» для связи с немецкими подлодками в различных районах Мирового океана



Антенное поле радиостанции «Голиаф»

кие подводные лодки могли принимать радиосообщения, даже находясь под водой на глубине до 20 метров. Световая сигнализация применялась, как правило, для переговоров между всплывавшими подлодками и судами обеспечения.

Для координации действий немецких подлодок из так называемых «волчьих стай» в 1943 г. у города Кальбе в Германии была построена новая сверхдлинноволновая радиостанция «Голиаф» с исключительно высокой мощностью передатчика — 1800 кВт, что в диапазоне 15–60 кГц обеспечивало связь с подводными лодками на расстоянии до нескольких тысяч километров в зависимости от глубины погружения антенны (см. таблицу 1).

Радиостанция «Голиаф» представляла собой мачтовое поле, где в качестве антенн служили кабели, растянутые между мачтами. Передающие антенны «Голиафа» состояли из 3-х зонтичных частей, расположенных вокруг трёх опор, представляющих собой стальные трубы высотой 210 м. Углы антенн закреплены на решетчатых мачтах высотой 170 метров, расположенных в вершинах правильных шестиугольников.

Эта станция позволяла связаться с подлодкой практически в любой точке мирового океана, даже в районе Карибских островов. Однако немецкие подлодки, базировавшиеся в норвежских фьордах, из-за сложного рельефа не имели такой возможности. Связь была односторонней без подтверждения приёма. Поэтому радиопеленгация подлодок союзническими странами была невозможна.

Сообщения для каждой подлодки имели индивидуальные номерные серии и передавались большей частью

ночью, строго по расписанию, иногда несколькими передатчиками одновременно. К моменту связи подлодка выходила на правильную глубину. Эффективность приёма составляла 90%, что являлось хорошим результатом.

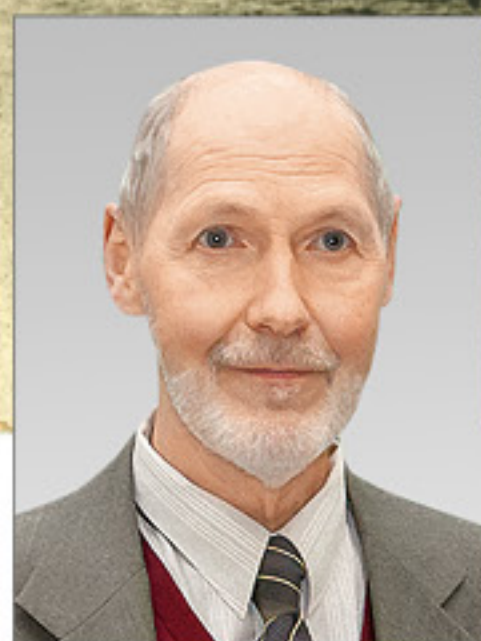
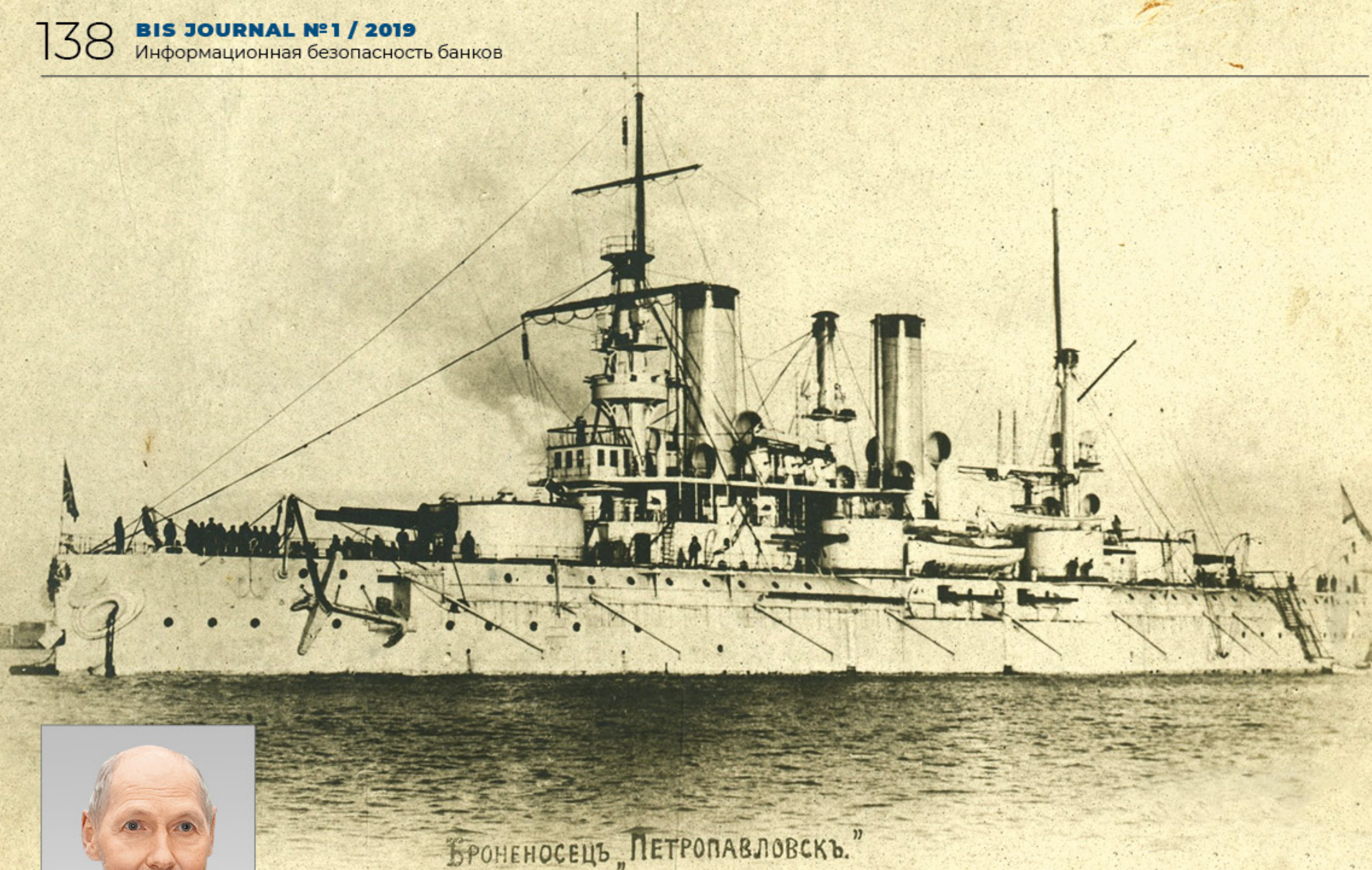
Тем не менее полученная информация тщательно анализировалась разведкой СФ. В результате удалось установить районы действия немецких подводных лодок. Маршруты конвоев стали прокладывать в обход опасных участков. При невозможности обогнуть такой участок туда направлялись дополнительные противолодочные силы и усиливалась охрана транспортных судов. Эти меры позволили существенно снизить потери наших судов, а в некоторых случаях и унич-

тожить врага. В августе 1943 г. в предполагаемом районе действия немецких субмарин патрулировала советская лодка С-101. Наши подводники обнаружили идущую в надводном положении немецкую лодку U-639 и потопили её залпом трёх торпед. На месте гибели U-639 среди плавающих обломков советские моряки обнаружили почти неповреждённую сигнальную книгу [Ковалёв, 2006].

Читали североморские криптоаналитики и шифрпереписку союзников, в частности в 1943 году, как вспоминал командующий Северным флотом адмирал Горшков, он знал о планах английского адмирала Фрезера атаковать немецкий линкор Шарнхорст в декабре 1943 г. [listarchives].

ЛИТЕРАТУРА

1. [АиФ, 2007] Морской «Голиаф». // Аргументы и Факты Нижний Новгород (АиФ Нижний Новгород). 05 сентября 2007 г., № 37, № 7(58) 2003, с. 16–18.
2. [Болтунов, 2011] Болтунов М. Е. «Золотое ухо» военной разведки. М.: Вече 2011. // <http://read24.ru/fb2/mihail-boltunov-zolotoe-uh-voennoy-razvedki/>
3. Война без линии фронта. М.: Воениздат, 1981.
4. [Жельников, 1996] Жельников В. Криптография от папируса до компьютера. М., АБФ, 1996. // <http://www.twinpx.com/file/237431/>
5. [Круглов, 1983] Круглов В. А. Чекисты эфира // Вторая ударная в битве за Ленинград. Л., Лениздат, 1983. Использован текст, размещенный на сайте «Ленинград Блокада Подвиг».
6. [Кузьмин, 1998–1] Кузьмин Л. А. Не забывать своих героев // Защита информации. Конфидент № 1, 1998, с. 83–85.
7. [Кузьмин, 1998–2] Кузьмин Л. А. ГУСС — этап в развитии советской криптографии // Защита информации. Конфидент. № 4, 1998, с. 89–94.
8. [Кузьмин, 1999] Кузьмин Л. А. Становление кафедры криптографии // Защита информации. Конфидент. № 1–2, 1999, с. 85–90.



Борис СТОЛПАКОВ
историк криптографии, кандидат
физико-математических наук

«ЗАМРИТЕ СО СКЛОНЁННОЙ ГОЛОВОЙ ПРИ ЗВУКАХ ИМЕНИ ЕГО: МАКАРОВ...»

115 ЛЕТ НАЗАД ВПЕРВЫЕ НАЧАЛОСЬ БОЕВОЕ
ПРОТИВОСТОЯНИЕ КРИПТОГРАФОВ В РАДИОЭФИРЕ¹

7 марта 1904 года (далее все даты по старому стилю) в российском флоте впервые появился боевой приказ, предписывающий перехватывать неприятельские радиogramмы. Произошло это в начале русско-японской войны и перехватывать предстояло японские радиосообщения. Забота об информационной безопасности впервые стала одной из важнейших задач флота. Отдал приказ командующий Тихоокеанским флотом вице-адмирал Степан Осипович Макаров.

