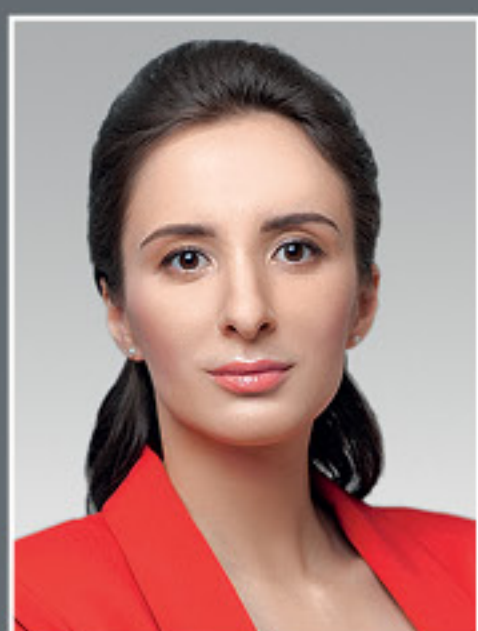




**30** > Вадим УВАРОВ  
Банк России  
**Векторы развития**

**34** > Алексей ВОЙЛУКОВ  
Ассоциация банков России  
**Аутсорсинг  
для небольших  
и средних банков**



**82** > Дарья ВЕРЕСТНИКОВА  
SafeTech  
**Подпись в смартфоне —  
для безопасности  
и для бизнеса**

**123** > Сергей ПАЗИЗИН  
Банк ВТБ  
**Действовать по  
всем направлениям**

**131** > Илья ГОРЮНОВ  
ООО «АФИ Дистрибьюшн»  
**Кого взломают  
в 2020 году?**

## СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ. НОВЫЕ МАНИПУЛЯЦИИ





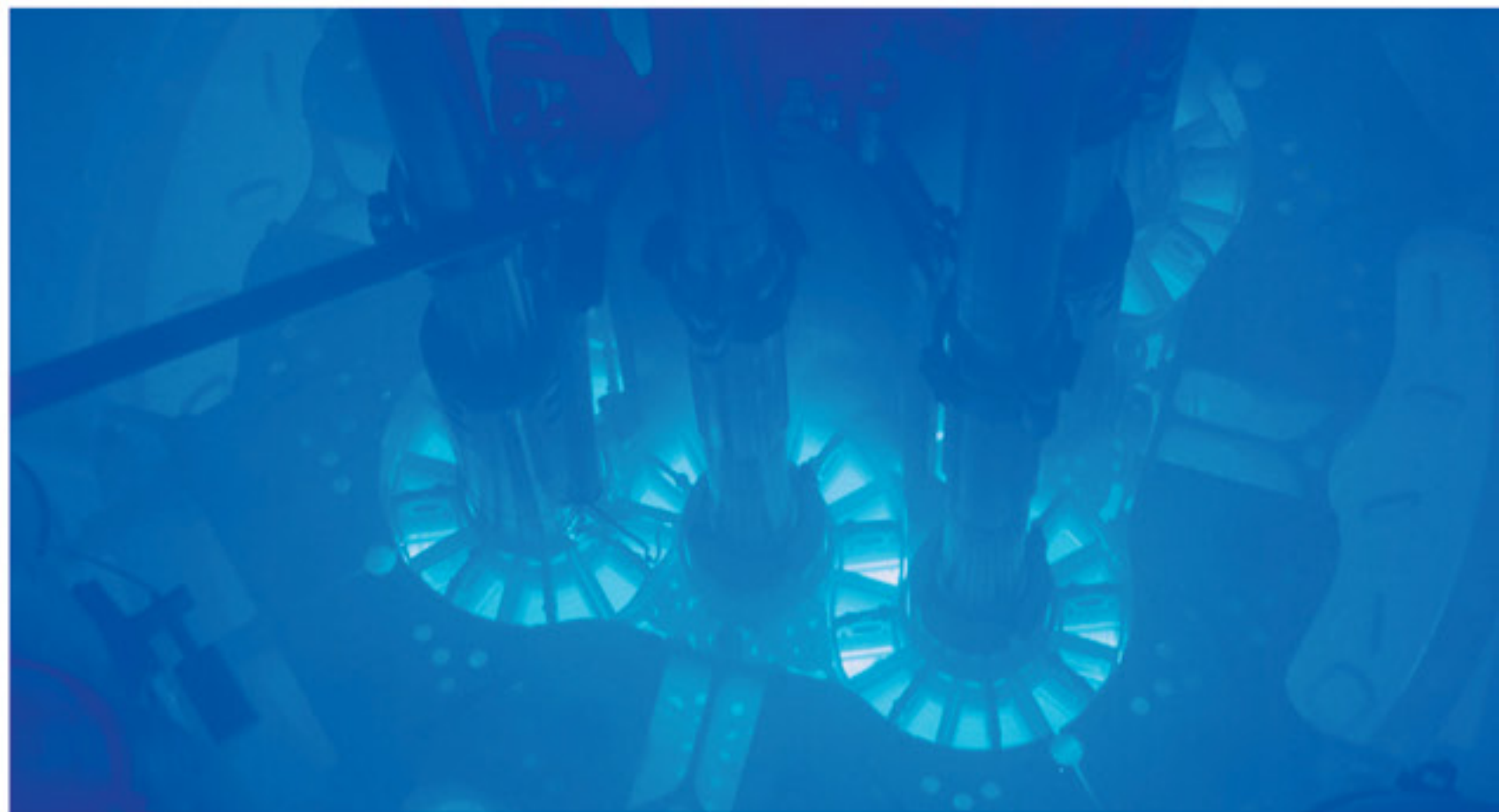
**Практическая конференция  
профессионального сообщества специалистов  
по промышленной кибербезопасности**

# **RUSCADASEC**

## **Con 2020**



**Москва  
23.04**



Конференция соберет профессионалов из промышленных отраслей и экспертов по кибербезопасности и промышленной автоматизации для обмена опытом и экспертизой в уникальной среде единомышленников.

**con.ruscadasec.ru**







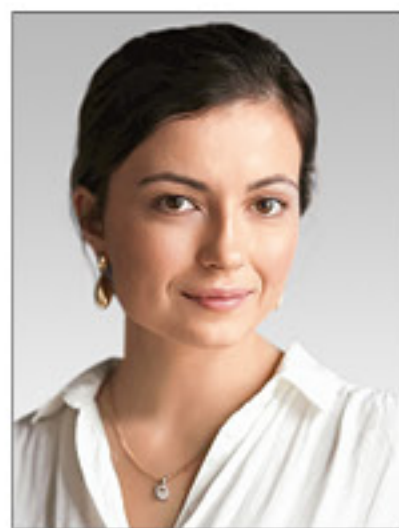
**Артём  
ЗУБКОВ**  
издатель



**Игорь  
НЕКРАСОВ**  
главный редактор



**Павел  
БЫЛЕВСКИЙ**  
шеф-редактор



**Анна  
ВОРОБЬЁВА**  
руководитель  
интернет-проектов



**Андрей  
МИНАКОВ**  
директор  
по развитию



**Никита  
МЕЛЬНИКОВ**  
арт-директор

## МЫ — ОДНА КОМАНДА!

Человеческий фактор всё больше выходит на первый план: всё более острой становится проблема социальной инженерии. Чудеса техники окружают нас теперь повсюду, а вот люди, кажется, остались прежними, если даже не стали ещё хуже.

Проблема стара как мир: при любом техническом прогрессе за ширмой любых «технологий» главным остаётся человек. Рано или поздно истина обнажается: человек — и исходный, и конечный пункт; и источник, и цель. Как в плохом, так и в хорошем смысле, со всеми своими достоинствами и недостатками.

Проблема социальной инженерии многопланова, она кустится и ветвится всё больше и больше. Множатся личины злоумышленников: это матёрые киберпаханы, «злые гении» хакинга. Им верно служат инсайдеры — «засланные казачки», а также подлые душонки, готовые за тридцать сребренников на худший из смертных грехов — предать своих благодетелей.

Всё больше разнообразятся и портреты жертв: доверчивые пенсионеры, самоуверенные «миллениалы», матёрые предприниматели и сотрудники спецслужб, которых «проводят на мякине». На всякого мудреца оказывается довольно своей простоты, к каждому злоумышленнику подбирают свою «отмычку». Даже президенты других стран умудряются выставлять себя на всеобщее посмешище, откровенничая по мобильному телефону со злыми шутниками-пранкерами.

К счастью, к информационной безопасности применим принцип гомеопатии: кто придёт к нам с мечом, тот от меча и погибнет. На самых хитрых «социальных инженеров» найдутся укротители, которые не дадут свершиться злодейству. К этой славной когорте принадлежим и мы с вами, уважаемые коллеги по отрасли. Мы — одна команда, цели наши справедливы. И вообще хороших людей больше, чем плохих, нужно только сплотиться и повышать эффективность взаимодействия. Битва нелёгкая, но нас не испугать. Победа, как говорится, будет за нами.

### 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, доктор технических наук

**Шипилов В.В.** — исполнительный директор Ассоциации российских банков, кандидат технических наук

### РЕДАКЦИОННАЯ КОЛЛЕГИЯ

**Былевский П.Г.** — шеф-редактор, кандидат философских наук

**Велигура А.Н.** — председатель комитета по банковской безопасности Ассоциации российских банков, руководитель комитета по безопасности НП «НПС», CISA, кандидат физико-математических наук

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

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

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

**Курило А.П.** — президент компании «Реальная Безопасность», кандидат технических наук

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

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

**Некрасов И.В.** — главный редактор журнала

**Окулевский В.А.** — заместитель начальника службы ИБ

банка «Возрождение», кандидат технических наук

**Пазизин С.В.** — заместитель начальника Управления по обеспечению информационной безопасности ДБ

Банка ВТБ (ПАО), 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.**

Руководитель интернет-проектов: **Воробьёва А.А.**

Руководитель спецпроектов: **Седов О.В.**

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

**Куликов В.А., Бродская М.А., к.т.н.**

Иллюстрация на 1-й обложке: **Виктор Миллер Гауса**

Фото в номере: **фотобанк DepositPhotos, Салаватова Я.М.,**

**wikipedia.org, waralbum.ru, pamyat-naroda.ru**

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

Цветокорректор: **Науменко М.Б.**

Корректор: **Бальтерманц Л.Ф.**

### УЧРЕДИТЕЛЬ-ИЗДАТЕЛЬ

ООО «Медиа Группы „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](http://journal.ib-bank.ru)

E-mail: [bis@ib-bank.ru](mailto:bis@ib-bank.ru)

Отдел рекламы: [reklama@ib-bank.ru](mailto:reklama@ib-bank.ru)

Отдел распространения: [tirazh@ib-bank.ru](mailto: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 25.01.2020. Тираж 7000 экз.

Заказ №242020. Цена договорная.

Отпечатан в типографии

«Московский Печатный Двор», 123298, г. Москва, 3-я Хорошевская 18, корп.1, офис 201А

© BIS Journal, 2020





## НОВОСТИ

- 5 **Законодательство, технологии, криминал**

## ТЕМА НОМЕРА

- 10 **Социальная инженерия и утечки данных**  
**Кто виноват и что делать?**
- 11 Сергей Вихорев (ООО «ИТ-экспертиза»)  
**«Бороться надо с первопричиной»**
- 13 Тимур Аитов (ГК «Программный продукт»)  
**«Развязать руки полиции»**
- 14 Виталий Номоконов (ДВФУ)  
**«Помогут специальные профилактические программы»**
- 15 Михаил Емельяников  
(КА «Емельяников, Попова и партнёры»)  
**«Главная сложность — в комплексности проблемы»**
- 17 Олег Седов (Ростелеком-Солар)  
**«Почему силовики равнодушны к банкирам?»**
- 19 Александр Ивашкин  
(Лига финансовых институтов)  
**«Нужна альтернатива мегарегулятору»**
- 20 Сергей Голованов  
(Лаборатория Касперского)  
**«Виновата человеческая жадность»**
- 22 Василий Окулесский (Банк «Возрождение»)  
**Не ученьем единым**
- 25 Александр Бодрик (Cyberlands B.V.)  
**Семь раз отмерь**

## РЕГУЛЯТОРЫ

- 28 **Законотворчество**  
Анатолий Аксаков (Государственная дума РФ)  
**Стоп-знак для «телефонных мошенников»**
- 30 **Текущие задачи**  
Вадим Уваров (Банк России)  
**Векторы развития**



## БАНКИ

- 34 **Аутсорсинг**  
Алексей Войлуков  
(Ассоциация банков России)  
**Оптимальный аутсорсинг для небольших и средних банков**
- 38 **Модель угроз**  
Сергей Вихорев (ООО «ИТ-экспертиза»)  
**«Перемен! — требуют наши сердца»**
- 44 **Модель угроз**  
Андрей Курило («Реальная безопасность»)  
**Смена парадигмы защиты ИТ-систем**
- 47 **Межотраслевое взаимодействие**  
Дмитрий Махаев (ФГУП «Российская телевизионная и радиовещательная сеть»)  
**Слабое звено**
- 50 **Биометрия**  
Дмитрий Улыбин (ПАО «Ростелеком»)  
**Средство от боли**

## УГРОЗЫ И РЕШЕНИЯ

- 54 **Нормативная база**  
Антон Свиницкий, Ксения Засецкая  
(АО «ДиалогНаука»)  
**Новый вектор**
- 56 **Анализ трафика**  
Алексей Новиков, Наталия Казанькова  
(Positive Technologies)  
**SOC без анализа трафика = центр недостаточного реагирования**



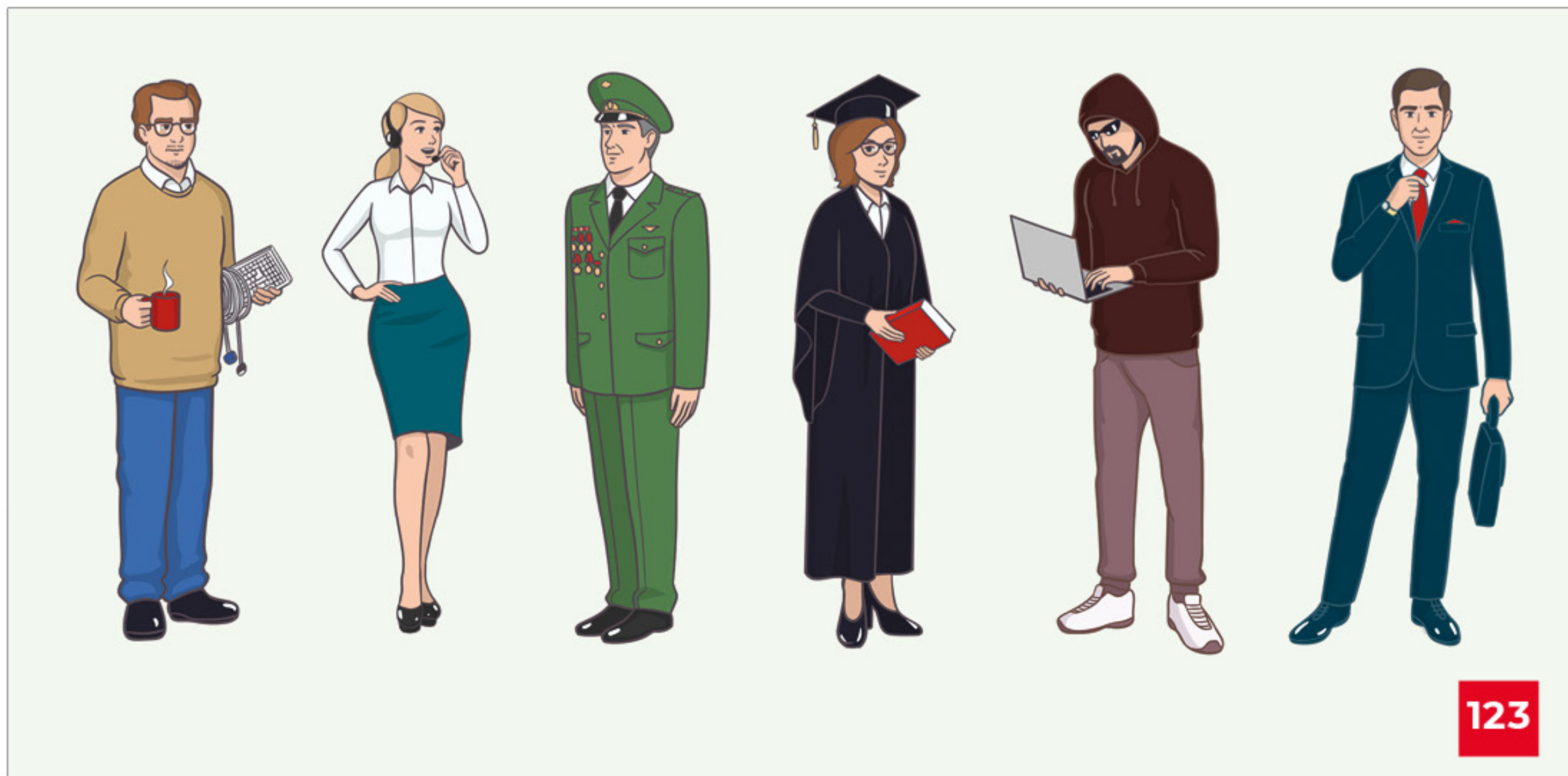
- 58 Анализ трафика**  
Антон Афанасьев (СТИ)  
**Анализ трафика как средство проактивного обеспечения информационной безопасности**
- 60 Новые подходы**  
Павел Коростелев (Код безопасности)  
**Концепция нулевого доверия**
- 62 Аутсорсинг**  
Яна Анджелло (ГК Angara)  
**Как выбрать провайдера MSS?**
- 65 Аутсорсинг**  
Алексей Курских (ARinteg)  
**Очевидные и неочевидные преимущества сервисной модели информационной безопасности**
- 68 Антифрод**  
Николай Фокин (BI.ZONE)  
**Цифровой профиль: информация на страже денег**
- 71 Инсайд**  
Леонид Бондаренко (Сикрет Технолоджис)  
**Фотограф экрана монитора уже не аноним**
- 72 Инсайд**  
Сергей Добрушский (Гарда Технологии)  
**Актуальная архитектура защиты от инсайдера**
- 74 ДБО**  
Виктория Чирва (компания «Актив»)  
**Рутокен — стандарт де-факто**
- 78 Киберучения**  
Дарья Сутормина (АО НИП «ИНФОРМЗАЩИТА»)  
**«Белые хакеры» на страже бизнеса**
- 80 Мобильный банкинг**  
Никита Дуров (Check Point Software Technologies)  
**Знаешь угрозы — защита надёжна**
- 82 Электронная подпись**  
Дарья Верестникова (SafeTech)  
**Подпись в смартфоне — для безопасности и для бизнеса**

## ИНФРАСТРУКТУРА

- 86 События**  
Екатерина Крылова, Юлия Фарабе, Иван Меденников (ООО «ЦРТ-Инновации»)  
**Golden VOICES из России**
- 90 Деловые мероприятия**  
Николай Кольский (BIS Journal)  
**«Киберстабильность: подходы, перспективы, вызовы» 2019**
- 92 Деловые мероприятия**  
Алекаандр Бодрик (BIS Journal)  
**SOC-Форум 2019**
- 97 Право**  
Рузанна Ахобекова, Виктор Наумов (Dentons)  
**Как не утратить права на ПО**
- 102 ИТ-трансформация**  
Дмитрий Романченко (IBS)  
**«Пропуск» в завтра информатизации**
- 104 Импортзамещение**  
Валерий Куликов (BIS Journal)  
**Антисанкции или индустриализация 2.0?**
- 108 Импортзамещение**  
Антон Чухнов (АВ Софт)  
**Проактивная кибербезопасность**







## HI-NUME

- 110 Социальная инженерия**  
Александр Шмелев, Олег Тарасов  
(Московский Индустриальный банк)  
**Самая большая проблема**
- 113 Социальная инженерия**  
Ольга Лимонова, Андрей Жаркевич  
(ООО «Антифишинг»)  
**Многоликий фишинг**
- 118 Презентация**  
Оксана Дяченко (BIS Journal)  
**Инсайдеры в банках — мифы и реальность**

## ОБРАЗОВАНИЕ И КАРЬЕРА

- 120 Обзор**  
Марина Бродская (BIS Journal)  
**Британия в тревоге**
- 123 Дефицит кадров**  
Сергей Пазизин (Банк ВТБ (ПАО))  
**Действовать по всем направлениям**

## СУБЪЕКТЫ

- 126 История**  
Борис Столпаков (историк криптографии)  
**Эфир льда и пламени**
- 131 Прогноз**  
Илья Горюнов (ООО «АФИ Дистрибьюшн»)  
**Кого взломают в 2020 году?**
- 134 Юбилей**  
Дмитрий Ларин (историк криптографии)  
**Перспектива для призвания**





## В РОССИИ ПРИНЯЛИ «АНТИЯБЛОЧНЫЙ» ЗАКОН

Госдума РФ приняла в окончательном чтении закон об обязательной предустановке российских приложений на гаджеты. Он вступит в силу 1 июля 2021 года. Apple уже предупредила, что в случае принятия закона может уйти с рынка РФ.

Законопроект предполагает установку отечественных приложений на всех продаваемых в России гаджетах. Речь не идёт о полном переходе на российский софт — список приложений ещё должно утвердить Правительство России. Минкомсвязи

РФ уже предложило ограничить его поисковиками и браузерами. Депутаты предполагают, что инициатива должна коснуться смартфонов, компьютеров и телевизоров с функцией «смарт-ТВ». За нарушение предусмотрен штраф в 200 000 рублей.

В пользу нового закона говорит рынок: например, после того как суд запретил Google отказывать российскому «Яндексу» в предустановке его приложений в смартфоны на Android, доля «Яндекса» в мобильном поиске выросла.



## ЦИФРОВОЙ ПРОФИЛЬ ЧРЕВАТ НОВЫМИ УТЕЧКАМИ

Комитет Госдумы РФ по государственному строительству и законодательству придерживается мнения, что в законопроекте о цифровом профиле не учтена проблема возможных утечек персональных данных граждан.

Недоработки документа в части сохранности и безопасности персональных данных могут спровоцировать рост числа киберпреступлений, связанных с утечкой информации. Хакеров может привлекать возможность получить разом большой объём данных из цифрового профиля.

Недочёты документа в этой части включают отсутствие ясной ответственности за несанкционированное использование данных. Также и непроработанность механизма обратимости сделок, совершённые без ведома владельца цифровой подписи.



# iFin-2020

XX ЮБИЛЕЙНЫЙ ФОРУМ

19-20 февраля 2020, г. Москва,  
«Рэдиссон Славянская»

**Электронные финансовые  
услуги и технологии**

### Спонсоры



### Партнеры



### Тематические акценты Форума:

- Электронные финансовые услуги и сервисы для физических лиц, ИП, МСБ и корпораций
- ИТ-базис современной финансовой организации. Совершенствование инфраструктуры. Цифровая трансформация бизнеса
- Информационная и кибербезопасность финансовых организаций и их клиентов
- СБП: С2С и В2С-переводы, С2В-платежи и эквайринг
- Маркетплейсы, финансовые экосистемы, небанковские услуги и сервисы в ДБО
- Открытый банкинг и Open API
- Клиентский опыт, интерфейсы и психология потребителей финансовых услуг
- Прорывные технологии настоящего и будущего в финансах: Big Data, AI, Роботизация, Биометрия, Блокчейн, IoT, AR/VR



## ОБЖ В ШКОЛЕ ДОПОЛНЯТ КУРСОМ КИБЕР- БЕЗОПАСНОСТИ

С предложением расширить школьный курс ОБЖ за счёт раздела о кибербезопасности выступили в Общественной палате и эту идею поддержали в Министерстве просвещения России.

Сейчас идёт работа над Федеральными государственными образовательными стандартами с учётом нововведений. Далее будет скорректирована школьная программа.

Эксперты считают, введение нового курса в школе позволит защитить детей от кибербуллинга, а также поможет объяснить школьникам правила безопасного поведения в Сети, включая защиту личных данных и умение распознавать мошенников и педофилов.



**Минпросвещения России**  
Министерство просвещения Российской Федерации

## БИОМЕТРИЯ НА ПАУЗЕ

В 2020 году принятия кардинальных решений в сфере биометрии не ожидается, принятие законопроекта о сборе биометрических данных приостановлено. Об этом сообщил председатель комитета Госдумы РФ по финансовому рынку Анатолий Аксаков.

«Законопроект по биометрии лежит в Госдуме. Мы приостановили его принятие, хотя Банк России настаивал на скорейшем принятии, в связи с тем, что аккуратно стараемся относиться к принятию цифровых законов. Известно, что и финансирование цифрового направления в национальных проектах идёт медленнее, чем в других направлениях, и многие законопроекты медленнее принимаются. Это связано с тем, что тема непростая, прежде всего связана с защитой прав граждан, защитой персональных данных, и с защитой бизнеса тоже», — сказал А. Г. Аксаков.

Парламентарий отметил, что использование биометрии пока не но-

сит массового характера — данная форма работы для граждан является новой и не очень востребованной. Сбор может быть дорогостоящим для банков, поэтому сначала необходимо проконсультироваться с рынком, а затем продвигать идею в правовом пространстве. Банки с базовой лицензией, отметил депутат, нужно вообще освободить от сбора биометрических данных. Универсальные системообразующие банки тоже не нужно обременять затратами, «если это не приведёт к благу для граждан, которые будут пользоваться данной услугой».



### IDC Security Roadshow 2020

**Будущее информационной безопасности: доверие к цифровым технологиям**  
Москва, 18 марта 2020 г.

#### Основные темы:

- Повышение киберустойчивости бизнеса, тенденции высокотехнологичных преступлений, инциденты нового типа и механизмы их предотвращения.
- Построение эффективной стратегии ИБ в условиях перехода к цифровой экономике.
- Культура ИБ в компании, управление рисками и будущее CISO.
- Оптимизация и повышение операционной эффективности ИБ.
- Использование ИИ и машинного обучения для автоматизации процессов обеспечения кибербезопасности и защиты данных.
- Изменение в нормативно-правовом регулировании в области защиты информации.

#### Аудитория:

- Руководители служб и директора по информационной безопасности крупнейших предприятий и организаций России, работающие с критически важными инфраструктурами.
- Аналитики по вопросам ИБ, ИТ-директора.
- Директора по управлению рисками.
- Топ-менеджеры мировых технологических лидеров в области ИБ.

Сайт: [www.idc.com/russia](http://www.idc.com/russia)

Более подробная информация у менеджера мероприятия Дарьи Сорокиной, [dsorokina@idc.com](mailto:dsorokina@idc.com)





## ТЕЛЕФОННОГО МОШЕННИКА ВЫДАСТ ЦИФРОВОЙ ОТПЕЧАТОК

В России предложен новый способ борьбы с телефонными мошенниками и спамерскими звонками — использование технологии цифрового отпечатка звонка. Инициативу выдвинула Ассоциация профессиональных пользователей социальных сетей и мессенджеров (АППСИМ), взяв за основу похожие технологии, над которыми работают зарубежные специалисты.

Решение — цифровой сертификат, оснащённый системой шифрования, присваиваемый операторами связи каждому звонку. Работает принцип белого списка — если прошёл звонок без цифрового отпечатка, вероятно, номер абонента подделан. В таком случае оператор может заблокировать такой звонок. Если предложенная концепция получит развитие, будет можно вычислять злоумышленников по цифровому отпечатку и местоположению. Если на этапе

проверки возникнет нестыковка данных, звонок просто не дойдёт до получателя.



## БЕСКОНТАКТНАЯ ОПЛАТА ДЛЯ СБП

Национальная система платёжных карт и банки прорабатывают возможность добавить в Систему быстрых платежей Банка России технологию NFC для бесконтактной оплаты смартфоном.

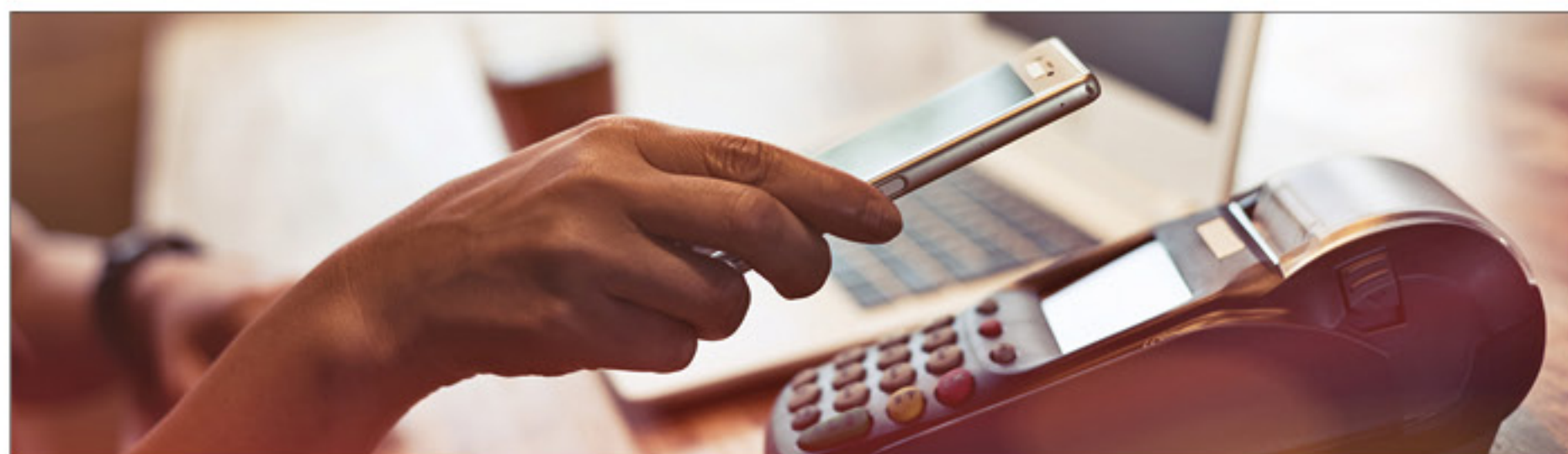
Обсуждение внедрения технологии ведётся с ВТБ, «Тинькофф банком», «Рокетбанком», «Открытием» и «Промсвязьбанком». НСПК изучает несколько вариантов использования NFC в СБП:

1) Магазины устанавливают NFC-метку, по наполнению идентичную QR-коду. Покупателю нужно будет поднести

к ней смартфон и подтвердить платёж. Иногда — ввести сумму покупки.