ИСТОРИЧЕСКИЙ ПРИКАЗ

Напомним содержание этого известного документа.

Приказ № 27 от 7 марта 1904 года, рейд Порт-Артура, «Секретно».

«Принять к руководству следующее: Беспроволочный телеграф обнаруживает присутствие, а поэтому теперь же поставить телеграфирование это под контроль и не допускать никаких отправительных депеш или отдельных знаков без разрешения командира, а в эскадре — флагмана...

Приёмная часть телеграфа должна быть всё время замкнута так, чтобы можно было следить за депешами, и если будет чувствоваться неприятельская депеша, то тотчас же доложить

командиру и определить... приблизительно направление на неприятеля и доложить об этом...

Неприятельские телеграммы следует все записывать, и затем командир должен принять меры, чтобы распознать вызов старшего, ответный знак, а если можно, то и смысл депеши.

Для способных молодых офицеров тут целая интересная область.

Для руководства прилагается японская телеграфная азбука.

Вице-адмирал С. Макаров».

Как видим, для нового боевого приёма в ту пору штабисты ещё не выработали специальной терминологии, даже слово радиogramма ещё не получило признания.

¹ Публикация подготовлена в рамках проекта «Безопасность цифровой экономики Москвы: Новое поколение», поддержанного грантом Мэра Москвы №085-МГ/18

Следует сказать, что сама идея боевого применения радиоперехвата была не нова. Ещё в 1901 году разведкой отмечались попытки организации радиоперехвата на британском флоте во время его манёвров. И это спустя всего 6 лет после открытия самой возможности радиопередачи сигналов!

И ещё. В те мартовские дни 1904 года в Порт-Артуре оказались все будущие организаторы и руководители радиоразведки Балтийского флота: Н. О. Эссен, А. И. Непенин, И. И. Ренгартен, А. М. Щастный, П. А. Новопашенный. Хотя тогда состоялось лишь их первое знакомство с новым полем для противоборства с неприятелем, всё же триумф российской морской радиоразведки в 1914–1916 годах имел порт-артурские корни.

ПЕРВЫЕ ДОСТИЖЕНИЯ

Необходимые кадры ещё только предстояло обучить. Особенно не хватало переводчиков. К этой работе пришлось привлечь даже студентов 2-го курса немногочисленного владивостокского Восточного института. Тем не менее, в течение нескольких суток после появления приказа № 27 почти на всех кораблях и судах Тихоокеанской эскадры, оснащённых радиостанциями, организовали вахты радиоперехвата. Кроме корабельных, к ней привлекли и береговые радиостанции, расположенные рядом с Порт-Артуром и Владивостоком. Уже по активизации радиообмена русские моряки могли понять, что готовятся какие-то действия японского флота, а за счёт перехвата и дешифровки радиোগрамм — узнать подробности (4).

Вахта радиоперехвата была открыта и на эскадренном броненосце «Полтава». Наличие собственного переводчика позволило организовать здесь полноценный пост радиоразведки. Упоминание о нём содержится в дневниковых записях мичмана И. И. Ренгартена, служившего тогда на «Полтаве». Так, в записи за 30 марта 1904 г. отмечено:

«30-го [марта]. Днём 2-й отряд миноносцев вышел в море с целью осмотреть острова Эллиот... Принята японская телеграмма по беспроволочному телеграфу — наш переводчик — студент

По активизации радиообмена русские моряки могли понять, что готовятся какие-то действия японского флота, а за счёт перехвата и дешифровки радиোগрамм — узнать подробности

Лебедев разобрал, что было возможно: «скрытно. зажечь. прорваться» (4).

Согласно литературе по истории войны, японское командование в конце первой декады апреля 1904 г. приняло решение о проведении под Порт-Артуром очередной массовой постановки мин. И уже 9 апреля Морской походный штаб Наместника Е. И. В. известил штаб крепости Порт-Артур:

«Сегодня утром на эскадре были разобраны японские телеграммы по беспроволочному телеграфу, из которых можно предположить, что предполагается новая атака брандеров, и при этом указываются сигналы фонарём для облегчения брандерам подхода».

Немедленно была усилена охрана главной базы флота. Японцы в ночь на 15 апреля провели у Порт-Артура разведку с целью ознакомить с районом предстоящей операции вновь назначенных командиров судов-заградителей. И в эту ночь радиотелеграфисты «Полтавы» вновь осуществили радиоперехват, связанный с предстоящими действиями противника. В результате запланированная операция по постановке мин была сорвана русским флотом (4).

Отличились и моряки отряда кораблей, базировавшихся во Владивостоке. Их задачей был перехват иностранных судов у берегов Японии. Среди различных документов, захваченных русскими моряками на японских судах, оказался телеграфный код.

«Разбор и перевод документа оперативно выполнил А. Занковский, снабдив его весьма толковыми для студента 2-го курса комментариями. Кроме того, на пароходе «Хагинура Мару» была обнаружена зашифрованная телеграмма с исходным текстом. Эти документы были направлены в Морской штаб Наместника Е. И. В., затем их переслали в Санкт-Петербург в Главный морской

штаб, откуда передали в дешифровальную службу Министерства иностранных дел» (4).

Все описанные события происходили уже после гибели адмирала С. О. Макарова на броненосце «Петропавловск» 31 марта 1904 года. Как известно, в боевой обстановке «Петропавловск» подорвался на mine и погиб от взрыва детонирующего боезапаса. Вместе с адмиралом эта трагедия унесла и художника В. В. Верещагина.

СОЧУВСТВИЕ НЕ ЗНАЕТ ГРАНИЦ

Велика была скорбь моряков Порт-Артура, да и всех российских воинов. Но примечательно, что печальная весть о смерти С. О. Макарова вызвала сочувствие и в Японии. Свидетельством тому является стихотворение «Памяти адмирала Макарова», написанное японским поэтом Исикава Такубоку в 1904 году (3). Оно содержит следующие строки (в переводе В. Н. Марковой):

*Враг доблестный! Ты встретил свой конец,
Бесстрашно на посту командном стоя,
С Макаровым сравнив, почтут героя
Спустя века. Бессмертен твой венец!*

*И я, поэт, в Японии рождённый,
В стране твоих врагов, на дальнем берегу,
Я, горестною вестью потрясённый,
Сдержать порыва скорби не могу.*

*Вы, духи распри, до земли склонитесь!
Друзья и недруги, отбросьте прочь мечи!
При имени Макарова молчи, О битва!*

*Сопричислен русский витязь
Великим полководцам всех времён,
Но смертью беспощадной он сражён.*

*Спокойно руки на груди скрестив,
Вперив свой взор в бездонную пучину,
Где в злом торжестве кружился вал,
Исчез навеки славный адмирал...*

*Не наносите яростных ударов!
Замрите со склонённой головой!
Пусть в тишине мой голос огневой
Вас к скорби призовет: погиб Макаров!*



Рисунок 1. Гибель С. О. Макарова. Японский плакат военного времени

Обратим внимание и на японский плакат 1904 года (рисунок 1). В нём нетрудно увидеть уважение к противникам, встречающим смерть в бою.

Авторы стихов и плаката явно различают человеческую суть людей и принесённые извне в их жизнь обстоятельства. Каким же был С. О. Макаров, как он прошёл свой жизненный путь? Обратимся к биографии Степана Осиповича (1), благо в нынешнем году исполнилось 170 лет со дня его рождения в январе 1849 года.

«ТЯЖЕЛО В УЧЕНИИ — ...»

Известно, что отец Степана Осиповича, Осип Фёдорович, был военным. Сын солдата, он начал свою долгую службу матросом, плавал на Балтике. Человек умный и энергичный, он продвигался по службе, стал боцманом, его перевели в Николаев Херсонской губернии. Здесь в его семье родились пятеро детей, младший — Степан. За исправную службу к двадцати пяти годам, перед рождением Степана, Осип Макаров получил первый офицерский чин — прапорщика, а вместе с ним и дворянство.

После Крымской войны по условиям мирного договора Черноморский флот подлежал сокращению и Осипа Фёдоровича весной 1858 года перевели в Сибирскую флотилию, в город Николаевск-на-Амуре. Там он стал водить речные пароходы, совершавшие рейсы по Амуру, дослужился до штабс-капитана. Степан Макаров, которому в момент переезда семьи на Дальний Восток

было всего 9 лет, в сентябре 1858 года поступил в местное морское училище, готовившее штурманов. Со смертью матери, случившейся вскоре, его жизнь резко переменилась. Впоследствии он вспоминал: «С девяти лет я почти никогда не имел случая пользоваться чьими-нибудь советами».

Уже летом 1861 года (в 12 лет!) будущий адмирал совершил свои первые учебные плавания из Николаевска-на-Амуре в залив Де-Кастри Японского моря (ныне залив Чихачёва) и обратно. А в июле 1863 года состоялось его первое плавание к североамериканским берегам на корвете «Богатырь» в составе эскадры. Эта экспедиция продолжалась более полугода. Практически весь 1864 год Степан провёл в длительных плаваниях. Учёба продолжалась и во время рейсов, его многообещающие способности были замечены наставниками.

ЯРКОЕ НАЧАЛО МОРСКОЙ СЛУЖБЫ

21 апреля 1865 года Степан Макаров окончил Николаевское-на-Амуре морское училище первым по успеваемости. После окончания училища он служил на Дальнем Востоке и в ноябре 1866 года на корвете «Аскольд» в составе эскадры совершил переход из Нагасаки в Кронштадт.

14 июля 1867 года в жизни восемнадцатилетнего моряка произошло знаменательное событие — за выдающиеся успехи в освоении наук он был произ-

ведён в гардемарины, подобно воспитанникам Морского кадетского корпуса в Петербурге, хотя ему полагалось только именование кондуктором корпуса штурманов. А в октябре того же года Степан Осипович опубликовал в журнале «Морской сборник» свою первую научную статью, посвящённую новым навигационным инструментам. В 1868 году — дальнейшее плавание на корвете «Дмитрий Донской». После возвращения, летом 1869 года, С. О. Макарова произвели в мичманы, он стал морским офицером. Тогда же появились его новые статьи по проблеме непотопляемости корабля.