2) Покупатель прикладывает смартфон к терминалу с поддержкой бесконтактной оплаты. Терминал посылает сигнал на смартфон, пользователь выбирает приложение банка-участника системы и подтверждает оплату.

Для первой схемы может потребоваться разрешение Google и Apple на внедрение технологии в смартфоны. Второй сценарий только на один шаг меньше по сравнению с QR-платежом, поэтому несильно облегчит процесс платежа для клиента.



## ВОЕННЫЕ ОКРУГА ЦЕНТРАЛИЗУЮТ ОТРАЖЕНИЕ КИБЕРАТАК

В военных округах будут созданы центры предотвращения несанкционированного доступа к сетям и защиты от вредоносного ПО. Под их контролем окажутся военные линии связи и передачи данных.

Все центры будут объединены в глобальную систему и будут защищать трафик Минобороны России, поступающий из сетей гражданских операторов и из так называемого «военного интернета». Одна из задач киберцентров — обеспечение защиты от кибератак. Учреждения скорее всего будут в тесном контакте с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Офицеры, получившие специальность в области ИБ, будут в круглосуточном режиме осуществлять мониторинг сетей.

## ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ СТАНДАРТИЗОВАН

Росстандарт утвердил первые национальные стандарты в области искусственного интеллекта — ГОСТ Р 58776-2019 «Средства мониторинга поведения и прогнозирования намерений людей. Термины и определения» и ГОСТ Р 58777-2019 «Воздушный транспорт. Аэропорты. Технические средства досмотра. Методика определения показателей качества распознавания незаконных вложений по теневым рентгеновским изображениям».

Документ создает основу для развития интеллектуальных систем, эффективность функционирования которых напрямую зависит от возможности прогнозирования поведения людей». Он должен обеспечить эффективную коммуникацию интеллектуальных робототехнических систем с пользователем.



## УКРАИНСКИЙ НЕФТЕГАЗ ПОД ПРИЦЕЛОМ FANCY BEAR

Киберпреступная группировка Fancy Bear (APT28) провела фишинговую кампанию против нефтегазовой компании Burisma Holdings.

Хакеры нацелились на связанные с компанией Burisma «КУБ-ГАЗ», «ЕСКО-ПІВНІЧ» и «CUB Energy Inc». Злоумышленники использовали похожие домены, чтобы вынудить сотрудников компаний ввести свои емейл-пароли.

Корпоративный сайт подвергался многочисленным попыткам взлома в течение полугода. Взлом почтовых серверов мог привести к раскрытию переписки Хантера Байдена, который входил в состав совета директоров компании (в 2014–2019 гг.). Компромат на него, возможно, искали политические конкуренты его отца Джо Байдена, вероятно, соперника Дональда Трампа на выборах президента США в 2020 году.

## РУССКИХ «ПОХИТИТЕЛЕЙ ЛИЧНОСТИ» ОСУДИЛИ В США

Проживающие в США россияне Игорь и Денис Грушко были приговорены к 145 месяцам лишения свободы за «кражу личности» при отягчающих обстоятельствах, сговор с целью завладения и использования данных украденных банков-

ских карт, а также за изготовление поддельных кредитных карт и других документов.

В ходе обыска сотрудники правоохранительных органов США обнаружили резиновые формы и пластиковые смолы для изготовления скиммеров, сами скиммеры, наклейки для банкоматов, видеокамеры. А также устройство для изготовления кредитных карт и считывающее устройство для их магнитных лент, листы используемой в штате Мэриленд защитной голографической фольги и принтер для печати удостоверений личности, а также множество образцов поддельных кредитных карт и документов. На компьютере кардеров — тысячи номеров кредитных и дебетовых карт.

Соучастником братьев был гражданин Украины, 24-летний Вадим Вознюк, который получил 27 месяцев лишения свободы.



26-я Международная выставка технических средств охраны и оборудования для обеспечения безопасности и противопожарной защиты



Москва

13–16  
апреля  
2020

МВЦ «КРОКУС-ЭКСПО»

Бесплатный билет  
по промо-коду:  
**sec20BIS**



[securika-moscow.ru](http://securika-moscow.ru)



Видеонаблюдение



Контроль  
доступа



Охрана  
периметра



Противопожарная  
защита



Сигнализация  
и оповещение



Автоматизация  
зданий







# Kaspersky® Anti Targeted Attack Platform

## Комплексное решение для защиты от целевых атак и сложных угроз

- Блокирование сложных угроз и снижение риска целевых атак
- Постоянный мониторинг на уровне сети и рабочих мест
- Выявление аномалий в поведении объектов IT-инфраструктуры
- Экспертное сопровождение и помощь в расследовании компьютерных инцидентов
- Оценка потенциальных рисков IT-безопасности в текущей инфраструктуре

[www.kaspersky.ru/enterprise](http://www.kaspersky.ru/enterprise)

© АО «Лаборатория Касперского», 2019. Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей





# КТО ВИНОВАТ И ЧТО ДЕЛАТЬ?

ЭКСПЕРТЫ BIS JOURNAL О ТРЕНДАХ 2019 ГОДА<sup>1</sup>

**Н**акал страстей по поводу утечек клиентских баз данных возрастает. Сегодня они нужны всем: и «белым» и «чёрным». Записи о людях живут собственной насыщенной жизнью, в результате чего в смартфон любого человека попадают все, кто ни попадя.

Рыбу хорошо ловить в мутной воде. Как понять, кто скрывается за очередным телефонным звонком: мошенник или добропорядочный менеджер? В то же время в планах банков — монетизация обезличенных клиентских данных. Сбербанк уже объявил о запуске проекта продажи своего финансового трафика «всем, кому это может быть интересно».

Причину «мутной воды» видят в отсутствии определений и градаций открытости (публичной доступности) данных,

а также механизмов «открывания» и, наоборот, де-анонимизации личных данных. Профильные министерства и ведомства только-только начинают обсуждать, какую концепцию выберет Россия: «азиатскую» или «европейскую». Первая ставит во главу угла государство: оно является основным владельцем данных граждан, занимается их классификацией и защитой. Вторая определяет владельцем самого человека и базируется на жёстком законодательстве о приватности личных данных и их защите (например, GDPR).

\*\*\*

Вопросов много — ответов меньше. BIS Journal собрал мнения экспертов в надежде, что они станут затравкой для серьёзного разговора на Уральском форуме.

<sup>1</sup> BIS Journal благодарит журналиста Елену Покатаеву за активную помощь в подготовке раздела «Тема номера»



# «БОРОТЬСЯ НАДО С ПЕРВОПРИЧИНОЙ»

**У**малить роль социальной инженерии бессмысленно — это, действительно, мощный инструмент для внедрения в круг доверенных лиц человека. И это, действительно, становится возможным только потому, что большое число людей не соблюдают «правил гигиены» информационной безопасности. В этом смысле социальная инженерия будет действовать всегда — до тех пор, пока люди поголовно не научатся «мыть руки», вступая в информационные взаимодействия с виртуальными незнакомцами. Другое дело — насколько справедлив тезис о первичности социальной инженерии как корне нынешних проблем? На этот счёт есть большие сомнения.

Для начала элементарное соображение: чтобы до кого-то достучаться, мне нужен выход на него, то есть контактная информация. Плюс некоторая другая информация, которая позволит злоумышленнику психологически воздействовать на жертву. В этом вопросе есть несколько важных составных частей. В частности, доступные базы данных, из которых можно черпать эти индивидуальные сведения. Это отдельный интересный вопрос: люди сами оставляют в Интернете большое количество личной информации, и при нынешнем уровне развития средств аналитической обработки больших данных сформировался целый рынок коммерческих услуг по предоставлению данных на заказ. Из огромных залежей пёстрых данных с помощью информационных фильтров практически в автоматическом режиме формируются базы данных, поступающие в продажу, — фактически под любые задачи. Сегодня эта работа поставлена на поток: если раньше искали данные под задачу, и это было недешёвым заказным проектом, то сегодня предлагаются готовые базы под любую задачу, что, естественно, гораздо дешевле. В этой части, кстати, — непочатый край работы по созданию системы регулирования оборота личных данных граждан.

Так что, если говорить про «информационную гигиену», то она, на мой взгляд, должна насаждаться, в первую очередь, в этой части — ответственном отношении к раскрытию сведений о себе в публичном пространстве. Правда, в социальных сетях далеко не всегда содержится тот объём информации, который необходим.

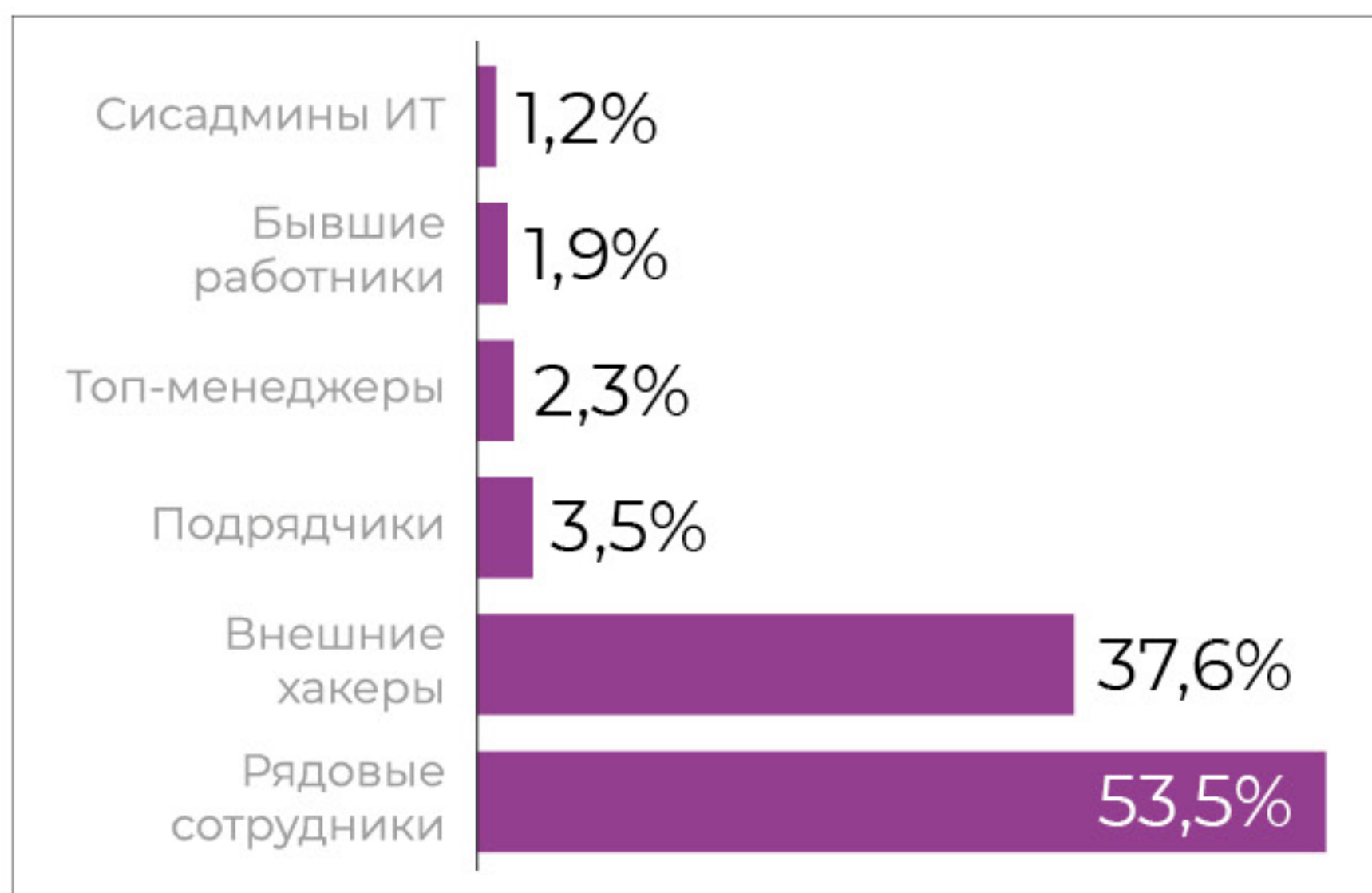
А вот если связать её с данными из банковских баз, получится отличный результат — синергия данных, которые работают вместе, усиливая друг друга. Таким образом, базовый канал получения сведений — это базы банков, то есть, собственно, контакт с жертвой, а публичная информация дополняет его полезными сведениями для убедительной обработки жертвы методами социальной инженерии.

Значит, бороться надо с первопричиной — утечкой базовых контактных данных из банковских систем, а не со следствием, воспитывая в клиентах информационную «чистоплотность». Первейшая задача — не дать в руки злоумышленников ИНСТРУМЕНТ воздействия на жертву, коим являются его личные данные. Если перекрыть мошенникам доступ к этим данным, вся социальная инженерия окажется бесполезной. Вот, собственно, однозначный ответ на вопрос, что является первичным? Базы данных и их защита.

Следует подчеркнуть, что в части этой защиты сделано далеко не всё возможное. В разговорах об утечках клиентских баз, как правило, упоминают обиженных сисадминов или уволенных сотрудников. Но посмотрите на профиль возможного нарушителя: эти категории занимают единицы процентов в общем количестве инцидентов, а более половины виновников — рядовые сотрудники (Рисунок 1).



**Сергей ВИХОРЕВ**  
советник  
генерального  
директора по ИБ  
ООО «ИТ-  
экспертиза»



**Рисунок 1.** Модель нарушителя для ситуаций утечки клиентских баз.  
Источник: отчёт аналитического центра INFOWATCH





С точки зрения технических решений, способы решения проблемы есть. В своё время Анатолий Васильевич Шеин, профессор МИФИ и автор знаменитого средства защиты НСД «Снег», выдвинул, на первый взгляд, парадоксальный тезис: если в информационной системе правильно организовано разграничение доступа (защита от НСД) на основе мандатного принципа, то антивирусная защита оказывается вообще не нужна. Действительно, в компьютере любые действия осуществляются через 13 прерываний, которые заложены в BIOS. И если разграничение доступа организовано правильно, то вирус, даже попав в систему, ничего сделать не может, поскольку у него вообще нет доступа к операциям. Система заражена, но продолжает работать в штатном режиме.

На мой взгляд, налицо ещё более важная системная проблема: те угрозы, которые сегодня реально существуют, не оценены должным образом. Более того, нуждается в дальнейшем развитии сам подход к защите информационных систем, который сегодня базируется на риск-ориентированной модели. Полагаю, что следует добавить отдельную группу рисков, связанную с риском утраты корпоративных данных. Это поможет структурировать угрозы такого плана и, что очень важно, сопоставить им параметры экономических потерь. Тогда может оказаться,

что потеря данных интеллектуальной собственности равносильна потере бизнеса, а утечки клиентских данных наносят ущерб лояльности клиентов на уровне сокращения бизнеса на порядок.

\* \* \*

Итак, подводя итог размышлениям. Ситуация с утечками клиентских баз подобна рассмотренной выше истории с защитой компьютера от вируса: с помощью технических мер можно сделать так, что некий сотрудник сможет добраться до клиентской базы, но ему не удастся её вынести наружу. А если нет базы, то и нет атаки, основанной на социальной инженерии. Этот подход радикально снизит уровень кибермошенничеств с банковскими счётами граждан. Однако и самим гражданам нужно помнить об «информационной чистоплотности» и не сорить своими личными данными ни в социальных сетях, ни в телефонных разговорах с незнакомыми людьми. Нередко в общественных местах мы видим плакаты с надписью «Бросать мусор запрещено!». Нужно, чтобы рядом с ними появились призывы типа «Человек, помни: раздавая направо и налево свои личные данные, ты превращаешь их в мусор, на котором развиваются всяческие болезнетворные инфекции!».



# «РАЗВЯЗАТЬ РУКИ ПОЛИЦИИ»

**В** начале о статистике по фроду. Так, карточный банкоматный фрод колеблется в пределах нескольких базисных пунктов (1 базисный пункт = 0,01 %). Тот же фрод, но уже в торгово-сервисных предприятиях, составляет 10 базисных пунктов. За уровнем фрода жёстко следят международные платёжные системы, и если фрод превосходит указанные нормативы, скажем, достигает 20–30 базисных пунктов, то эта торговая точка немедленно закрывается — таковы правила международных платёжных систем. Что же касается систем дистанционного банковского обслуживания, то там уровень мошеннических транзакций до недавнего времени был существенно занижен. После мер, принятых Банком России по более полному представлению банками статистики мошеннических транзакций, нынешней весной «внезапно» возник годовой прирост преступлений на уровне 40 %, что связано, конечно, не с ростом числа преступлений, а именно с тем, что ранее не было достоверной статистики.

Что касается пресечения утечек клиентских баз в руки социальных инженеров, то в нашем законодательстве нет даже понятия ответственности за утечки персональных данных (ПД). Иными словами того, кто допустил утечку, наказать практически невозможно. Конечно, сама возможность наказания существует, однако она относится к тем лицам или структурам, которые осуществили неправомерный доступ к базе данных, а это хакеры, которых перед тем, как наказать, нужно еще поймать. Законодатель так сконструировал нормы закона, что наказание за небрежное хранение ПД фактически не предусмотрено. Истории об утечках данных регулярно получают огласку, но нет информации о том, что кто-то понес за это наказание. Сравните эту ситуацию, например, с весьма жёсткими параметрами европейского закона GDPR.

Стопроцентная защита ПД на практике — вещь возможная, но труднодостижимая. Залить данные в бетон? Использовать технологии квантовых вычислений?

Между тем, сами банки работают по принципу «вы совершили этот перевод добровольно, поэтому мы ничего не должны вам возвращать». Напомню, что в соответствии со статьёй 9 закона «О национальной платёжной системе» (161-ФЗ), кредитная организация обязана возвращать деньги, которые были украдены у клиента со счёта в ходе противоправной транзакции. Но

даже если клиент успевает сообщить банку о такой транзакции в течение одного рабочего дня, как этого требует 161 закон, то до сих пор ещё ни один банк деньги, украденные социальными инженерами, не возвратил. Подчеркну, что кредитные учреждения мотивируют свой отказ тем, что клиент совершил операцию добровольно.

Однако следует помнить, что между банком и клиентом заключается договор банковского счёта, в соответствии с которым банк обязан выполнять указания клиента. А если он выполнил указание злоумышленника, значит, он нарушил договор, и пострадавшему человеку остаётся это доказать. Некоторым это даже удавалось... Если настырный клиент с неограниченными запасами терпения, средств и времени выходит на уровень кассационной жалобы на решение суда первой инстанции, то на этом этапе суд может принять сторону клиента, потому что ориентируется на постановление Пленума Верховного суда.

Другое дело, что есть и такие граждане, которые добровольно передают ПД злоумышленникам, или даже сами лично дают указания совершить платёж по заданным хакерами реквизитам. Эти граждане действуют как зомби, и это пример, так называемой, социальной инженерии 1 типа (СИ1). С такими гражданами — особая история, противодействовать атакам СИ1 невозможно. Даже если такого зомбированного клиента банк намертво защитит от возможных атак по каналам интернета, он найдёт способ перевести деньги, например, физически придёт в отделение банка и переведёт злоумышленникам все свои сбережения.

И в заключение ещё одна важная мысль — цифровые технологии дали мошенникам новый огромный набор специфических возможностей, которые ранее были недоступны. Конечно, противодействовать этим возможностям можно, но только обладая соответствующим цифровым инструментарием. Скажем, такой же инструментарий и возможности должны быть у полицейских.

*Есть и такие граждане, которые добровольно передают персональные данные злоумышленникам, или даже сами лично дают указания совершить платёж по заданным хакерами реквизитам*



**Тимур АИТОВ**  
заместитель председателя комиссии по цифровым финансовым технологиям ТПП РФ, заместитель генерального директора ГК «Программный продукт»



Так же, как банкиры контролируют перемещение финансовых средств, так и полицейские должны иметь возможность контролировать и вмешиваться в совершение платежей, следить за тем, кто именно переводит средства, куда, как, в какие сроки и так далее. Тогда и дело пойдёт, и будет, за что спросить. Конечно, такие расширенные возможности (если вдруг будут предоставлены органам МВД) тут же войдут в противоречие с действующим законодательством, в частности, с законом о банковской тайне.

С другой стороны, ПД продолжают поступать на чёрный рынок, и купить там сегодня можно, что угодно — тоже в явном противоречии с нормами законов. Получается так: преступникам нарушать закон и воровать ПД можно, а борцам с ними нельзя даже позвонить в соседний банк и назвать фамилию клиента-дропа, который только что снял деньги в одном из банков и двигается в следующий. Ведь надо перед звонком заручиться у дропа согласием на обработку его ПД...



**Виталий НОМОКОНОВ**  
профессор Дальневосточного  
федерального университета,  
вице-президент Российской  
криминологической ассоциации

#### BIS-КОММЕНТАРИЙ

## «ПОМОГУТ СПЕЦИАЛЬНЫЕ ПРОФИЛАКТИЧЕСКИЕ ПРОГРАММЫ»

**Н**адо сказать, что сегодня преступность вообще в мире, в том числе и в нашей стране, всё больше виртуализируется, уходит в сферу гаджетов и Интернета. В прошлом 2018 году число такого рода преступлений выросло за год почти в два раза (более 174 тыс. преступлений). За 9 месяцев 2019 года данная категория преступлений выросла уже до 205 тыс. (рост — 70%), что составило 13,5 % от всех совершённых преступлений. Это объясняется большей лёгкостью и сравнительной безопасностью совершения таких преступлений. Не надо по ночам с ножом или обрезом караулить жертву, не надо проливать чужую кровь. Гораздо приятнее извлекать денежные знаки, просто сидя дома за компьютером или телефоном. Сегодня таким способом облегчения карманов населения всё больше пользуются злоумышленники, причём, даже если они отбывают свой срок в местах лишения свободы.

Используются самые разные схемы. Так, например, мошенники стали активно использовать технологии подме-

ны исходящих телефонных звонков с номера на номера, идентичные номерам кол-центров кредитных организаций. Они нахально выдают себя за сотрудников служб безопасности банков. Под видом блокировок подозрительных транзакций мошенники совершают хищения средств своих жертв. Активно используются приёмы социальной инженерии, что связано не столько с собственно киберпреступностью, сколько со специальным негативным психическим воздействием на потерпевших.

\*\*\*

Для предупреждения такого рода мошенничеств банковским и иным заинтересованным организациям следует реализовывать специальные профилактические программы. Скажем, в одном из магазинов я слышал по громкой трансляции разъяснения Сбербанка для клиентов по поводу возможных мошеннических обращений к ним. Такую практику надо продолжить.



# «ГЛАВНАЯ СЛОЖНОСТЬ — В КОМПЛЕКСНОСТИ ПРОБЛЕМЫ»

**С**обственно, самой большой проблемой является то, что в одной точке сошлось несколько факторов, которые в сумме создают широкие возможности для совершения таких преступлений, и при этом ни государство, ни граждане оказались к этому не готовы. Что я имею в виду?

## СКОЛЬКО ФАКТОРОВ?

Во-первых, за 12 лет действия закона о «О персональных данных» наше государство так и не установило ответственность за утечку этих самых персональных данных. И утечки, естественно, стали массовым явлением: раз ответственности нет, а спрос есть, значит, утечки будут активно использоваться. Причём, что бы ни говорили банки, основным источником утечек является банковский персонал. Скачать несколько миллионов записей через Интернет никакой хакер не может, информацию явно выносят из недр банка. Злоумышленник, который занимается социальной инженерией, знает не только фамилию, имя и телефон, он знает и о наличии счёта, порой знает остаток на счёте, а иногда и номер карты, что гораздо больше того, что может стать известным при незлонамеренных утечках. Это первый фактор, стимулирующий рост таких кибер-преступлений.

Во-вторых, в нашей стране фактически нет ответственности за кибер-преступления. Наши суды относятся к ним крайне либерально: ограбить банк с автоматом в руках и вынести 5 миллионов в сумках — это до 15 лет лишения свободы, а вывести из банка 5 миллионов через Интернет — это два года условно. Такая ситуация создает очень благоприятные условия даже для тех, кто изначально, может быть, не был настроен на криминальные действия, но возник большой соблазн и новый лёгкий способ зарабатывать деньги.

Третья проблема заключается в том, что банки всех нас очень активно подталкивают к онлайн-платежам. Банку это выгодно по ряду причин. Во-первых, это даёт колоссальную экономию. Во-вторых, способствует увеличению скорости оборота денежных средств. В-третьих, это эффективный способ простимулировать существенные денежные траты граждан: они ведь

не видят реальных денег в своём кошельке, контроль за расходом денежных средств оказывается весьма ослабленным. На эту идею работают, в частности, так называемые экосистемы банков, которые объединяют множество банковских продуктов и услуг. Однако граждане к этому оказались совсем не готовы. По одной простой причине: их никто не учил жить в таких условиях.

Самый простой и эффективный способ борьбы с социальными инженерами известен: попросить звонящего назвать свою фамилию, имя, отчество и должность и сообщить, что я перезвоню ему по официальному телефону банка. На этом разговор заканчивается в 99,99 % случаев. Однако даже таких элементарных вещей люди не знают. А банк почему-то не рассказывает. Впрочем, можно догадаться, почему так: потому что статья 9 закона о национальной платёжной системе, которая предусматривает возврат денежных средств при неправомерных действиях, на настоящий момент вообще не работает. Деньги не возвращают, а виноват всегда этот несчастный пользователь банковских услуг.

Кроме того, дистанционные преступления очень эффективны с точки зрения ухода злоумышленника от ответственности. Действительно, никто на месте преступления преступника не поймал, видеокамера преступления не зафиксировала. Не удивительно, что в этот бизнес активно включился криминал, находящийся в местах отбывания наказания. Там, можно сказать, настоящие контакт-центры работают. Но государство с этим явлением почему-то тоже не борется. Интересно, что представители ФСИН каждый год предлагают методы борьбы с мобильными телефонами на зоне, но каждый год там изымается порядка 60 тыс. телефонов, хотя они вообще не должны туда попадать. Но раз они там оказываются, значит, как говорил классик, «это кому-нибудь нужно», кто-то этим системно управляет. Это, видимо, тоже часть криминального бизнеса...

## ПАЗЛ НАЧИНАЕТ СКЛАДЫВАТЬСЯ

И вот эти все аспекты на практике сложились вместе в течение очень короткого промежутка времени, и в результате появился очень лёгкий,



**Михаил ЕМЕЛЬЯННИКОВ**  
управляющий партнёр консалтингового агентства «Емельяников, Попова и партнёры»



## Перспектива миллионов штрафов заставит банки поменять отношение к защите баз данных и к действиям сотрудников, которые стоят за утечками

эффективный и, главное, высокодоходный способ незаконных заработков. А вот государство регулировать эту ситуацию не хочет...

Можно ведь усилить ответственность за утечки персональных данных, скажем, по примеру европейского закона GDPR. Там полагается штраф 10 миллионов евро или 2% оборота за попытку скрыть утечку и 20 миллионов евро, если в этом виноват оператор, допустивший утечку. А у нас? Вспомните, сколько утечек произошло за последние месяцы? И как отреагировали соответствующие банки? Например, банк сделал заявление, что утекшие данные не актуальны, и извинился перед всеми пострадавшими. Это всё!

ФАС в декабре опубликовала разъяснения, как надо жаловаться на спам: надо предоставить детализацию переговоров, запись аудио-разговора. Но я же не включаю диктофон каждый раз, когда отвечаю на телефонный звонок. В соответствии с такими правилами, никто не сможет обратиться с официальной жалобой! Значит, государство с этим явлением не борется. Попробуйте подать в полицию заявление о мошенничестве по телефону, над вами просто посмеются.

Вместо этого в Государственную Думу должен быть внесён законопроект о свободном обороте так называемых обезличенных данных. Изменит ли это ситуацию с социальной инженерией в лучшую сторону? Конечно, нет. От того, что мошенник будет по-прежнему многое знать о человеке, но не сможет его сразу назвать по имени, гражданам сильно легче не станет. А от того, что персональные данные станут рыночным товаром, которым можно будет легально торговать на рынке без согласия субъекта в «фантике» обезличенных данных, ситуация только усугубится.

### ПАЗЛ СЛОЖИЛСЯ

В результате сложился «пазл»: государство эту сферу не регулирует и не создаёт условий, ограничивающих возможности преступников, банкам такое состояние очень выгодно и удобно, а граждане недостаточно грамотны.

Главная сложность проблемы в том, что к ней нужно подходить исключительно комплексно, рассматривая одновременно весь набор причин, которые в совокупности привели к нынешне-

му плачевному состоянию: от отсутствия регулирования в разных сферах до отсутствия усилий по борьбе с этим злом. Частичные меры мало эффективны. Показательный пример. На конференции по персональным данным, где я вёл секцию в качестве модератора, представитель Банка России высказал такое мнение: наша главная задача — создать условия, чтобы утекающие данные были не востребованы на рынке. Представляете, сколько нам придётся ждать, пока эти данные станут невостребованными, как предлагает наш финансовый регулятор?

Нужно действовать решительно и сразу по всем ключевым направлениям. Во-первых, сильно ужесточить ответственность за утечки, чтобы банкам самим стало невыгодно допускать утечки клиентских баз. Перспектива миллионов штрафов заставит банки поменять отношение к защите этих баз и к действиям сотрудников, которые стоят за этими утечками. Во-вторых, нужно ужесточить ответственность за онлайн-преступления. Причём, имеет смысл сделать её гораздо более жёсткой, чем за попытку физической кражи, потому что у кибер-преступников гораздо больше возможностей для совершения преступлений, гораздо больше масштаб преступной деятельности.