ЗВЁЗДНЫЙ ЧАС

В 1876 году Степана Осиповича перевели на Черноморский флот. Здесь настал его «звёздный час». В преддверии войны, в условиях отсутствия у России сильного военного флота на Чёрном море, Макаров предложил переоборудовать быстроходные корабли под транспорты для перевозки минных катеров. Эти катера, доставленные в район стоянки судов противника, должны были атаковать их минами и торпедами. Получив в своё командование пароход «Великий князь Константин», лейтенант Макаров за четыре месяца напряжённого труда переоборудовал его в соответствии со своим проектом. Так началось создание миноносных кораблей и торпедных катеров во флотах морских держав.

К началу русско-турецкой войны, в апреле 1877 года, пароход с катерами на борту встал в боевой строй и уже вскоре начались его рейды к стоянкам турецкого флота. Макаров осуществил несколько успешных атак турецких кораблей своими катерами, при этом впервые использовал новые мины и самодвижущиеся торпеды. Эффективность таких атак вынудила турецкий флот покинуть Чёрное море: Макаров выполнил задачу всего Черноморского флота! И слава нашла героя. Менее, чем за год Степан Осипович получил в качестве наград: золотое оружие с надписью «За храбрость», ордена святого Владимира 4-й степени и святого Георгия 4-й степени, очередные чины до капитана 2-го ранга включительно, придворное звание флигель-адъютанта.

СЛОЖНЫЙ ПУТЬ КОМАНДИРА И УЧЁНОГО

В дальнейшем его командная деятельность на флоте постоянно сочеталась с научными изысканиями. В конце 1881 года С. О. Макаров исследовал течения в проливе Босфор и открыл существование разнонаправленных потоков, его труд «Об обмене вод Чёрного и Средиземного морей» был удостоен премии Российской Академии наук.

В 1886–1889 годах, командуя корветом «Витязь», Степан Осипович совершил кругосветное плавание из Кронштадта. Его путь пролегал через Атлантику, Магелланов пролив, Иокогаму в Японии, Сингапур, Суэцкий канал, Гибралтар. В каждодневных командирских заботах С. О. Макаров выкраивал время для систематических гидрологических и метеорологических наблюдений, результаты которых затем изложил в двухтомной работе «Витязь» и Тихий океан», удостоенной премии Академии наук и золотой медали Российского географического общества. Благодаря прессе, плавание получило широкую известность.

В 1891 г. контр-адмирал Макаров стал главным инспектором морской артиллерии, тогда же началось его сотрудничество с Д. И. Менделеевым. Великий химик составил для моряков бездымный порох, а адмирал изобрёл бронёбойные наконечники к артиллерийским снарядам.

С. О. Макаров, уже начиная с 1895 года, всячески поддерживал радиопыты А. С. Попова, а затем добивался размещения радиостанций на судах Балтийского флота и побережье. Интересуясь возможностями передачи сигналов, адмирал сам разработал для нужд моряков семафорную азбуку.

В 1897 году, уже будучи вице-адмиралом, Степан Осипович опубликовал капитальный труд «Рассуждения по вопросам морской тактики». Он систематизировал свой опыт последних лет, когда ему довелось командовать эскадрами в Средиземном море и Тихом океане. В этом труде с эпиграфом «Помни войну» он изложил свой взгляд на ведение эскадренного боя броненосными кораблями. Девиз «Помни войну» появился и в кабине-



Рисунок 2. Памятник С. О. Макарову в Кронштадте

те адмирала, а много позже и на памятнике С. О. Макарову в Кронштадте (рисунок 2).

В АРКТИКУ — НАПРОЛОМ

В 90-е годы Макаров переключил свою энергию на арктические исследования. Это было время борьбы за славу первенства в покорении Северного полюса, которую мировая пресса всячески подогревала. Но адмирал видел, прежде всего, экономическую потребность в освоении водных северных путей, необходимость морских дорог в устья сибирских рек. В своём докладе «К северному полюсу — напролом» в Академии наук в марте 1897 года он сказал:

«Если сравнить Россию со зданием, то нельзя не признать, что она своим главным фасадом выходит на Ледовитый океан... Мощный ледокол откроет дверь в этом главном фасаде... Природа заковала наши моря льдами, но в настоящее время ледяной покров не представляет более непреодолимого препятствия к судоходству. Я знаю, как достичь Северного полюса: надо построить ледокол такой силы, чтобы он мог ломать полярные льды. Ни одна нация не заинтересована в ледоколах столько, сколько Россия».

Поддержка учёных, прежде всего, П. П. Семёнова-Тян-Шанского и Д. И. Менделеева, обладавших большим авторитетом в правительствен-

ных кругах, помогла добиться необходимых ассигнований на постройку мощного ледокола. Дмитрий Иванович был единомышленником С. О. Макарова и тоже желал возглавить морскую экспедицию в Арктику, несмотря на свой солидный возраст.

Самый мощный в мире ледокол «Ермак» построили в Ньюкасле под наблюдением Степана Осиповича и при его участии в конструировании, в сотрудничестве с молодым инженером-кораблестроителем А. Н. Крыловым, будущим академиком, и британскими инженерами на верфи. В марте 1899 г. новый корабль показал свои возможности, пробившись сквозь метровые льды в Кронштадтскую гавань. Через несколько дней «Ермак» освободил из ледового плена 11 торговых судов недалеко от Ревеля (Таллина).

Освоив ледокол, Макаров возглавил арктические экспедиционные плавания к Шпицбергену, Земле Франца-Иосифа и Новой Земле. Своё видение освоения арктических морей и северных территорий С. О. Макаров обстоятельно описал в книге «Ермак во льдах», доказывая, что ледокол способен и должен работать в Арктике. Он убеждал: «У нас есть корабль, который даёт возможность сделать то, что не под силу ни одной нации и к чему нас нравственно обязывают старые традиции, географическое положение и величие самой России».



Фотопортрет Степана Осиповича Макарова (1849–1904) с автографом

Яркая книга привлекла внимание и зарубежных читателей. Но «Ермак» мог преодолевать далеко не все льды, и Министерство финансов, на балансе которого находился корабль, ограничило его службу проводкой судов на Балтийском море. Лишь в 30-е годы XX века «Ермак» вернулся в Заполярье и до 1964 года прокладывал путь арктическим караванам судов. И всё же мечта адмирала сбылась. Атомный ледокол «Арктика» покорила Северный полюс в 1977 году, спустя 80 лет после знаменитого доклада в Академии наук.

С. О. Макаров приобрёл мировую известность наряду со своим другом Ф. Нансеном и другими популярными в ту пору полярными исследователями. Поэтому его геройская смерть вызвала повсеместный печальный отклик.

ОТЕЧЕСКОЕ НАПУТСТВИЕ СЫНУ

Предчувствовал ли Степан Осипович свою близкую гибель? Пожалуй, да. Судите сами, вот письмо, написанное адмиралом двенадцатилетнему сыну Вадиму в ночь перед роковым выходом в море (2).

Дорогой мой сыночек!

Это моё первое письмо, посланное именно тебе, а не в отрывках в письмах к маме, как бывало ранее. Ты уже подросток, почти юноша, но я обращаюсь к тебе с другого конца России уже как к взрослому мужчине. Письмо посылаю своему старому товарищу

в Кронштадт, он найдёт способ передать тебе в руки.

Вадим, тут идёт жестокая война, очень опасная для родины, хоть и за пределами её границ. Нет, не временный перевес неприятеля в силах тревожит меня. Русский флот, ты знаешь, творил и не такие чудеса. Но я чувствую (о чём ты пока никому не скажешь!), что нам — и мне в том числе — словно бы мешают. Не адмирал Того, нет, а как бы сбоку подталкивают, как бы подкрадываются сзади. Кто? Не знаю. Душа моя в смятении, чего я никогда не испытывал. Начинаю уже чего-то улавливать, но смутно пока. Вот Верещагин Василий Васильевич что-то мне пытается объяснить, но сбивчиво, как все эти художники и поэты (ты им не очень верь, публика эта шальная! Доверяй только людям основательным!). Вот такое у меня настроение, сынок. Но знаешь пока об этом ты один. Молчи, как положено мужчине, но запомни.

И ещё. Объясню уж тебе, почему адресуюсь помимо нашей любимой мамы. Запомни на всю жизнь: на женщин никогда нельзя перекладывать тяготы нашей мужской доли. Иной болван и трус может заявиться домой чуть ли не в слезах и супруге своей с порога: вот на войну посылают вроде... стоит ли... Что скажет тут любящая мать, жена, сестра? «Ни за что, погибнешь, ты у нас один, уклонись уж как-нибудь!» Ну, по-женски понятно, что с них взять. Но настоящий мужчина должен явиться домой бодрым и сказать: ну, дорогая, собирай меня в дорогу, тут на границе весёлое дело предстоит! Она поплачет, соберёт тебя и успокоится, положившись на волю Божию.

Обнимаю тебя, сынок. Учись старательно, помогай маме и сестре. Бога бой-

тись, Царю служите. Твой Макаров-старший. Порт-Артур, 31 марта 1904 года.

ВЕРЕН ЗАВЕТАМ ОТЦА

Читателям, вероятно, интересно будет узнать и о судьбе Вадима, Макарова-младшего. В. С. Макаров (1892–1964?) в 1912 году окончил Морской корпус и был направлен на крейсер «Адмирал Макаров», на котором ему пришлось участвовать в сражениях Первой мировой войны. Февральскую революцию молодой офицер не принял и в мае 1917 года выехал в служебную командировку за рубеж, получив назначение в русскую морскую миссию в США, во главе с А. В. Колчаком.