И, наконец, государство должно отрегулировать оборот данных, не пускать их в свободное плавание до тех пор, пока не будут продуманы все необходимые механизмы. Яркий пример: заявляется о разработке законопроекта и свободном обращении обезличенных и больших данных, но у нас до сих пор ни в одном законе не дано определения, что такое большие данные. Если же мы не знаем, что именно собираемся регулировать, то как вообще можно говорить о грамотном регулировании?

\* \* \*

Только если действовать в этих направлениях одновременно и согласованно, можно рассчитывать на заметные подвижки в части киберпреступности с использованием социальной инженерии. И на этом фоне запустить социальную рекламу для граждан с правилами реакции на «звонок из банка». Скажем, не только таблетки от головной боли рекламировать по телевизору, но и «гигиену» телефонного общения. Правда, Центробанк в лице своего представителя сообщил, что это слишком дорогая затея. И это ещё одна задача для государства: продумать, что значит «дорого», когда речь идёт о массовых преступлениях против налогоплательщиков в финансовой сфере?



# «ПОЧЕМУ СИЛОВИКИ РАВНОДУШНЫ К БАНКИРАМ?»

**Н**ачну с того, что внутри системы двух участников — банк и клиент — данная проблема не решается. Нужно смотреть на ситуацию более широко и системно. Однако системного подхода к этому вопросу на данный момент не наблюдается. Любой человек, который берётся за решение этой задачи, собирает из лоскутков свою картину идеального мира. Большинство этих попыток однобоки и более всего напоминают шаманский «танец дождя»: шаман бьёт в бубен, танцует и вызывает дождь. Все составные части гармонично складываются в единую картинку: и танцор замечательный, и звук громкий, одна проблема — к дождю всё происходящее не имеет никакого отношения. У нас ситуация часто напоминает этот танец дождя. Мы боремся с технологиями, принимаем законы, запрещающие какие-то технические средства, но забываем о том, что преступления совершают люди, а не технологии!

Выделю ряд элементов, которые, на мой взгляд, являются ключевыми для рассматриваемой проблемы. Первая большая загвоздка заключается в том, что все попытки ИБ-сообщества доказать свою состоятельность разбиваются об одну вещь: у нас есть мощные инструменты реагирования на инциденты, но по факту регистрации в компании какого-либо события безопасности редко сразу же предпринимаются оперативные действия. Образно говоря, произошла утечка клиентской базы из банка, и оперативные службы отправляются на захват тех, кто в этом участвовал. Мне, конечно, сразу возразят, мол, киберпреступления совершаются в виртуале со скоростью клика, физическому реальному миру таких скоростей не достичь. Отвечу вопросом: а кто пытался хоть что-то сделать в этом направлении? Киберпреступления совершаются быстро, но готовятся долго. Так же и с мерами борьбы: должна быть подготовленная «виртуальная» почва, на которой будет разворачиваться сценарий действий в реале. Что я имею в виду?

## ПРО ПОЛИЦЕЙСКИЙ УЧАСТОК

Базовый принцип цифрового управления — наблюдаемость процессов. Нам идти и идти к тому,

чтобы понимание состояния киберпреступности приблизилось к тому уровню, который мы имеем в отношении реальной преступности. Фактически нужно строить такую же систему. Но сегодня в части киберпреступлений нет даже более-менее достоверной статистики о происходящем. Все понимают, что проблема существует, и пытаются её оценить со своего «шестка». В результате, сколько шестков, столько и видов статистики... Пожалуй, момент истины наступает в отдельно взятом полицейском участке, куда стекаются заявления от пострадавших граждан. Если туда заглянуть, то можно увидеть, какие стопки дел такого рода лежат на столах оперативных сотрудников МВД — это своего рода визуализация проблемы. А если посмотреть, как эта стопка выросла за год, это даёт представление о динамике проблемы. Однако никто не знает, что с этими заявлениями делать. А потому нет единой статистики, нет профилей



**Олег СЕДОВ**  
директор  
направления  
«Кибербезопасность  
для населения»  
«Ростелеком-Солар»





пострадавших и профилей злоумышленников и т.д. Есть ощущение, что «силы света» не очень-то и понимают, с кем нужно вступать в борьбу. Теперь приведу пример из сферы информационной безопасности.

### **А НА ТЁМНОЙ СТОРОНЕ ЦВЕТЫ... НЕОБЫЧАЙНОЙ КРАСОТЫ**

На одной из конференций по ИБ в секции по социальной инженерии я попросил участников из числа тех, кто становился объектом телефонной социальной инженерии, описать, как, по их мнению, выглядел злоумышленник, который находился в тот момент на другом конце провода. Говорили про мужчину, женщину, средний возраст и т.д. Но никто — а это, напомним, были ИБ-профессионалы — даже не предположил, что это могла быть роботизированная цепочка! На дворе — XXI век, а ИБ-профессионалы по-прежнему уверены, что на том конце провода — человек с телефонной трубкой и текстом сценария разводки на бумажке. А ведь на тёмной стороне задействованы огромные силы: знания лучших психологов, умения талантливых программистов, смарт-контракты, искусственный интеллект, передовые системы обучения. Мы на эти темы только доклады делаем на конференциях, а у них всё уже реализовано на практике, вложены конкретные серьёзные деньги.

Нельзя выделять один из целого комплекса вопросов, потому что мы живём в мире, в котором все границы стёрты. У нас нет отдельно взятой модели атак на конкретный банк. В них всегда задействуется много разных векторов: это могут быть и дети, взятые в заложники, и прослушанные телефоны, и акаунты в социальных сетях жены, подруги, родственники, подкупленные сотрудники. Всё идёт в ход, когда есть солидный призовой фонд. Угрозы приходят отовсюду и достигают результата в том месте, которому вы придаёте наименьшее значение.

### **ТУПИК**

Есть, в частности, одна такая точка, которая находится вне зоны внимания тех или иных служб. Структуры МВД не дернутся с места по факту фиксации утечки из какого-то банка. Силовики объясняют это тем, что они не могут начать действовать, пока нет заявления от банка, что он пострадал от киберпреступников. Но банк от такого заявления старается уклониться, потому что сразу после этого он из пострадавшего превратится в виновного, и его же, пострадавшего, и накажут. Как минимум дополнительной отчётностью. Тупиковая ситуация, скажем прямо.

И 152-ФЗ, принятый когда-то для того, чтобы персональные данные граждан не утекали на сторону, действует так, что защищает что угодно, но только не данные граждан. В целом, это большая проблема — отсутствие наработанной практики по делам, связанным с киберпреступлениями в отношении граждан.

Возможно, ситуация могла бы измениться, если бы такие дела можно было объединять в большую единую историю. Если у одного человека списали 500 рублей с карточки, то это совсем мелкое хулиганство, никто заниматься им не будет. Но если подобные дела будут объединены, то ущерб потянет уже на миллион рублей. И это уже будет хищением в крупных размерах, которое заставляет действовать. Но такой практики у нас, скорее, нет...

### **ВИНОВАТ ТОТ, КТО СЛАБЕЕ**

И вот в таких условиях предлагается искать виновного. Конечно, виновным проще считать того, кто слабее, то есть самого пострадавшего гражданина. Но разве это нормальная практика? Я считаю, что к этой ситуации вполне применимо простое житейское правило: в случае ссоры первым извиняется не тот, кто виноват, а тот, кто больше дорожит отношениями. И в этом смысле ближе всего к гражданину бизнес, в частности, банк, со счёта которого умыкнули деньги.

### **ПОЧЕМУ ТЫ КИБЕРДЫРЯВЫЙ?**

А как выглядит бизнес с этой точки зрения? Посмотрите на количество деловых журналов, которые нас окружают. И в каждом журнале обязательно есть статья на тему, как бизнесу стать здоровым, энергичным и т.д., — в стиле «если ты такой богатый, то почему у тебя офис некрасивый?». Но в этих журналах нет статей на тему: «если ты, бизнес, такой богатый, то почему ты такой кибердырявый?». Почему клиенты делятся с тобой своим самым сокровенным: деньгами, личной информацией, а твои сотрудники со своих телефонов ходят на какие-то сомнительные сайты, их смартфоны давно взломаны, и данные прослушивают все, кому не лень? Почему достойный клиент должен тебе верить, доверять свои коммерческие секреты и вообще иметь с тобой дело?

Я думаю, что это очень серьёзный момент: бизнес крайне редко занимается созданием образа защищённого надёжного партнёра. А ведь это составляет существенный кусок того, что сегодня называется кибергигиеной организации. Но этого нет в нынешней бизнес-ментальности. Яркий пример: не так давно на одной из



конференций по ИБ один человек из банковской среды спросил: «Что такое кибергигиена? Я хорошо знаю про финансовую грамотность, а кибергигиена — это, наверное, что-то из рекламы и маркетинга?». Этот человек, видимо, совсем не имеет представления, что этим словом называется такое состояние ума, при котором мы понимаем, что наша цифровая собственность — это именно собственность, а цифровая личность — это именно личность, которую точно так же, как и в реальной жизни, нужно уважать.

### НУЖНЫ СИЛЬНЫЕ ГОРИЗОНТАЛЬНЫЕ СВЯЗИ

Мошенники — они на то и мошенники, чтобы не уважать личность, но то, что граждане из легального бизнеса не имеют понятия об

уважении к цифровой личности, это реально плохо. Ну, хоть хакеры перестали в последние годы быть персонажами, которыми восхищается юное поколение. Хотя бы в общественном сознании они стали ассоциироваться с мерзавцами, ворующими у людей последнюю копейку. Но нужно, чтобы такое понимание стало всепроникающим: и в бизнесе, и в государстве.

А ведь государство может сыграть свою роль, например, объединить усилия на некотором горизонтальном уровне: с помощью межведомственного обмена данными сделать так, чтобы данные об утечках из финансовой сферы стали доступны для МВД, ФСБ и других органов. Но пока горизонтальные связи и оперативное взаимодействие выглядят крайне слабо и продолжают упираться в банальное «нет заявления от пострадавшего ...»



**Александр ИВАШКИН**  
председатель некоммерческого  
партнёрства «Лига финансовых  
институтов» (Владивосток)

BIS-КОММЕНТАРИЙ

## «НУЖНА АЛЬТЕРНАТИВА МЕГАРЕГУЛЯТОРУ»

**В**сё дело в том, что по мере развития технологий мошенники будут всё время опережать предложения продавцов, включая даже тех покупателей розничных финансовых продуктов, которые таким продуктом ещё вчера даже и не собирались пользоваться. Это естественная эволюция, происходящая в финансовой среде, на волне которой работают маркетологи и продавцы! Более того, дальше — с помощью баз данных, имеющих у оптового продавца на своих клиентов: у страховых компаний — ОСАГО, у крупного федерального банка, где скапливаются массивы данных, — потраченные деньги, владение автомобилем определённой марки, кредиты, переводы и др. — всегда будет вестись чёткая фрагментация рынка (по полу, возрасту, предпочтениям и пр.)!

И поверьте, на этом фоне обязательно и непременно будут появляться клоны тех, кто успешен на рынке. Вы знаете, сколько в России операционных касс раскрашены зелёным цветом под бренд Сбербанка? Или как страховые компании работают по ОСАГО, имитируя натуральность продажи этого обязательного для автомобилистов вида страхования? При этом жулики-банкиры пользуются прорехами законодательства.

Здесь единственное правильное решение: нужна альтернатива контролёру этого рынка — мегарегулятору, то есть Центральному банку. Но этого, боюсь, не случится... И второе: нужна финансовая грамотность населения — она является важнейшим фактором потребительского общества. Думаю, население не виновато в том, что ведётся на любые уловки финансистов. Причины уходят глубоко в область психологии и менталитета потребителя.





**Сергей ГОЛОВАНОВ**  
ведущий  
антивирусный  
эксперт  
«Лаборатории  
Касперского»

# «ВИНОВАТА ЧЕЛОВЕЧЕСКАЯ ЖАДНОСТЬ»

**У**течки клиентских баз — это, безусловно, горячие новости 2019. В прошлом году злоумышленники постоянно совершенствовали свои инструменты для получения чувствительной информации, а компании внедряли новые системы защиты. Однако риски, которые иногда описывались в СМИ, были преувеличены.

## ПОЧЕМУ ВСЁ НЕ ТАК

Во-первых, часть утечек, в которых обвиняют финансовые организации, происходят вовсе не по их вине. Информация может быть украдена, например, из компаний, сотрудничающих с банком, или агрегаторов информации. Необходимо понимать, что защите конфиденциальных и личных данных в банках уделяют огромное внимание, а у небольших компаний для этого гораздо меньше ресурсов. Типичный пример может выглядеть так: человек сам оставляет данные своей банковской карты на сайте торговой организации или иные сведения о себе, заполняя анкету для получения какого-нибудь подарочного сертификата. Если эти сведения потом стали достоянием злоумышленников, это вовсе не означает, что утекли они именно из финансовой организации. С такими случаями мы регулярно сталкиваемся на практике в ходе расследований: источником украденных данных оказывалась сторонняя организация. Это у неё были проблемы с защитой данных, и злоумышленники атаковали именно её, а вовсе не финансовую организацию.

Во-вторых, нуждается в пояснении, из-за кого чаще всего происходят такие утечки? Например, встречается утверждение, что главный виновник происшествий — инсайдер, то есть сотрудник банка, именно через него происходит самая большая доля утечек клиентских данных. Глядя на такой статистический «портрет», я сразу хочу задать вопрос: что считали? Количество обращений к базам данных или объёмы украденных данных? В разных случаях будут разные ответы. Поясню свою мысль.

Есть такой известный метод получения данных из систем банка, который на жаргоне бан-

ковских сотрудников называется «пробивом»: сотрудник не скачивает базу полностью, а по запросу выбирает данные, связанные с конкретными клиентами. Обычно заказ на такие сведения покупатель размещает на закрытых интернет-форумах либо использует Telegram с закрытыми чатами и т.д. А нечистый на руку сотрудник банка, польстившийся на обещанное вознаграждение, со своего рабочего места выполняет запрос к клиентской базе, вытаскивает нужные персональные данные по конкретному запросу.

Сервисов, которые предоставляют услугу подобного «пробива», немало, счёт идёт на десятки. Владелец каждого такого сервиса ищет заказчиков на информацию из базы финансовой организации, и также инсайдеров — исполнителей. Если теперь задуматься, каких событий больше: обращений сотрудников банков за информацией с целью дальнейшей продажи или хакерских атак извне? — то окажется, что человек в качестве источника утечек встречается неизмеримо чаще. Однако, с точки зрения массовости утечек, конечно, далеко впереди окажутся хакерские атаки — они в ходе одного инцидента могут утащить миллионы записей. Так что вопрос в том, что считаем: если количество обращений в штуках, то больше всего происшествий по вине инсайдеров. Если же считаем количество украденных гигабайтов данных, то главные виновники — внешние хакеры.

В-третьих, не всегда понятен сам термин «клиентская база» банка. Люди, далекие от внутренней жизни финансовой организации, обычно представляют её в виде одной компьютерной программы, которую можно легко забрать себе с помощью команды «Копировать». Но это совсем не так. Система, которая хранит клиентские данные, — гигантская. Она занимает огромное хранилище, может быть, даже целый этаж, заставленный компьютерами, жёсткими дисками и специальным оборудованием. Причём у разных функциональных систем могут быть отдельные хранилища, скажем, для карточного процессинга — одно, а для интернет-



банкинга — другое. Данные могут быть разнесены также на несколько офисов, городов и даже стран, если банк международный.

Собственно, из-за всех этих факторов по каждому факту утечки данных требуется специальное расследование, потому что очень много источников, откуда могут быть извлечены разные данные.

### МОЙ ПРОСТОЙ ОТВЕТ

Теперь, приняв во внимание все подробности, о которых я рассказывал, попробуйте дать короткий ответ на вопрос: кто виноват? Это будет не просто, так как сами ситуации очень непростые. Но у меня как у человека, который давно занимается этими вопросами, есть свой простой ответ. Виновата человеческая жадность. И это не является уникальным свойством нашей страны. Это общее для всего мира свойство человеческой натуры. Взрыв мошенничества, который мы наблюдали в 2019 году, — это новый подход к обычному обману.

### ДАЛЕКО НЕ НОВИНКА

Телефонное мошенничество — далеко не новинка 2019 года. Подобная «эпидемия» прошла лет семь назад, когда рассылали SMS о блокировке карты. Тогда научились блокировать SMS с подменой номера. Нынешний вал мошенничеств связан с новой уловкой злоумышленников. По сути, они использовали психологическую неготовность граждан скептически относиться к звонкам в новой реальности. Можно провести аналогию: в Москве конца 90-х, когда мобильный телефон — ещё редкость, к вам на улице подходит человек и говорит: я про вас многое знаю, например, как вас зовут, и в каком банке у вас открыт счёт, на этом основании отдайте мне деньги из вашего кошелька. Бред, скажете? Но, по сути, то же самое происходит во время телефонного разговора. Пройдёт немного времени, и все это осознают. То есть общество выработает систему защиты от этой конкретной напасти. Ну а злоумышленники пойдут искать новые методы и способы отъёма денег у граждан...

Системы защиты постоянно развиваются, какими именно они будут в будущем, я точно сейчас сказать не могу. Но то, что кибербезопасность будет комплексной, это очевидно. Очевидно в том числе потому, что она уже выстраивается. Возьмите, к примеру, ФинЦЕРТ. Если 10 лет назад каждый банк защищался от злоумышленников как мог, самостоятельно, то потом регулятор решил создать ФинЦЕРТ и накрыть этим «куполом» защиты все финансовые организации. Подобный процесс идёт в отно-

*Системы защиты постоянно развиваются, какими именно они будут в будущем, я точно сейчас сказать не могу. Но то, что кибербезопасность будет комплексной, это очевидно*

шении критической информационной инфраструктуры. Стало ли лучше? Однозначно. Скажу по своему личному опыту: пять лет назад у меня было много выездов на расследования в районе Садового кольца, Третьего транспортного кольца, а теперь я путешествую в основном по зарубежью. По одной причине — здесь инцидентов становится меньше, потому что научились защищаться.

\* \* \*

Кстати, наши проблемы 2019 г. — вовсе не новинка для остального мира. Нечто подобное прокатилось по Западной Европе несколько лет назад. Разница — в деталях: там звонили главным образом не физическим, а юридическим лицам. А в остальном — знакомый сценарий социальной инженерии. Всё это уже было в других странах. И теперь пришло к нам. На Западе с этим научились бороться. В частности, появился GDPR, общая директива Евросоюза, которая единым «зонтиком» накрывает все организации, независимо от их сферы деятельности: всем вменено в обязанность защищать персональные данные граждан. А тот, кто проявит халатность, будет строго наказан. Думаю, что что-то подобное появится и у нас в стране. Ведь источники утечек, как было сказано в самом начале, могут быть не только в финансовой организации, и не будет особого смысла вводить жёсткие штрафы именно для банков, если сервисные компании, агрегаторы данных окажутся за границей этих мер. Сейчас давление на регуляторов растёт, и это дополнительно стимулирует их деятельность, например, в области обращения личных данных граждан, которая уже запланирована, скажем, в рамках госпрограмм цифровизации. Вновь приведу пример ФинЦЕРТ: он появился не в пожарном порядке, его создание было продумано и тщательно спланировано. Так и с циркулированием персональных данных: уверен, что необходимые процессы уже идут и скоро выйдут на поверхность, станут заметны всем.



**Василий  
ОКУЛЕССКИЙ**

заместитель  
начальника службы  
информационной  
безопасности Банка  
«Возрождение»,  
кандидат технических  
наук

# НЕ УЧЕНЬЕМ ЕДИНЫМ

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ МНОГОГРАННА,  
НО ДЛЯ СПЕЦИАЛИСТОВ СЕКРЕТОВ В НЕЙ НЕТ

**В** последнее время самая модная тема в сфере безопасности ДБО — это социальная инженерия (СИ). Кто и где только не говорят о ней! «Новые технологии мошенников», «Крах технической защиты» и т.д. и т.п. Что это: очередной «хайп» или, действительно, что-то новое?

## ИСТОРИЯ И ЗАКОНОМЕРНОСТИ

Само понятие «социальная инженерия» ввёл в употребление Кевин Митник — знаковая фигура в сфере ИБ, бывший хакер серьёзного уровня. Однако злоумышленники использовали такие методы задолго до появления самого термина.

История мошенничеств с использованием СИ уходит своими корнями во времена появления дистанционных каналов банковского обслуживания — более 30 лет назад, когда идентификация клиента при проведении операции стала опосредованной. Всё это время уровень мошенничеств менялся волнообразно, всплески соответствовали периодам появления каких-либо новых банковских технологий, услуг или продуктов. Цепочка в этой области выстраивалась в классической последовательности: новое технологическое решение — всплеск мошеннической активности — разработка контрмер — стабилизация активности — распространение контрмер — спад активности. И так до появления новых решений. В среднем на рынке каждые два-три года, а теперь и чаще, появляется что-то новое, и цепочка запускается вновь. Обычный цикл составляет примерно 8–9 месяцев, после чего наступает незначительный период внешнего спокойствия, когда обе стороны борьбы собираются с силами и пытаются придумать что-то особенное. Сейчас мы находимся в фазе относительной стабилизации — контрмеры выработаны и происходит их распространение.

## В НАСТОЯЩЕЕ ВРЕМЯ

В настоящее время уровень атак на клиентов банков в целом стабилизировался, более того, наблюдается постепенный спад. Основной спо-

соб борьбы текущего момента — повышение осведомлённости как непосредственно клиентов, так и сотрудников банков о рисках реализации мошенничеств с использованием телефонных звонков. Повышение осведомлённости происходило и продолжается на всех уровнях и в самых разных аудиториях — СМИ, интернет, социальные сети, специальные памятки, «напоминалки» в личных кабинетах, выступления на конференциях, открытых уроках, включение соответствующих разделов в программы обучения и т.д.

Судя по информации из тех же СМИ, эта деятельность оказалась относительно успешной.

Если с начала последнего витка, т.е. примерно с середины лета 2019 года, «успешным» был каждый третий звонок мошенников (при этом суммы списаний были самые разные — от одной тысячи до миллиона рублей), то сейчас, благодаря большой разъяснительной работе сотрудников банка, уровень реализованных мошенничеств снизился в десяток раз. На пике этих мошенничеств, по словам первого заместителя директора ДИБ БР Сычева А.М. (из выступления на осенней сессии Уральского Форума 2019), по стране уровень мошенничеств, связанных с социальной инженерией, составил до 97% от всех мошенничеств и достиг суммы более миллиарда рублей. Из последующих выступлений сумма мошенничеств увеличивалась незначительно.

## ПОПРОБУЕМ РАЗОБРАТЬСЯ

Методы социальной инженерии направлены, как правило, на достижение двух целей: получить недостающие для мошенничества учётные данные клиента или установить вредоносное программное обеспечение на электронные средства проведения платежей. В нашем случае преследуется первая цель, мошенники используют полученные из самых разных источников обрывочные сведения о клиентах (например, из баз данных телекоммуникационных компаний, данных on-line сервисов по оплате товаров и услуг и т.д., где могут фигурировать



номера телефонов и имена-отчества клиентов, слипы электронных чеков с последними цифрами из номера карты и др.), затем эти данные специальным образом собираются, систематизируются и из них готовятся базы данных для обзвонов. Не секрет, что в некоторых банках такими источниками клиентских данных являются недобросовестные сотрудники, злоупотребляющие служебным положением. Далее подготовленные данные поступают на специальные площадки, имитирующие работы Call-центров, зачастую такими площадками являются исправительные заведения. Для таких «сотрудников» специально обученные психологи пишут скрипты звонков, цель которых удержать клиента на линии, получить от него недостающие данные о номере карты и коды подтверждения операции.

Сама мошенническая операция достаточно стандартная: одновременно со звонящим второй «сотрудник» открывает страницу регистрации Интернет-банка, используя полученные от первого сотрудника цифры номера карты и коды подтверждения, входит в Интернет-банк от имени клиента, отключает СМС-информирование о списаниях, переводит все денежные средства со счетов клиента на счета его банковских карт, а затем с карт делает переводы на мошеннические карты, включая виртуальные карты других банков, электронные кошельки, покупки в интернет-магазинах и т.д.

Основная «изюминка» таких манипуляций состоит в том, что все переводы подтверждаются одноразовыми паролями, сообщёнными клиентами мошенникам добровольно.

### КАК С ЭТИМ БОРОТЬСЯ?

В рассматриваемом случае главный объект воздействия — это сам клиент — человек. И основной упор борьбы с СИ, конечно, социальный. Человеку надо настойчиво объяснять, разъяснять, показывать на примерах, как надо и как не надо общаться с незнакомыми людьми. Регулярно напоминать, что сотрудники банка **никогда** не спрашивают данные карт у клиентов и не просят сообщить коды подтверждения. В этой работе никогда не надо забывать о правиле Парета. Клиенты в основной своей массе (80%) вполне нормальные (с точки зрения информационной безопасности) люди и в полной мере осознают риски мошенничества. Часть клиентов (10% справа) параноики безопасности, и они не только соблюдают рекомендации банков, но придумывают собственные способы защиты за пределами разумной достаточности. И только незначительное число (10% слева) подвержены этой самой СИ.

*Надо серьёзно анализировать все категории своих клиентов, по самым разным аспектам — возраст, пол, образование, социальную среду, типовые транзакции, хобби и т.д.*

Самое обидное в расходовании средств на «повышение осведомлённости» то, что мы ориентируемся на 80% аудитории, имея в виду при этом «10% слева», до которых все наши усилия так и не долетают. Иначе говоря, вся разъяснительная работа должна строиться с учётом конкретной аудитории воздействия. Это означает, что надо серьёзно анализировать, во-первых, все категории своих клиентов, по самым разным аспектам — возраст, пол, образование, социальную среду, типовые транзакции, хобби и т.д., т.е. по любым доступным признакам. Это позволит точнее понять «среду обитания» клиентов, а затем по каждой выделенной категории (совокупности категорий) провести анализ частоты и характера мошенничеств. Такой анализ покажет, как надо работать с каждой категорией для повышения именно её осведомлённости.

### ВО-ВТОРЫХ!

И вот тогда приходит «во-вторых». Тут необходимо разрабатывать не просто какие-то программы повышения осведомлённости, но и типичные каналы доведения этой информации до каждой выделенной категории клиентов. Простой пример. Ещё пару-тройку лет назад основной категорией потерпевших были люди старшего возраста, преимущественно пенсионеры. Работа именно с этой категорией по специфическим каналам информирования (программы «активное долголетие», программы повышения финансовой грамотности в банках, клубах по интересам и т.д.) сместило фокус на более активные группы клиентов — молодёжь с высшим образованием и активным проникновением в интернет-сервисы. Соответственно, работу надо выстраивать заново, не прекращая предыдущей.

### НЕОБХОДИМО, НО НЕДОСТАТОЧНО

Повышение осведомлённости — это многообразный, многослойный процесс, и эта статья — одна из его составляющих. Другие составляющие — памятки на сайте, рекомендации по безопасности на сайте и в личном кабинете, консультации клиентов, выступления в СМИ и т.д. Большую работу в этом направлении делает и БР.



*Анализируя сотни телефонных звонков злоумышленников, можно сделать вывод, что существует не более 5–6 сценариев их действий. Основные различия касаются «зацепки клиента» и алгоритмов вывода средств со счёта*

### ВАЖНЫЕ МЕРЫ

Понятно, что только разъяснительно-воспитательной работы недостаточно.

Дополнительно я бы выделил ещё меры, как минимум, в двух направлениях:

- ♦ разрушение социально экономической базы «исполнителей» из числа обитателей и охранников подразделений исполнения наказаний
- ♦ разработка специальных технических решений.

### УДАР ПО «ЭКОНОМИКЕ»

Экономическую основу таких правонарушений всегда составляет соотношение стоимость реализации атаки / полученный «доход». Это классика жанра. В данном случае «экономической основой» является низкая стоимость получения исходных данных для проведения атаки, практическое отсутствие специального инструмента, «дешёвые» способы сокрытия истинных номеров звонящих телефонов и, как следствие, практически отсутствуют требования к специальной подготовке исполнителей. Специальные технические решения должны быть направлены, во-первых, на резкое повышение сложности и стоимости получения исходных данных для телефонных звонков, во-вторых, создание системы невозможности подмены номера на номер банка, и, наконец, в-третьих, на доработку антифрод-систем, контролирующих платежи физических лиц.

Повышение стоимости и сложности добычи «исходных данных» может быть достигнуто усилением контроля доступа к базам данных, содержащим чувствительные клиентские данные. Это огромный пласт работы, содержащий и выверку ролей, и поддержание актуальных доступов, и актуализацию различных отчётных и учётных форм, и использование систем контроля доступа к базам данных. Такой комплекс мероприятий позволит максимально минимизировать вероятность несанкционированного доступа и копирования чувствительной информации, и, соответственно, её утечки.

Банком России совместно с телеком-компаниями проводится большая работа в области

правомерности использования номеров телефонов банков, и есть надежда, что эта работа даст свои результаты.

### РАЗРАБОТКА АЛГОРИТМОВ И ВЗАИМОДЕЙСТВИЕ БАНКОВ

И, наконец, разработка и внедрение специальных алгоритмов анализа поведения клиентов при работе в системах ДБО с целью выявления нехарактерных для клиента действий. Анализируя сотни телефонных звонков злоумышленников, можно сделать вывод, что существует не более пяти-шести сценариев их действий. Основные различия касаются «зацепки клиента» и алгоритмов вывода средств со счёта. Коль скоро выявляется алгоритм действий мошенника, то появляется возможность разработки алгоритмов контроля поведения плательщика с целью выявления нетипичных операций и способ их проведения. Использование такого рода алгоритмов в антифрод-системах позволит временно блокировать операции, дожидаться пока клиент «остынет», и тогда вернуться к проведению операции ещё раз.