В октябре 1918 года он добрался из Америки до Омска и в морском министерстве правительства Колчака занимался переоборудованием гражданских судов в боевые корабли. После поражения белых войск в начале 1920 года Вадим Степанович выехал в США. Там он проявил себя как изобретатель, разработал алмазное сверло для бурения нефтяных скважин, конструировал яхты, стал известным яхтсменом. Вторым браком Вадим Степанович был женат на дочери Уильяма П. Хардинга, председателя Федеральной резервной системы США, правда, к моменту их свадьбы уже покойного. В. С. Макаров до последних дней состоял в Обществе бывших русских морских офицеров в Америке. Он жертвовал немалые средства для помощи соотечественникам, и при жизни, и в своём завещании. В 1966 году, через два года после смерти Вадима Степановича, в г. Лейквуде (штат Нью-Джерси) был открыт Русский морской музей, созданный на его средства. Музеем было присвоено имя адмирала Степана Осиповича Макарова.

ЛИТЕРАТУРА

1. Семанов С. Н. Макаров. «Молодая гвардия». М., 1972.
2. Семанов С. Н. Тайна гибели адмирала Макарова. Новые страницы русско-японской войны 1904–1905 гг. «Вече». М., 2000.
3. Такубоку И. Лирика. «Детская литература». М., 1981.
4. Партала М. А. «С включением в списки офицеров флота в Тихом океане» (К теме участия студентов Восточного института в русско-японской войне). <https://cyberleninka.ru>

«О СКОЛЬКО НАМ ОТКРЫТИЙ ЧУДНЫХ ГОТОВЯТ...»

О ВРЕМЕНИ ПУШКИНА И ЛОБАЧЕВСКОГО

Пушкин и Лобачевский были почти ровесниками: Александр Сергеевич родился 220 лет назад, в 1799 году, а Николай Иванович — семью годами ранее. Оба стали знаковыми фигурами для России первой половины XIX столетия.

«ВДОХНОВЕНИЕ НУЖНО В ГЕОМЕТРИИ, КАК И В ПОЭЗИИ»

Историки давно отметили ту связь, которая объединила столь разных, на первый взгляд, великих сынов нашего Отечества: «В тот момент, когда Пушкин печатно признавал роль вдохновения при создании выдающихся произведений «точных» наук, в Казани уже была произнесена речь Н. И. Лобачевского о воображаемой геометрии... Пушкин и Лобачевский были порождены одной и той же эпохой нашего культурного развития» [1]. Это была эпоха общенационального подъёма в России, вызванного победой над Наполеоном. Именно в ту пору стала энергично развиваться система образования и просвещения.

«МАТЕМАТИКА СЛУЖИТ К ИЗОЩРЕНИЮ ЯСНОСТИ В МЫСЛЯХ»

Уже в начале XIX века всё древо российского образования подверглось реформированию, были созданы Министерство народного просвещения, учебные округа, постепенно строилась система Императорских университетов. Первый из 12 Императорских университетов России, Московский, появился, как известно, в 1755 году. А следующие 7 были открыты в 1802–1834 годах. Столичный, Петербургский, был лишь шестым по времени создания. Он открылся ровно 200 лет назад, в 1819 году.

Для подготовки будущих студентов одновременно выстраивалась система гимназического образования. Его устав 1828 года провозгласил математику одним из главных предметов, поскольку она служит «в особенности к изощрению ясности в мыслях, их образованию, проницательности и силе размышления». В недельном учебном плане первых трёх классов, составлявших период общего образования, математике уделялось 6 полуторочасовых уроков.

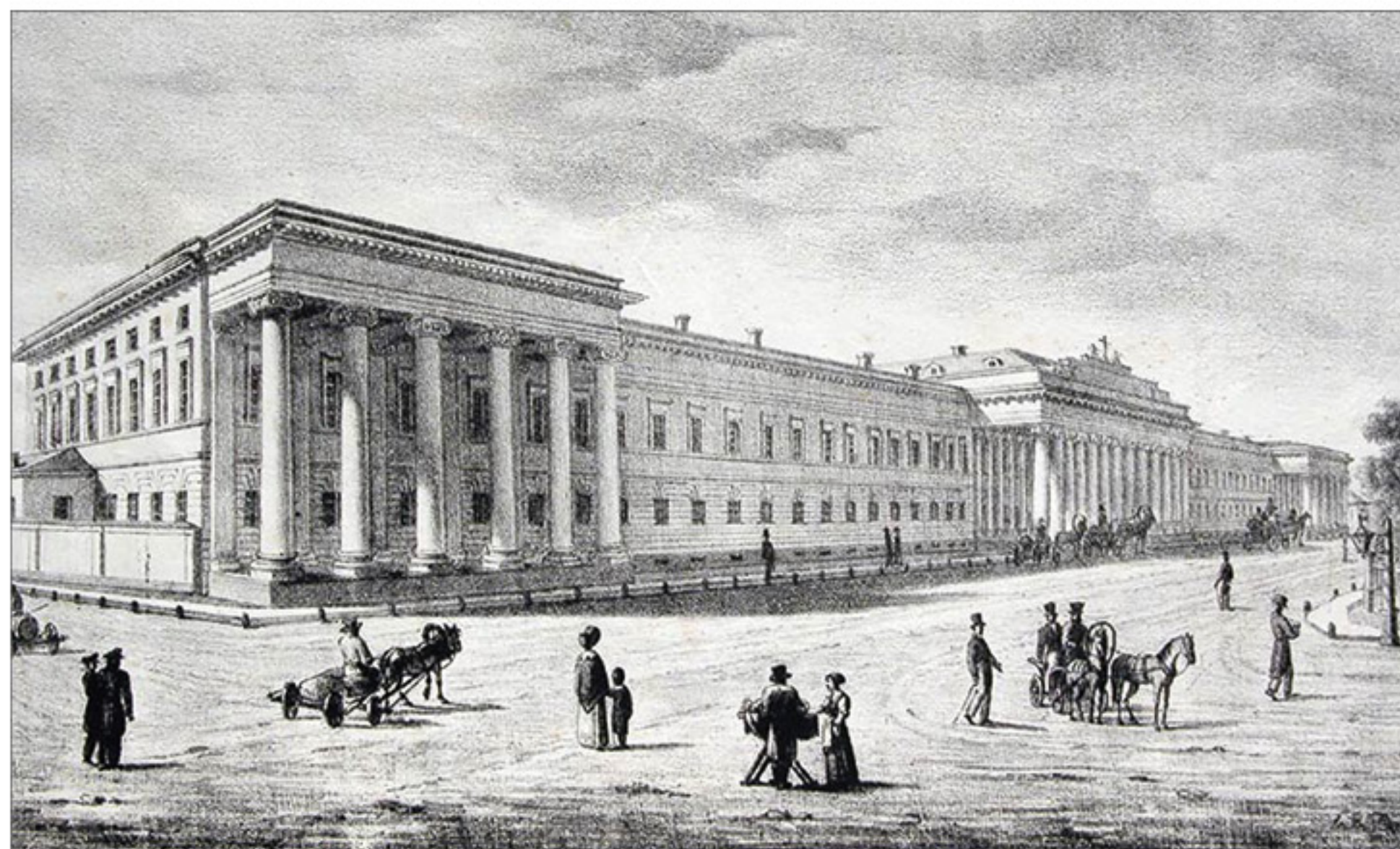
Интересно отношение современников к такому привилегированному положению математики в деле образования молодёжи.

«НАСТАЕТ ВРЕМЯ ТОРЖЕСТВЕННОЕ ДЛЯ НАУК ТОЧНЫХ»

Писатель и дипломат И. М. Муравьев-Апостол, отец декабристов, писал об увлечении, которое «довольно сильно начинает уже вкореняться в домаш-

нем нашем воспитании — именно: исключительное предпочтение математики всем прочим наукам. Математика! Кричат во всё горло те, которые, кроме математики, ничему не учились, — и Математика! повторяет за ними толпа людей, которые и математики не знают, — вот единственная наука, достойная человека!.. Я встречался уже не с одним отцом, который положил себе за правило ничему другому не учить детей, как только математике» [1].

В 1824 году в журнале «Вестник Европы» была напечатана речь П. Морозова, произнесённая в Московском университетском пансионе, где говорилось: «Кажется, настанет время торжественное для наук точных и в нашем отечестве. Обогащённые произведениями духа доблестного и чувства высокого, обладающие одним из прекраснейших языков Европы, мы начинаем чувствовать необходимость строжайших исследований... Потребность математиче-



Казанский университет в 1830-е годы



Портрет Н. И. Лобачевского 1830-х гг.

ских знаний ощущается на всех путях службы; отличное уважение, знаки почестей, путь блистательный сретают (*встречают — авт.*) каждого юношу, посвятившего труды свои сим занятиям» [1].

«КОПЕРНИК ГЕОМЕТРИИ»

В развитии российского образования Н. И. Лобачевский принял весьма заметное участие, хотя мы больше знаем его как великого математика. Николай Иванович родился в Нижнем Новгороде, но почти всю свою жизнь провёл в Казани. Там он учился сначала в гимназии, затем в университете (1807–1811 гг.). После окончания университета был оставлен в нём для подготовки к педагогической деятельности, в 1816 году стал профессором.

Много позже английский математик Клиффорд назовет Лобачевского «Коперником геометрии», удачное сравнение. И Коперник, и Лобачевский ознаменовали своими достижениями начало новых этапов развития науки. Кроме того, они оба получили общественное признание при жизни как эффективные государственные деятели, а вовсе не за новые научные теории. Николай Иванович был деканом физико-математического факультета (1820–25 гг.) и ректором университета (1827–46 гг.), а с 1845 по 1856 годы, до своей кончины, руководил Казанским учебным округом, в который входили всё Поволжье от Астрахани до Вятки, а так-

же Урал и Сибирь. Административная деятельность Лобачевского положила начало процветанию и славе Казанского университета. В 1836 году университет посетил император Николай I и, в знак признания заслуг Лобачевского, наградил его орденом св. Анны II степени, это был уже третий орден Николая Ивановича.

«МЫ РОЖДЕНЫ ДЛЯ ВДОХНОВЕНИЯ!»