Если средства всё-таки утекли, то надо не забывать про улучшение взаимодействия банков между собой, в том числе через каналы ФинЦЕРТ Банка России, для организации возврата средств, списанных со счетов клиентов без их согласия.

### ИТОГО

Для финансовых организаций нужно пытаться реализовывать всё перечисленное выше. И в работе с клиентами с учётом аудитории не уставать доводить рекомендации до клиента: беречь от доступа третьих лиц свои средства электронных платежей — платёжные карты, мобильные телефоны, планшеты и компьютеры. Не разглашать данные карт и в каких банках открыты счёта.

\* \* \*

И постоянно напоминать клиентам, что сотрудники банка никогда не спрашивают данные карт у клиентов и не просят сообщить коды подтверждения. Если такое случается, необходимо запомнить последовательность вопросов мошенников и сообщить об этом в банк по телефону на банковской карте. И если всё-таки случилась неприятность, надо срочно связываться с банком и срочно блокировать карту. Иногда удаётся вернуть деньги.



# СЕМЬ РАЗ ОТМЕРЬ

## ПРАКТИКА УМЕНЬШЕНИЯ УЩЕРБА ОТ УТЕЧЕК КЛИЕНТСКОЙ ИНФОРМАЦИИ В БАНКОВСКОЙ ОТРАСЛИ

**З**а последние 10–20 лет утечки стали казаться неизбежным злом в банковской отрасли, но, как и всякая проблема, утечки поддаются управлению по мере их структурирования и конкретизации. В статье мы рассмотрим ряд ситуаций, связанных с утечками в банках, предпринятые меры, а также упорядочим их, используя актуальные своды лучших практик.

### СИТУАЦИИ И ПРЕДПРИНЯТЫЕ БАНКАМИ МЕРЫ

**Ситуации 1–2.** Российский банк с развитой розничной сетью и бизнесом кредитования (Банк А) обнаружил, что его потенциальных заёмщиков уводят другие банки. Конкурентная борьба за клиента активизировалась сразу после проведения Банком А этапа кредитного конвейера «Оценка платёжеспособности клиента». Таким образом, банк, понеся затраты на клиента, не получал от него дохода, и клиент становился убыточным без возможности поправить ситуацию.

По итогам расследования выяснилось, что клиенты получали контрпредложения от самых разных банков, а значит, маловероятно, что кто-то из сотрудников продал целую базу одному конкретному банку. Служба ИБ Банка А стала проводить техническое расследование всех обстоятельств работы с базами данных, но не нашла следов копирования и вывода всей базы, и приступила к анализу других каналов доступа к базе, в первую очередь, доступа розничных отделений.

В результате выяснилось, что сотрудники розничных отделений воровали данные клиентов «по одному» и продавали их кредитным брокерам. Так как доступ к данным клиентов является рабочей необходимостью сотрудников отделений, то запретить его было нельзя, но банк внедрил специализированное программное обеспечение (WAF — Мера 1), которое выявляло

подозрительный доступ сотрудников розничного отделения к клиентским данным с помощью технологий машинного обучения.

В частности, система считала аномально большое число обращений к данным (больше, чем у других сотрудников такого же профиля), а также аномально большое число обращений во внеурочное время — время, когда другие сотрудники отделения не могли спросить коллегу, почему он (она) переписывает данные клиента.

В подобной ситуации другой российский инвестиционный банк (Банк Б) использовал другое решение: внедрил программное обеспечение, целью которого была простая запись всего, что происходило на экране и всего что вводилось с клавиатуры (UBA — Мера 2). Сотрудники знали, что за ними ведётся наблюдение и не имели возможности массового безнаказанного воровства информации.



**Александр  
БОДРИК**

управляющий  
партнёр бизнес-  
инкубатора  
по кибер-  
безопасности  
Cyberlands B.V.,  
вице-президент  
по ИБ ISACA  
Moscow Chapter





**Ситуация 3.** Российский банк с развитой сетью POS-кредитования (Банк В) в рамках реализации стратегии информационной безопасности решил выявлять перемещение больших объёмов данных — потенциальных утечек. Банк запросил коммерческие предложения производителей решений класса «предотвращение утечек» (DLP), но предложенные варианты показались ему дорогими. Вместо DLP банк внедрил комплекс мер, состоящих из межсетевого экрана следующего поколения (NGFW — Мера 3.1), обновления системы сбора и анализа событий безопасности (SIEM — Мера 3.2) и обновлённых регламентов реагирования на потенциальные утечки. Совокупная стоимость владения комплексом мер была снижена в три раза (20 млн руб. против 60 млн руб. в случае с DLP).

**Ситуация 4.** Крупный российский банк с фокусом на обслуживание корпоративных клиентов (Банк Г) получил письма от вымогателей. Преступники угрожали раскрытием неведомо как полученных ими клиентских данных и даже предоставили на проверку образец — оказавшийся достоверным. Банк отказался платить преступникам и передал всю информацию в правоохранительные органы. В процессе расследования выяснилось, что клиентские данные Банка Г предлагались на подпольных форумах киберпреступности (CyberUnderground). Для проактивного выявления таких объявлений банк создал у себя функцию мониторинга угроз (киберразведки) — Мера 4, а также приобрёл подписку на перечень потенциально скомпрометированных клиентов (подписка Threat Intelligence — Мера 5).

**Ситуация 5.** Крупный российский банк с фокусом на обслуживание корпоративных клиентов в ЦФО (банк Д) обнаружил, что к базам данных АБС в качестве администраторов имеют доступ 200 учётных записей. Столько учётных записей накопилось за года, и эта цифра в 50 раз превысила ожидания ИТ-директора. Каждая из указанных учётных записей позволяла скопировать либо удалить массивы данных в АБС. Поразмыслив, банк ввёл регламент мониторинга безопасности баз данных (Мера 6), в частности: регулярная проверка списка администраторов, проверка настроек безопасности баз данных. К слову, банк обнаружил такое количество администраторов с помощью специализированного комплекса защиты баз данных (DAM — Мера 7).

### СИСТЕМНЫЙ ПОДХОД

Несмотря на действенность указанных мер, применять их изолированно, подобно рецептам из поваренной книги, не рациональ-

но — банковское дело не терпит вкусовщины. Упомянутые и другие меры могут быть упорядочены с использованием известных развитых стандартов информационной безопасности, например, стандарта Национального института стандартов и технологий США по защите критических информационных инфраструктур (NIST CSF). Стандарт подразумевает 6 стадий противодействия киберрискам: Идентификация (Identify), Защита (Protect), Выявление (Detect), Реагирование (Respond) и Восстановление (Recover).

Соответственно, ранее указанные меры относятся к следующим стадиям:

#### 1. Идентификация

1. Мера 4 — направление киберразведки
2. Мера 5 — подписка Threat Intelligence

#### 2. Защита

3. Мера 3.1 — межсетевой экран следующего поколения
4. Мера 6 — регламент мониторинга защиты баз данных
5. Мера 7 — комплекс защиты баз данных

#### 3. Выявление

3. Мера 3.2 — система сбора и анализа событий безопасности
4. Мера 1 — система выявления подозрительного доступа к клиентским данным через браузер
5. Мера 2 — система мониторинга поведения сотрудников

В отношении утечек реагирование и восстановление часто происходит в том числе и в публичной плоскости. Чтобы чувствовать себя увереннее, отвечая на вопросы журналистов, можно подготовиться загодя, например, последовав примеру QIWI. Компания подготовила сайт ([qiwi.com/security.action](https://qiwi.com/security.action)) с такой информацией о системе ИБ банка, раскрытие которой ещё не влияет на степень защиты, но уже готовит общество к мысли о серьёзном отношении банка к безопасности своих систем и клиентских данных.

\* \* \*

Инвестиции в безопасность клиентских данных сложнее всего просчитываются на ранних этапах (Идентификация и Защита), но эти же этапы приоритетны, так как работа на них даёт банку время справиться с атакой злоумышленников или саботажем сотрудников. Утечки клиентских данных разрушают доверие к банку, а значит, ведут к оттоку клиентской базы и к увеличению стоимости привлечения клиентов в будущем.





# Центр обработки инцидентов / ЦФТ-ЦОИ

**Сервис для взаимодействия банка с АСОИ «ФинЦЕРТ»**

- Сбор, регистрация, обработка инцидентов информационной безопасности банка
- Формирование единой базы инцидентов
- Отправка данных в ЦБ по протоколу безопасности «ФинЦЕРТ»
- Автоматическая загрузка в АБС и работа с файлами фидов из «ФинЦЕРТа»



Web-интерфейс  
Модель использования – в облаке  
Лёгкая интеграция в IT-ландшафт банка  
Соответствие требованиям ИБ и законодательства  
Оптимизация затрат банка на организацию подключения к сервису





**Анатолий АКСАКОВ**  
председатель Комитета  
Государственной Думы РФ  
по финансовому рынку

# СТОП-ЗНАК ДЛЯ «ТЕЛЕФОННЫХ МОШЕННИКОВ»

ФИНАНСОВЫЕ ОРГАНИЗАЦИИ СМОГУТ ОПЕРАТИВНО  
ПРОВЕРЯТЬ НОМЕР МОБИЛЬНОГО ТЕЛЕФОНА КЛИЕНТА  
ЧЕРЕЗ «ЕДИНЫЙ ШЛЮЗ»

**О**дним из распространённых средств мошеннических операций со средствами клиентов финансовых организаций стало использование номеров чужих мобильных телефонов. Помочь решить эту актуальную проблему призван проект федерального закона № 514780-7 «О внесении изменений в Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путём и финансированию терроризма» и иные законодательные акты Российской Федерации», над которым идёт работа в Государственной Думе РФ.

## СТОП «ТЕЛЕФОННЫМ МОШЕННИЧЕСТВАМ»

Одной из наиболее существенных проблем в последние годы было и остаётся значительное количество лиц, пользующихся мобильными телефонами, но без договоров на оказание услуг связи, оформленных на своё имя. По имеющимся данным, доля таких пользователей составляет до 70% от числа используемых номеров. Впоследствии на этот номер могут оформляться банковские услуги. В результате получается, что информацией, необходимой для перевода денежных средств, может завладеть и воспользоваться другой человек.

Законопроект № 514780-7 призван помочь решить целый «букет» смежных острых проблем безопасности финансовых сервисов, связанных с недобросовестным использованием номеров мобильных телефонов. В первую очередь — повысить достоверность идентификация лиц, обращающихся за финансовыми услугами.

Решением стало создание Единой информационной системы проверки сведений об абоненте — физическом лице и о пользователях услугами связи абонента — юридическое лица, индивидуального предпринимателя и физического лица (далее — ЕИС), с помощью которой банки и дру-

гие финансовые организации смогут оперативно проверять, принадлежит ли номер мобильного телефона использующему его лицу.

## ОТ МЕЖДУСОБОЙЧИКОВ — К УНИВЕРСАЛЬНОСТИ

Коротко говоря, ЕИС будет представлять собой единый шлюз, с помощью которого банки и иные финансовые организации смогут в оперативном режиме подтверждать у любого оператора связи информацию о принадлежности номера телефона.

При этом данные о пользователе будут поступать от банков оператору ЕИС в зашифрованном виде. Система ответит на вопрос о соответствии фамилии, имени и отчества, а также серии и номера удостоверения личности тем данным, на которые оформлен номер телефона. Ответ на запрос будет односложным: «да» (соответствует) или «нет» (не соответствует). Поскольку обмен персональными данными в такой схеме отсутствует, то и согласие на обработку персональных данных в данной ситуации оператору ЕИС получать не потребуется.

В настоящее время только отдельные, наиболее крупные банки имеют договоры с некоторыми операторами мобильной связи, предусматривающие возможность подтверждения информации об абоненте. Однако очевидно, что этот процесс должен быть унифицирован и доступен любой финансовой организации. При этом объединять базы клиентских данных операторов связи никто, конечно же, не планирует.

Создание такой системы поможет в борьбе с мошенничествами, помешает злоумышленникам использовать номера чужих мобильных телефонов. Также ЕИС сократит число ошибочных звонков коллекторских агентств на номера, оставшиеся от прежних владельцев.



**ПРЕИМУЩЕСТВА  
«ЕДИНОГО ШЛЮЗА»**

Цель принятия законопроекта № 514780-7 — формирование правовой базы для создания и функционирования ЕИС. Законопроект о создании ЕИС был принят в первом чтении ещё в марте 2019 года. Редакция первого чтения законопроекта о создании этой системы устанавливала обязательность такой проверки, что могло создать серьёзные затруднения при оказании дистанционных услуг и проведении упрощённой идентификации на первом этапе формирования ЕИС.

Подготовленные поправки к законопроекту закрепляют возможность такой проверки как право, а не обязанность финансовых организаций. И только в дальнейшем при обеспечении необходимого уровня бесперебойности и нагрузочного тестирования ЕИС Банк России в отношении финансовых организаций, а Минюст России в отношении коллекторов получают право установить случаи обязательного проведения проверки номера, в том числе через ЕИС.

ЕИС должна представлять собой полноценную систему проверки пользователями сведений об абоненте в виде подтверждения или опровержения. Пользователями выступают различные участники отрасли, среди которых финансовые организации, операторы связи, Банк России, федеральные органы исполнительной власти.

**ОБЩИЙ ЗНАМЕНАТЕЛЬ «ЗА» И «ПРОТИВ»**

Процесс согласования поправок ко второму чтению оказался непростым. Разные участники финансового рынка приводят свои «за» и «против» предлагаемых законотворческих решений. По ряду мнений, введение обязательности использования ЕИС, предлагаемое Правительством России, пока преждевременно. Нужно дождаться наполнения баз операторов связи данными пользователей абонентов — физических лиц, включая паспортные, и выверки этих данных с использованием информации из МВД.

Если ввести обязательность использования ЕИС раньше, то это приведёт к многочисленным отказам в обслуживании пользователей услуг связи. То есть к массовым нарушениям прав потребителей и дискредитации всей системы антифрод-мероприятий, направленных на защиту законных прав граждан.

Против создания указанной системы выступают операторы связи и отдельные крупные банки, которым выгодно сохранить действующую систему, при которой сведения об абоненте передаются от операторов связи в банки на основании двусторонних договоров вне контура государственного надзора. В то же время даже из числа крупных банков



на практике такие договоры имеют не более 20 %, а среди средних и малых банков вообще практически никто. В качестве одного из основных препятствий для заключения таких договоров банки отмечают непомерно высокие тарифы на услуги проверки сведений об абонентах, выставляемые операторами связи.

Кроме того, по нашему мнению, тарифная политика операторов за последние годы — регулярные значительные повышения тарифов — требует обязательного государственного контроля в условиях создания и использования ЕИС. Её активное использование на возмездной основе предполагается всеми участниками финансового рынка, а это около 20 000 организаций.

При этом Законопроект предполагает установление не размера тарифа, а только максимально допустимого размера части платы, которая может выплачиваться операторам связи. По действующему законодательству это не является прямым тарифным регулированием. «Максимум» направлен на решение стратегической задачи. С одной стороны, дать возможность взаимодействовать с ЕИС всем финансовым организациям независимо от их величины и количества осуществляемых проверок. С другой — обеспечить покрытие эксплуатационных расходов оператора ЕИС.