Если Лобачевский сыграл весьма заметную роль в российском образовании, то трудно переоценить вклад Пушкина в дело просвещения, о чём каждый из нас знает уже со школы. Такое поприще он наметил для себя ещё двадцатилетним юношей, в стихах заявив о желании «в просвещении стать с веком наравне». Как представляется, Пушкин подразумевал здесь прежде всего пополнение своих знаний в различных областях науки, к чему он постоянно стремился. Позже пришло понимание просвещения как духовного действия, неотделимого от воспитания.

И «стать с веком наравне» было не так-то просто. Само время, в которое жил Пушкин, казалось, демонстрировало торжество научной мысли в России. В 20–30-е годы XIX в. выдающиеся открытия и изобретения следовали одно за другим, привлекая к себе внимание и любопытство широкой общественности: неевклидова геометрия Н. И. Лобачевского и теоремы М. В. Остроградского, важные для физики и техники; «ропись 3112 двойных звёзд, из коих 2392 были до того времени неизвестны», представленная астрономом В. Я. Струве. Открытие Э. Х. Ленцем электромагнитной индукции, а также изобретение Б. С. Якоби электродвигателей и П. Л. Шиллингом электромагнитного телеграфа в начале 30-х годов сделали Петербург одним из мировых центров электротехнических исследований. Закономерно, что первый в Европе электротехнический вуз появился именно там.

ПУШКИН ЗНАКОМИЛ СОВРЕМЕННИКОВ С ТЕОРИЕЙ ВЕРОЯТНОСТЕЙ

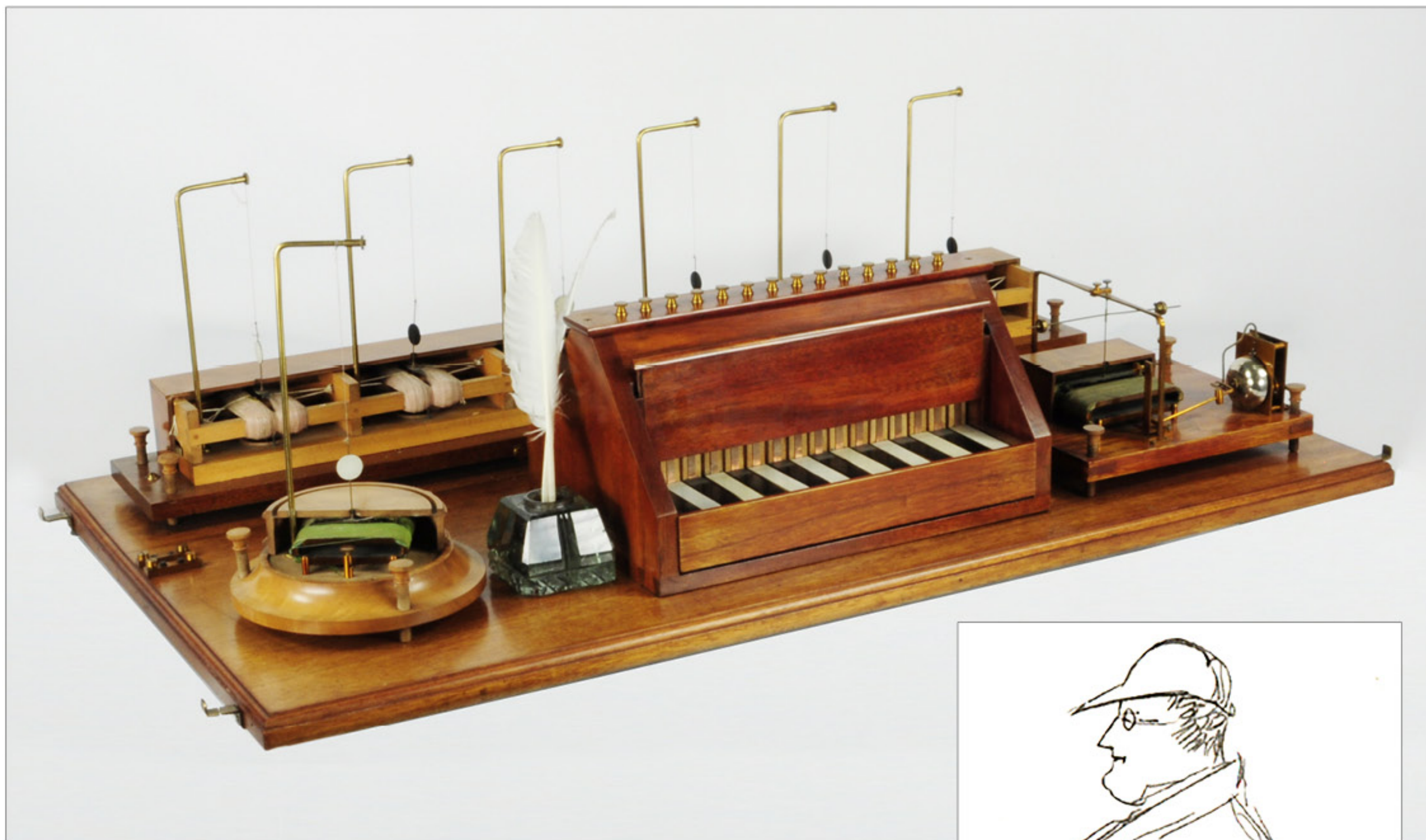
На общественный интерес немедленно откликнулась журналистика. Все рус-

ские журналы 20–30-х годов уделяли значительное место научно-популярным статьям и учёным сообщениям. В 1825 году начали печатать «Московский телеграф» — первый журнал энциклопедического содержания, каждые две недели выходил новый номер объёмом 120 страниц формата А4. Журнал быстро приобрёл около 5000 подписчиков.

Задумывая свой «Современник», Пушкин, конечно, учитывал опыт других изданий. Но его вдохновенный талант проявился своеобразием и при выборе содержания журнала. В эту пору все средства путей сообщения у нас быстро развивались, что ощутимо меняло уклад жизни в столицах и провинции и оживлённо обсуждалось в русской печати. Именно темы транспорта и жизненных перемен стали освещаться в журнале.

Обладая хорошими знакомыми среди инженерных офицеров, Пушкин стал привлекать их к сотрудничеству. Он помещал в «Современнике» оригинальные научные статьи вместо переводных, которыми наполнялись тогда русские журналы. Уже в первом томе журнала появилась статья П. Б. Козловского «Разбор парижского математического ежегодника на 1836 г.», в третьем томе — его же статья о теории вероятностей, ещё раньше интересовавшей поэта.

Так, в библиотеке Пушкина сохранились два сочинения по теории вероятностей, среди них знаменитый труд Лапласа «Опыт философии теории вероятностей». «Опыт» представлял собой вполне доступное для читателей, малознакомых с математикой, изложение вероятностных применений [1]. А накануне своей гибели Пушкин заказал Козловскому новую статью — о паровых машинах. П. Б. Козловский вспоминал вскоре после смерти поэта: «Когда незабвенный издатель «Современника» убеждал меня быть его сотрудником в этом журнале, я представлял ему, без всякой лицемерной скромности, без всяких увёрток самолюбия, сколько сухие статьи мои должны были казаться неуместными в периодических листах, одной лёгкой литературе посвящённых. Не так думал Пушкин...» [1].



Телеграфный аппарат Шиллинга

«КАЛИОСТРО ИЛИ ЧТО-ТО ПРИБЛИЖАЮЩЕЕСЯ»

Интерес Пушкина к развитию отечественной науки и техники в немалой степени был связан с его кругом общения. Особенно впечатлял в нём Павел Львович Шиллинг, выдающийся деятель на многих поприщах, прославившийся изобретением электромагнитного телеграфа. Он заслужил признание и как востоковед, был избран в Петербургскую академию наук.

Знакомство Пушкина с Шиллингом состоялось ещё в 1818 г. В конце 20-х знакомство их возобновилось и стало даже более близким. Когда в конце 1829 г. П.Л. Шиллинг готовился к экспедиции в Монголию и Китай в сопровождении китаевода И. Бичурина, Пушкин хотел поехать вместе с ними. К концу 1829 г. относятся два его отрывка, в первом из которых он обращается к обоим возможным спутникам:

*Поедем, я готов; куда бы вы, друзья,
Куда б ни вздумали, готов за вами я
Повсюду следовать, надменной убегая:
К подножию ль стены далёкого Китая...*

Упоминание «надменной» связано здесь с первым неудачным сватовством к Наталье Николаевне Гончаровой. Поездка Пушкина к китайским пределам, как известно, не состоялась. К счастью, так как повторное сватовство к Наталье Николаевне завершилось браком и знаменитой Болдинской осенью 1830 года.

Второй отрывок, гораздо более известный, давно заслужил восхищение всех тех, кто знаком с процессом творчества и ценит знания:

*О сколько нам открытий чудных
Готовят просвещенья дух
И Опыт, сын ошибок трудных,
И Гений, парадоксов друг,
И Случай, Бог изобретатель...*

Вполне вероятно, что именно личность Шиллинга вызвала такой отклик Пушкина. Примечательно свидетельство о Шиллинге чиновника МИД Ф.П. Фонтона в частном письме 1829 года. Шиллинг — это «Калиостро или что-то приближающееся». Он «сочинил для министерства такой тайный алфавит, то есть так называемый шифр, что даже австрийский, так искусный тайный кабинет, и через полвека не успеет про-



Портрет П.Л. Шиллинга. Рисунок А.С. Пушкина в альбоме Е.Н. Ушаковой, конец 1829 г.

честь!». «Кроме того, он изобрёл новый образ телеграфа. Посредством электрического тока, проводимого по проволокам, растянутым между двумя пунктами, он производит знаки, коих комбинации составляют алфавит, слова, предложения и так далее» [1].

Прямо скажем, по нынешним понятиям написано излишне откровенно. А вот выписка из газетного сообщения в первую годовщину кончины П.Л. Шиллинга в 1838 году: «Он изобрёл разные, весьма остроумные и ува-

*Лист бумаги был сложен вдвое,
и на его внутренних сторонах
характерным пушкинским почерком
были написаны какие-то стихи.
Но строчки словно были перепутаны*

жаемые по своей простоте и удобству, системы сигналов, а особенно криптографических и ключевых (цифирных) письмён. В пример, мы упомянем только об удивительном способе, придуманном им для изображения тремя лишь флагами (символами — авт.) до 3 тыс. различных знаков, способе, изумившем своею простотою и непроницаемостью многочисленных знатоков, собравшихся на опытах, произведённых им в Вене в 1836 году. Впрочем, в этом деле покойный барон был едва ли не первым человеком во всей Европе». Так, счёл возможным написать в газете «Северная пчела» крупный государственный деятель К. В. Чевкин. Именно под его руководством по просторам России были протянуты сети телеграфных линий связи, о чём мечтал Шиллинг.

Фонто́н и Чевкин высветили главное поприще трудов Шиллинга: в 1817–1835 годах он заведовал цифирной частью, руководил шифровальной деятельностью МИДа, достигнув должности старшего советника министерства и генеральского чина — действительно статского советника. Именно Шиллинг впервые ввёл в практику шифрования особые биграммные шифры, в которых по сложному алгоритму цифрами шифровались пары букв. Данные шифры являлись настолько сложными для вскрытия противником при перехвате сообщений, что ими успешно пользовались вплоть до внедрения машинных систем шифрования, т.е. до Второй мировой войны. Хотя сам принцип биграммного шифрования был известен давно, до Шиллинга на практике он не использовался из-за его чрезмерной трудоёмкости при ручной работе. Именно Шиллингу удалось изобрести специальное механическое устройство, предназначенное для такого шифрования — наклеенную на бумагу разборную таблицу. Очень скоро его новыми шифрами стали активно пользоваться

сначала российские дипломаты, а затем и военные. Труды Шиллинга принесли ему славу самого выдающегося русского криптографа XIX века [2].

«КРИПТОГРАФИЧЕСКИЙ СЛЕД» ПОЭТА

Пушкин, несомненно, был осведомлен о роли Шиллинга в МИДе. Интересовался ли сам Александр Сергеевич криптографией? Вполне вероятно, но только следов такого интереса он практически не оставил. Единственный «криптографический след» поэта обнаружили ещё в 1900 году. Тогда, в обширном архиве, переданном в Академию наук, среди пушкинских документов нашли загадочную страницу. Лист бумаги был сложен вдвое, и на его внутренних сторонах характерным пушкинским почерком были написаны какие-то стихи. Но строчки словно были перепутаны. Эти пушкинские стихи никто не мог прочесть, пока в 1909 году страница не попала в руки известного пушкиниста П. О. Морозова.

Ему удалось найти ключ к «перепутыванию» строк: чтение надо было начинать с правой страницы сверху вниз — на ней были первая и через шестнадцать строк вторая строка четверостишия. Продолжать следовало на левой странице, тоже читая сверху вниз, — здесь были строчки четверостишия третья и через тот же интервал (16 строк) четвертая. Читая через шестнадцать строк, П. О. Морозов выписывал одно четверостишие за другим. Но не все они оказались полными, часть их строк помещалась, очевидно, на утраченных страницах. Стихи, которые сумел в конце концов прочитать исследователь, известны сегодня как остатки десятой главы «Евгения Онегина», сожжённой Пушкиным 19 октября 1830 года [3]. Видимо, в момент переписывания и шифрования, он собирался сберечь эти стихи, они ему были до-

роги. Тем не менее, позже Пушкин их сжёг. Похоже, что единственный сохранившийся лист просто затерялся среди бумаг поэта. Замечательно, что мы практически от самого Пушкина можем узнать причину такого неожиданного его поступка.

«НЕТ УБЕДИТЕЛЬНОСТИ В ПОНОШЕНИЯХ...»

В. Ходасевич в своей работе «Пушкин и Николай I» поместил воспоминания графа Ю. Струтынского, записанные со слов Пушкина (не позднее 1830 года):

«Молодость — это горячка, безумие, напасть. Её побуждения обычно бывают благородны, в нравственном смысле даже возвышенны, но чаще всего ведут к великой глупости, а то и к большой вине. Вы, вероятно, знаете, что я считался либералом, революционером, конспиратором, — словом, одним из самых упорных врагов монархизма и в особенности самодержавия. Таков я и был в действительности... Мне казалось, что подчинение закону есть унижение, всякая власть — насилие, каждый монарх — угнетатель, тиран своей страны, и что не только можно, но и похвально покушаться на него словом и делом... Я не помнил себя от радости, когда мне запретили въезд в обе столицы и окружили меня строгим полицейским надзором. Я воображал, что вырос до размеров великого человека... Но всему своя пора и свой срок. Время изменило лихорадочный бред молодости. Всё ребяческое отлетело прочь. Всё порочное исчезло... Послушный спасительному призыву ум вдруг опомнился, успокоился, усмирился; и когда я осмотрелся кругом, когда внимательней, глубже вникнул в видимое, — я понял, что казавшееся донныне правдой было ложью, чтимое — заблуждением, а цели, которые я себе ставил, грозили преступлением, падением, позором! Я понял, что абсолютная свобода, не ограниченная никаким Божеским законом, никакими общественными устоями, та свобода, о которой мечтают и красноречивуют молокососы или сумасшедшие, невозможна, а если бы была возможна, то была бы гибельна, как для личности, так и для общества; что без законной власти, блюдущей общую жизнь народа, не было бы ни родины, ни государ-

ства, ни его политической мощи, ни исторической славы, ни развития; что в такой стране, как Россия, где разнородность государственных элементов, огромность пространства и темноты народной (да и дворянской!) массы требуют мощного направляющего воздействия, — в такой стране власть должна быть объединяющей, гармонизирующей, воспитывающей и долго ещё должна оставаться диктаториальной или самодержавной, потому что иначе она не будет чтимой» [4].

«РОССИЯ СЛИШКОМ МАЛО ИЗВЕСТНА РУССКИМ»

Тема «Пушкин и информационная безопасность», вероятно, неотделима от представления о нашем великом поэте, как о выдающемся исследователе и общественном деятеле.

Известно, что А. С. Пушкин владел в той или иной степени 16-ю языками. А в декабре 1832 года состоялось избрание его в действительные члены Императорской российской академии. Позже, в 1841 году, эта академия вошла в Петербургскую академию наук как отделение русского языка и словесности. Пушкин впервые принял участие в академическом собрании 28 января 1833 года. Тогда и был вручён ему диплом академика.

Пушкин-исследователь, историк отчётливо виден в его «Истории Пугачёвского бунта», работа над которой происходила в 1832–1833 годах и завершилась в очередную Болдинскую осень. Интенсивная работа с архивными документами, беседы на местах прошедших событий с живыми их свидетелями (прошло всего полвека!) и собственный анализ всех собранных материалов показали силу его таланта в новом ракурсе. А ведь одновременно Пушкин

трудился над «Дубровским» и «Капитанской дочкой», «Пиковой дамой», «Медным всадником», «Сказками»...

Интересно, что С. М. Соловьёв считал подлинным создателем русской историографии не Карамзина, а Пушкина с его «Историей Пугачёвского бунта». К сожалению, Александр Сергеевич не успел достаточно полно раскрыть уже высказанное своё прозрение: «Россия никогда ничего не имела общего с остальной Европой..., история её требует другой мысли, другой формулы...».

«ВОТ ВЫ, НАКОНЕЦ, И НАЦИОНАЛЬНЫЙ ПОЭТ!»

Вместе с тем, это понимание сложилось не вдруг и, несомненно, присутствует уже в его знаменитом стихотворении «Клеветникам России», написанном в августе 1831 года. Стихи возникли, прежде всего, как ответ на инициированную депутатами французского парламента пиар-кампанию по поддержке Польского восстания 1830–1831 годов. Это восстание, начавшееся на территории царства Польского в Российской империи, до самого своего конца сопровождалось неизменным требованием отхода России не только с польских земель, но и из Литвы, Белоруссии, Украины. Западная агитация за военное вмешательство в болезненные внутрироссийские события была так сильна, что война с Европой тогда казалась весьма вероятной. И в июле 1831 года Пушкин обратился к А. Х. Бенкендорфу с предложением: «...Озлобленная Европа нападает покамest на Россию не оружием, но ежедневной, бешеной клеветой. Конституционные правительства хотят мира, а молодые поколения, волнуемые журналами, требуют войны... Пускай позволят нам, русским писателям, отражать бесстыдные и невежественные на-

падения иностранных газет...». Это ли не осознание насущной необходимости информационной защиты с предложением конкретных действий! Тогда и родились известные строки, адресованные клеветникам России:

*...И ненавидите вы нас...
За что ж? ответствуйте: за то ли,
Что на развалинах пылающей Москвы
Мы не признали наглой воли
Того, под кем дрожали вы?
За то ль, что в бездну повалили
Мы тяготеющий над царствами кумир
И нашей кровью испутили
Европы вольность, честь и мир?..*

Откликаясь на известие о взятии Варшавы, Пушкин написал стихотворение «Бородинская годовщина». Эти два стихотворения, а также стихотворение Жуковского «Старая песня на новый лад» после личного одобрения Николаем I были немедленно опубликованы в брошюре под названием «На взятие Варшавы». Брошюру вскоре перевели на иностранные языки. Публикация была замечена возбуждённой Европой, а также всколыхнула русское читающее общество, через которое прошла трещина, пока лишь разделившая поклонников и критиков новых стихов Пушкина. Знаменателен отзыв П. Я. Чаадаева (18 сентября 1831 года): «Вот вы, наконец, и национальный поэт; вы, наконец, угадали своё призвание... Стихотворение к врагам России особенно замечательно... Не все здесь одного со мною мнения, вы, конечно, не сомневаетесь в этом, но пусть говорят, что хотят — а мы пойдем вперед».

* * *

И как много было тогда ещё впереди! Но далеко не всё начатое удалось завершить в такой короткой пушкинской жизни. Вскоре после гибели Пушкина его друг А. И. Тургенев вспоминал: «Я находил в нём сокровища таланта, наблюдений и начитанности о России, особенно о Петре и Екатерине, редкие, единственные. Никто так хорошо не судил русскую новейшую историю: он созрел для неё и знал и отыскал в известность многое, чего другие не заметили... Ему оставалось дополнить и передать бумаге свои сведения. Великая потеря!» [1].

ЛИТЕРАТУРА

1. Алексеев М. П. Пушкин: Сравнительно-исторические исследования Л., 1984
2. Соболева Т. А. История шифровального дела в России М., 2002
3. Морозов П. О. Шифрованное стихотворение Пушкина // Пушкин и его современники: Материалы и исследования Спб., 1910
4. Ходасевич В. Ф. Книжки и люди М., 2002



Михаил САВЕЛЬЕВ
директор по развитию бизнеса
компании «Информзащита»

ОГЛЯНУТЬСЯ ВПЕРЕД

ЗИМА БЛИЗКО! ПРИБЛИЖАЕТСЯ ЭПОХА НУЛЕВОГО ДОВЕРИЯ

В IS Journal обратился к директору по развитию бизнеса компании «Информзащита» Михаилу Савельеву с просьбой обозначить наиболее яркие, на его взгляд, тенденции в сфере ИБ в 2018 году и сделать прогноз на 2019-й.

2018-й

Чтобы увидеть, что ждет впереди, порой стоит оглянуться назад. А в этом плане 2018 год принес нам немало:

- ♦ **Об инцидентах.** С одной стороны, в 2018 году не было таких громких, значимых атак, как в 2017. А с другой — в тени эпидемий шифровальщиков как-то затерялись и апрельская массовая атака на оборудование Cisco, и появление аппаратных уязвимостей, к которым, к слову, отрасль оказалась не очень готова. В результате чего, соответственно, усилия по их устранению обошлись намного дороже, чем предполагалось.

- ♦ **О нормативке.** ИБ-отрасль в нашей стране сильно зависима от нормативной базы. А она в 2018 году развивалась стремительно: вступление в силу 187 федерального закона и целого ряда подзаконных актов, выход 167-ФЗ, обновления Положения 382-П и пр., — все это вызвало бурную волну обсуждения как самих документов, так и тянущихся за ними последствий. Надо отметить, что регуляторам удалось взбудорить довольно широкие мас-

сы тех, кто либо не задумывался, либо откладывал вопросы безопасности в дальний ящик. Первые полгода прошли в панических обсуждениях, а вторая половина — в процессах составления перечней КИИ и старте процессов категорирования объектов. Я надеюсь, что год, отводящийся на категорирование (а это фаза, на которой находится подавляющая часть активных субъектов КИИ), не станет периодом забвения. Главное, что в головах выстроилось понимание, для чего, зачем и что нужно делать. К слову, я считаю, что регуляторам в рамках 187 закона удалось сформулировать достаточно гармоничный подход к защите объектов КИИ.

- ♦ **О СОС.** И инциденты, и нормативка (в части ГосСОПКА) стали стимулами к массовому строительству СОСов. И это хорошо тем, что появилось осознание необходимости мониторинга для выявления и оперативного реагирования на инциденты ИБ. Но...

- ♦ **О кадрах.** Но, оказалось, что катастрофически не хватает специалистов для работы на этих сложных комплексах, о которых говорилось выше. Этот фактор полностью обесмысливает многомиллионные затраты на строительство СОС. Кадровый голод на рынке ощущается остро: сегодня специалисты скорее перетекают из компании в компанию, чем воспроизводятся внутри. Их переманивают всем, чем только

можно. Это взвинчивает рынок труда, зарплаты растут, а вот проблемы дефицита кадров пока не решаются.

- ♦ **Об отрасли.** Главная тенденция на «ментальном» уровне: отрасль ИБ «мудреет». Под этим я подразумеваю как рост компетенций у молодого поколения ИБ-шников, так и захватывающее умы осознание того, что безопасность должна быть неотъемлемым свойством ИТ-решений. Надо сказать, что и извечная пропасть между айтишниками и безопасниками сокращается на глазах — мы чаще начинаем доверять друг другу и сближаться для совместного решения встающих перед нами проблем.

- ♦ **О рынке.** Меняется расстановка сил. Нельзя не заметить как тенденцию крупных заказчиков к созданию и использованию инсорсинговых компаний, так и выход на рынок таких игроков, как «Ростелеком».

2019-й

Что определит развитие отрасли ИБ в 2019 году? Если отбросить заведомо футуристические вещи и взглянуть на ИБ прагматически, то отметить хочется несколько главных, на мой взгляд, тенденций:

1. Кадровый голод потребует решения вопроса автоматизации рутинных операций. Тут речь идет и о мониторинге инфраструктурных событий, и о поиске фрода в различных его прояв-

лениях. Обрабатывать руками невозможно не только огромное количество событий, собираемых с инфраструктуры (для этого и появились SIEM и подобные платформы), но и проводить первичную обработку этих событий, не говоря уже об оперативном реагировании на понятные инциденты. Как это будет решено — пока не знаю. Но решения такого рода станут востребованы в ближайшем будущем.

2. Кадровый голод приведет и к росту сервисных услуг в области ИБ.

3. Повсеместное строительство SOC начнет перерастать в тенденцию «оцифровки бизнеса», т.е. сбора всех возможных данных о работе систем и процессов. Надо ждать, что вместо хайпа за счет «искусственного интеллекта и машинного обучения» мы начнем учиться выявлять девиации в производственных бизнес-процессах.

4. Повсеместное строительство SOC повысит популярность и востребованность услуги проведения киберучений, ведь их результаты смогут дать оценку как качеству правил, по которым осуществляется мониторинг (они обязаны видеть действия атакующих), так и слаженности и отработанности действий персонала SOC в процессе реагирования на инциденты.

5. Количество средств защиты должно начать переходить в качество. Мы видим, как большая часть заказчиков начинает решать проблемы не за счет приобретения новых решений по ИБ, а за счет базовых, гигиенических мер (управление уязвимостями, конфигурациями) и максимального использования уже имеющегося инструментария и настроек системного ПО. Сегодня грамотное использование только вышеназванных гигиенических мер может свести риск успешной реализации атак до минимального уровня.

6. Осознание важности работы с персоналом (а он-то и был, и остается самым уязвимым звеном) приведет к очередному витку попыток контроля за ним. Должен родиться не только и не столько поведенческий, сколько некий комплексный анализ действий пользователей.

7. Фокус безопасности станет шире: внимание компаний будет обращено не только на себя. В фокус безопас-

Атаки чаще стали идти не напрямую на организацию, а через третьи руки: партнеров по бизнесу, поставщиков различного рода услуг, разработчиков заказного ПО и т.п.

ков неизбежно станут попадать контрагенты и прочее окружение компаний. Вектор целевых атак меняется. Наш IZ: SOC видит, что атаки чаще стали идти не напрямую на организацию, а через третьи руки: партнеров по бизнесу, поставщиков различного рода услуг, разработчиков заказного ПО и т.п. Это является ярким маркером эпохи так называемого «нулевого доверия» — времени, когда под сомнение необходимо ставить абсолютно любую внешнюю коммуникацию.

8. Немалую роль будет играть принятый курс на импортозамещение. К счастью, в настоящее время реестр отечественного ПО активно чистится от псевдороссийских решений. И если государство будет дальше поддерживать этот курс, то интеграционных задач по переходу на отечественные решения хватит на всех.

В «ИНФОРМЗАЩИТЕ»

Компания «Информзащита» стремится развиваться опережающим темпом:

1. Основным потенциал компании — это люди. Наше развитие немыслимо без постоянного приобретения новых компетенций. Залогом успешного решения любой проблемы заказчика является возможность быстро собрать проектную команду, обладающую всеми необходимыми знаниями. Именно поэтому мы активно вкладываемся в развитие наших специалистов.

2. Вопрос кадрового голода мы успешно решаем за счет сотрудничества с ведущими техническими вузами Москвы и активного развития стажёрской программы. Так, по итогам зимней и летней стажировок 2018 года штат компании пополнили около 20 молодых специалистов. Стажировка в компании включает в себя как обучение, проводимое ведущими экспертами «Информзащиты», так и привлече-

ние стажеров к практической работе сначала в роли наблюдателей, а затем — младших специалистов. Практика такого своеобразного «Инкубатора» настолько понравилась всем, что в январе 2019-го к нам пришло более 50 заявок на новый поток стажировки, и мы с удовольствием примем в штат всех, кто себя хорошо зарекомендует в этот период.

3. В компании регулярно проводятся стратегические сессии топ-менеджеров, на которых анализируется динамика и потребности рынка. Сегодня мы, сохраняя фокус на ИБ, работаем над развитием отраслевых компетенций, которые позволят нам глубже понимать бизнес-процессы заказчиков и обоснованно предлагать встраивать в них механизмы защиты. Структурно это выражается в создании отдельных центров компетенции, более глубоко проникающих в предметную область заказчика.

4. Наличие собственного подразделения разработки позволяет нам с легкостью решать различные интеграционные задачи, сопрягать несвязанные системы, создавать и тиражировать новые решения. Некоторые из них мы готовимся выпустить в качестве продуктов.

5. Защищать без понимания того, как осуществляется атака — невозможно. Именно поэтому мы сформировали одну из самых многочисленных и квалифицированных команд «белых» хакеров. Опыт этих ребят позволяет нам на качественно ином уровне строить системы безопасности и анализировать защищенность бизнес-процессов.

6. Мы полностью готовы к сервисной модели обеспечения информационной безопасности. И главным залогом своего успеха на этом поприще мы видим отлаженность собственных процессов и широту компетенций наших специалистов.



ВРАГИ И СОЮЗНИКИ... ПРОЦЕССОВ ИБ

ПОМНИТЕ О ТУЗЕМЦАХ, ИСПОВЕДУЮЩИХ КУЛЬТ КАРГО!

За годы работы на рынке безопасности автору довелось увидеть десятки предприятий и сотни различных процессных регламентов. Нефтеперерабатывающие заводы, страховые компании, ритейл, банки и много других... Единственное, что их объединяло — процессы кибербезопасности, как правило, нигде не работали. В лучшем случае — процентов на 10, то есть 1–2 регламента из десятков. Среди топовых по бесполезности регламентов — контроль и согласование изменений в ИТ-инфраструктуре, аудиты ИБ, управление рисками ИБ.

Более того, чем больше регламентов существовало на предприятии, тем меньше из них работало. Под «работой» я подразумеваю не наличие записей и свидетельств о выполнении, а практическое достижение цели процесса, например, уменьшение количества фактов накопления доступов или уменьшения периода ожидания согласования доступов пользователями.

Как у всякой сущности, у процессов безопасности всегда находились свои враги и союзники. Рассмотрим ключевых.

ВРАГИ РЕЗУЛЬТАТИВНЫХ ПРОЦЕССОВ

Количество — враг качества в случае процессов безопасности. Чем больше параметров мы контролируем, чем больше подписей собираем, чем больше подозрительных событий расследуем, тем формальнее мы к ним относимся. Классическая байка «Волки-волки» применима в данном случае как никогда.

Системы управления качеством — извращают идею безопасности. «Бумажный забор» не только не защищает, он даёт ложное ощущение защищённости, уподобляя компании туземцам, исповедующим культ карго.

Внутренние аудиторы — чума корпоративных служб ИБ. Единицы из них имеют представление о безопасности больше, чем general computer controls, и их советы не только отдают нафталином, но и отвлекают ограниченные временные, человеческие и бюджетные ресурсы от актуальных угроз.

Регуляторы — вечный тормоз кибербезопасности. Появляются, когда угрозы поднимаются в полный рост, но после того, как передовые службы ИБ уже





завершили десятки проектов по теме... Съедают весь бюджет, требуя применения решений, от которых «цифровые» процессы просто встают.

СОЮЗНИКИ РЕЗУЛЬТАТИВНЫХ ПРОЦЕССОВ

Спонсор процесса — альфа и омега процесса безопасности. Если процесс никому не нужен, то не нужно его проектировать, внедрять и интегрировать с другими процессами. Сильным спонсором процесса может быть только зарабатывающее или управляющее подразделение. С различных «костов» (ИТ, АХО и др.) выходят плохие спонсоры, они избавляются от ИБ при малейшем кризисе или проблеме.

Проектный подход. Обязателен для успешного создания и закрепления в корпоративной жизни процесса ИБ. Среди важных для внедрения процессов ИБ доменов проектного управления (по модели PMB ook) — управление ожиданиями заинтересованных лиц (stakeholder management), управление объёмом проекта (scope management), управление интеграцией проектных активностей (integration management) и управление коммуникациями.

Владелец процесса. Даёт процессу возможность жить и развиваться. Бесхозный («сиротский») процесс проживёт недолго — падёт жертвой первого же сокращения костов, оптимизации корпоративных процессов или политических игр.

Процессная модель. Позволяет повысить КПД каждого процесса и полу-

чить от них синергию. Каждый процесс имеет свой потенциал полезности для других процессов. Например, процесс повышения осведомлённости пользователей (включая процедуру инструктажа) позволяет корректировать поведение пользователей, выполняя и комплаенс-требования и рекомендации службы мониторинга ИБ, а служба мониторинга ИБ, в свою очередь, даёт обратную связь практически всем другим процессам ИБ — насколько они результативны в выполнении своих целей.

Аутсорсинг процесса. Рационален практически всегда для сложных процессов в небольших инфраструктурах. Качество процесса зависит в первую очередь от квалификации участников процесса, и если нет возможности привлечь с рынка достаточное число лучших профессионалов, то желательно привлечь одного из лучших игроков в своём сегменте.

ОБЯЗАТЕЛЬНЫЕ ПРОЦЕССЫ БЕЗОПАСНОСТИ

Внедрение процесса ИБ должно дать компании максимум пользы и внедрить процесс максимально «бесшовно». Однако есть и процессы, без которых служба ИБ не сможет эффективно и стабильно выполнять свою задачу — защищать интересы организации в информационной сфере.

Управление политикой ИБ. Обязательно для определения «что можно, а что нельзя» делать с информационными активами организации. В практике автора бывало, что структуры с миллиардами долларов активов страдали от

примитивных инцидентов типа «сотрудник унёс жёсткий диск домой», и этому сотруднику ничего не могли вменить — служба HR думала, что инструктаж делает служба ИБ, а ИБ, — что HR.

Управление доступом. Обязательно, как с точки зрения любых стандартов ИБ (в том числе определённых законодательством как обязательные), так и с точки зрения здравого смысла: зачем сотрудникам знать больше, чем им требуется для выполнения должностных обязанностей? Правильно организованное управление доступом стимулирует бизнес брать на себя ответственность за свои информационные активы. Банально, не хочешь быть владельцем актива, значит, не имеешь права определять, кто получит к нему доступ.

Мониторинг и управление инцидентами ИБ. Просто даёт реальную картину: что происходит в информационной инфраструктуре и системах организации. Даёт факты: кто, что, где и как делал — пользователи, ИТ, автоматизированные сервисы, внешние нарушители и подрядчики... Без этого организация лишь догадывается о реальном состоянии защищённости своего информационного пространства.

Процессы безопасности позволяют организации уверенно смотреть в будущее: без опаски, что деньги украдут, сервера уронят, а отчётность фальсифицируют. Но внедрять их нужно фокусно и системно. И тут главное — желание.

ТРИДЦАТЬ ПЯТЬ ДЕВУШЕК И ОДИН МУЖЧИНА

BIS JOURNAL ПРОВЕЛ ПЕРВЫЙ BIS-ОГОНЁК ДЛЯ ПИАРЩИКОВ И МАРКЕТОЛОГОВ В СФЕРЕ ИБ

Первый BIS-Огонёк для пиарщиков и маркетологов ИБ-компаний состоялся в кафе «Сценариум» на Тверской. Официальный повод — презентация специального номера BIS Journal, посвященного Уральскому форуму — главному мероприятию года в сфере информационной безопасности.

Выступление директора по развитию BIS Journal Андрея Минакова настроило гостей на деловой лад. По замыслу организаторов, BIS-Огонёк — это не только приятные встречи и непринужденное общение коллег, но и насыщенная образовательная программа, позволяющая постоянно находиться на передовой профессиональных трендов. Первым в череде таких discussion and training activities стал мастер-класс специального гостя BIS Journal — основателя Московской школы PR, московской школы блогеров, лектора и ментора стартапов Академии Сколково —

Татьяны Яковлевой. Ее рассказ о последних тенденциях в маркетинге и новейшем инструментарии PR-сферы поразил неожиданностью и вызвал оживленную дискуссию.

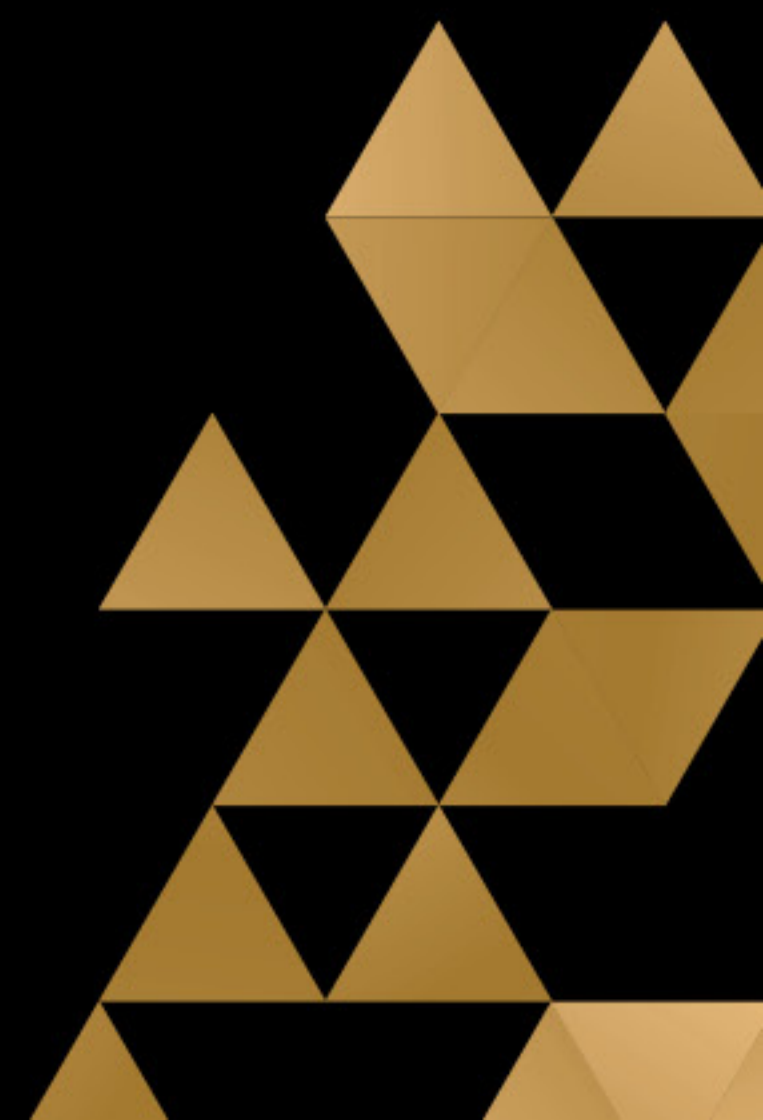
Следующий — Весенний BIS-Огонёк состоится 5 марта. До встречи!





Первое интеллектуальное шоу по информационной безопасности

*Смотри новые выпуски
и становись участником игры:
igra.ib-bank.ru*



АВАНГАРД

медиа группа



Организация
мероприятий



Отраслевой
журнал



Интернет-
телекомпания



Книжное
издательство

ib-bank.ru