\* \* \*

Целый ряд замечаний, которые необходимо учесть, возник как у Правительства РФ, так и у Банка России. Есть основания полагать, что все замечания удастся проработать, и Законопроект будет принят в весеннюю сессию 2020 года.





**Вадим УВАРОВ**  
директор Департамента  
информационной  
безопасности Банка России

# ВЕКТОРЫ РАЗВИТИЯ

## ОСНОВНЫЕ НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОТРАСЛИ В 2020 ГОДУ

**Н**а начало 2020 года уровень обеспечения информационной безопасности финансовых организаций отвечает имеющимся рискам. Разумеется, не всё идеально, но в целом ситуация в этой сфере на финансовом рынке находится под контролем. Благодаря совместной работе Банка России, самих поднадзорных и других организаций, в том числе международных. Цели дальнейшей работы определены по нескольким основным направлениям.

### КЛЮЧЕВЫЕ НАПРАВЛЕНИЯ

Есть два ключевых направления обеспечения информационной безопасности и киберустойчивости в отрасли, на которых концентрируются усилия:

- ♦ обеспечение информационной безопасности инновационных финансовых технологий;
- ♦ борьба с социальной инженерией.

Что касается первого направления, то Банк России прекрасно понимает: за ними будущее, а в некоторой степени уже и настоящее. Их внедрение способствует развитию конкуренции, а значит и повышению качества предоставляемых услуг и сервисов. Аспекты безопасности инновационных финансовых технологий прорабатываются глубоко и всесторонне, чтобы клиент был надёжно защищён и чувствовал это, поэтому специалисты Департамента информационной безопасности участвуют в этой работе начиная с самых ранних стадий создания той или иной технологии.

Эта многоплановая работа включает в себя развитие нормативного регулирования, изучение и внедрение лучшего международного опыта, а также межведомственное взаимодействие. В ходе этой работы важно соблюсти баланс: с одной стороны, оперативно обеспечить максимальный уровень информационной безопасности новых технологий, с другой — не закопать себя и поднадзорных в бюрократической рутине, избежать формализма.

Свежий пример положительного результата — ввод Банком России в эксплуатацию Системы быстрых платежей (СБП). На данный момент уровень информбезопасности этого сервиса весьма высок.

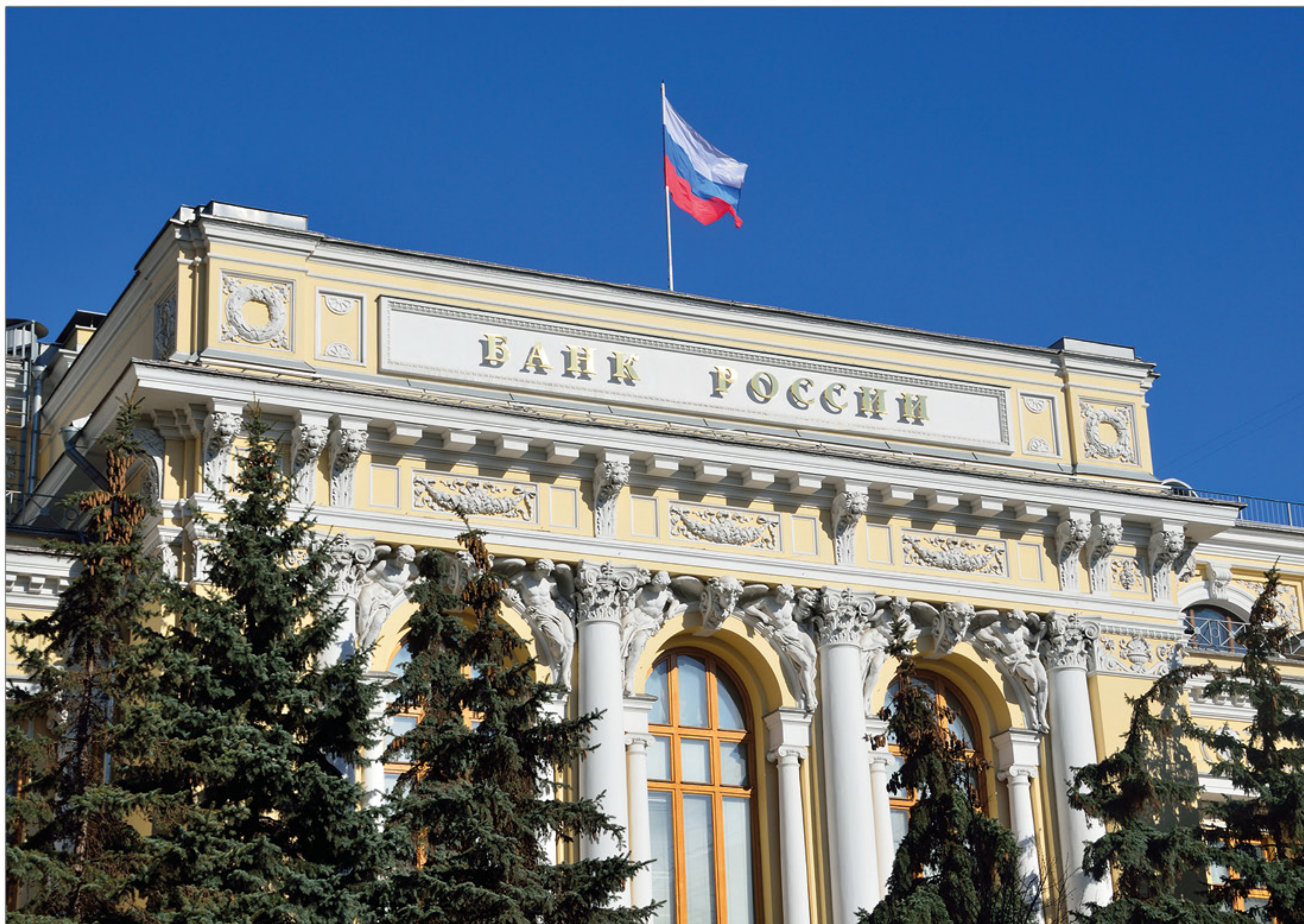
По второму направлению, социальной инженерии, важной мерой противодействия злоумышленникам является информирование граждан о существующих угрозах и методах противодействия. На данный момент основной целью для злоумышленников стали клиенты банков — главным образом физические лица. Мы уделяем много внимания их защите, например, обязали банки отслеживать несанкционированные операции, сформировали их признаки. Более того, мы доносим до граждан актуальную информацию о том, какие именно приёмы злоумышленников на данный момент актуальны, и что нужно делать, чтобы не стать их жертвой, не остаться без денег. Я считаю, что банки должны активнее вести работу по информированию своих клиентов о рисках мошенничества — это вопрос не только сохранности денег, но и репутации кредитных организаций.

### РАЗВИТИЕ НОРМАТИВНОГО РЕГУЛИРОВАНИЯ

Банк России внимательно изучает и использует опыт международных организаций — разработчиков нормативной базы информационной безопасности финансовой сферы. В первую очередь — Комитета по платёжным и рыночным инфраструктурам Банка международных расчётов. Лучшие наработки и рекомендации мы имплементируем в нашу нормативную базу, с учётом специфики российского финансового рынка.

В частности, речь идёт о двух основополагающих документах Банка международных расчётов — «Руководстве по киберустойчивости для финансовых рыночных инфраструктур» (Guidance on cyber resilience for financial market infrastructures) и «Стратегии безопасности крупнотомных платёжных систем» (Reducing the risk of wholesale payments fraud related to endpoint security). Ряд их положений мы





интегрировали в нормативы для системы управления рисками и обеспечения операционной надёжности в финансовых организациях.

Отдельные моменты будут реализованы в новой редакции Положения Банка России от 9 июня 2012 года № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».

Кроме того, мы достаточно внимательно следим за работой Международной организации стандартизации — ISO и Международного союза электросвязи — ITU в отношении технологий обеспечения информационной безопасности и киберустойчивости. Лучшие их наработки используются в нашей деятельности.

Важным направлением, которое прорабатывает Банк международных расчётов, — это киберучения. Мы считаем этот механизм оценки уровня защищённости достаточно эффективным, и будем его развивать на основе имеющихся и прогнозных данных о сценариях атак. Проведение киберучений мы заложили в стандарт по управлению рисками информационной безопасности и по их итогам будем в дальнейшем оценивать качество управления рисками.

Разумеется, сценарии киберучений будут доработаны с учётом особенностей, уровня и масштаба деятельности разных организаций. Наша цель — оценить эффективность реализуемых финансовыми организациями мер по противодействию компьютерным атакам, потенциальные потери. И на этой основе оценивать финансовую устойчивость как отдельных организаций, так и финансовых экосистем.

### **ВЗАИМОДЕЙСТВИЕ ВЕДОМСТВ**

Для повышения эффективности противодействия киберпреступности в финансовой сфере будет продолжаться развитие межведомственного взаимодействия. В федеральной программе «Цифровая экономика Российской Федерации» эта тематика для органов государственной исполнительной власти проработана достаточно хорошо и глубоко.

Одним из позитивных примеров является эффективное сотрудничество Банка России и ФСБ России в разработке функциональных технических требований к HSM-оборудованию, направленное на выполнение задачи импортозамещения СКЗИ.

Другой пример — работа над решением проблемы преступлений с помощью мобильной связи. Чтобы лишить злоумышленников существующих возможностей, есть организационно-технические решения. Во-первых, создание



единой информационной системы, которая открывает банкам доступ к информации о принадлежности сим-карт. Во-вторых — блокировка возможности «подмены» телефонных номеров.

Однако необходимо внесение изменений в федеральное законодательство, чтобы создать правовые основы для внедрения этого решения, а также привлечь к этой работе операторов мобильной связи. Такие варианты в настоящее время Банк России прорабатывает совместно с Минкомсвязи РФ и Государственной думой РФ.

Кроме того, в отрасли существует кадровая проблема: часто ощущается дефицит квалифицированных специалистов по информационной безопасности. Эта проблема вполне закономерна: наша отрасль молодая и быстрорастущая. Но, как известно, спрос рождает предложение, и Банк России старается содействовать скорейшему преодолению кадрового дефицита.

В федеральной программе «Цифровая экономика Российской Федерации» есть блок, посвящённый подготовке персонала. В него входят разработка профессионального и образовательного стандартов, программ профессиональной переподготовки и работа с вузами. Чтобы помочь удовлетворить кадровый голод, Банк России участвует в разработке профессионального стандарта, проходящего согласование в Министерстве труда и социальной защиты РФ.

### **«ВСЕОБУЧ» КИБЕРБЕЗОПАСНОСТИ**

Позиция Банка России однозначна: информированность и культуру граждан в сфере информационной безопасности повышать необходимо. Цели — повысить бдительность населения в отношении информационных угроз в финансовой сфере, предупреждать их об актуальных угрозах («телефонного мошенничества» и других), давать рекомендации по противодействию.

Такая работа уже ведётся Банком России во всех регионах страны, и в 2020 году будет продолжаться. В рамках выполнения ряда программ, начиная с федеральной программы «Цифровая экономика Российской Федерации», утверждённой Правительством России 28 июля 2017 года, и Национального проекта «Цифровая экономика Российской Федерации» на 2019–2024 годы.

Киберграмотность является одним из блоков, входящих в масштабный федеральный проект по повышению общей финансовой грамотности граждан. К этому проекту подключены многие государственные и частные структуры. Они должны участвовать в этом проекте в рамках своих полномочий и компетенций. Например, в конце прошлого года Банк России и МВД договорились объединить усилия по информированию граждан об опасностях социальной инженерии, так как борьба с противозаконной деятельностью является компетенцией МВД, а забота о стабильности финансовой системы и сохранении доверия к ней со стороны граждан — это зона ответственности Банка России.

Для этой работы мы привлекаем федеральные и региональные СМИ, социальные сети, публичные площадки — школы, библиотеки и другие.

### **АДРЕСНОЕ ИНФОРМИРОВАНИЕ**

Чтобы эта работа была максимально эффективной, информирование граждан должно быть адресным. Адресность достигается максимально точным описанием психологического портрета и ключевых точек уязвимости жертв. Совместно с представителями служб информационной безопасности банков, психологами и представителями структурных подразделений Банка России были проанализированы предоставленные кредитными организациями данные клиентов.

В результате выделили пять основных типов: домохозяйки, главы семей с высокой финансовой нагрузкой, пенсионеры, подростки и индивидуалисты-«миллениалы». На основе этих и других данных для каждой выявленной аудитории были сформулированы модели угроз, алгоритмы противодействия и обучающие материалы. Сотрудники ФинЦЕРТ используют разные форматы обучения этих сильно различающихся целевых аудиторий.

Среди примеров работы со старшим возрастом — лекции по финансовой безопасности и противодействию кибермошенничеству на площадке Центральной библиотеки им. Н.А. Некрасова в рамках столичной программы «Московское долголетие».

Для молодёжи — это открытые уроки по кибергигиене и лекции по киберграмотности для школьников, мероприятия по профориентации. Удаётся параллельно решать и смежные задачи профориентации, например, на базе образовательного фонда «Талант и успех». Недавно его участники разработали утилиту, позволяющую проводить экспресс-диагностику информационных систем банка на предмет вмешательства вредоносных программ. Подобного рода проекты мы будем развивать и далее для привлечения молодёжи к работе в организациях кредитно-финансового сектора, включая Банк России.

Должное внимание уделяется смежному вопросу — профессиональному обучению, подготовке для финансовой сферы специалистов по информационной безопасности и повышению их квалификации. Банк России заключил договоры с крупнейшими вузами о совместном повышении качества преподавания профильных дисциплин. Лучшие студенты проходят учебно-производственную практику в ФинЦЕРТ, и самые лучшие остаются здесь работать.

\* \* \*

Нормативные документы Банка России, касающиеся информационной безопасности, регулируют не технические аспекты установки и настроек средств защиты, а обеспечение сбалансированного уровня рисков. Уровень информационных рисков должен соответствовать возможностям конкретной организации, соотношению её капитала с потенциальным ущербом в случае реализации киберугроз.

Обеспечение информационной безопасности и киберустойчивости относятся к управлению операционными рисками, находящемуся в компетенции топ-менеджмента, иногда даже Советов директоров финансовых организаций. Поэтому руководство финансовых организаций, как правило, проявляет должное внимание к решению этих вопросов.





АССОЦИАЦИЯ  
БАНКОВ  
РОССИИ

# Ежегодная встреча кредитных организаций с руководством Банка России

Тема: «Регулирование Банком России  
деятельности коммерческих банков»



Целью ежегодно проводимых Ассоциацией банков России встреч с руководством Банка России является обсуждение текущих проблем, стоящих перед банковским сообществом, новых законодательных и нормативных документов.

Во встрече традиционно принимают участие Председатель Банка России, заместители Председателя Банка России, руководители департаментов и служб мегарегулятора.

Контакты оргкомитета:  
event@asros.ru  
т/факс +7(495)785-29-93  
+7(495)785-29-88

Информация  
о мероприятии



[www.asros.ru](http://www.asros.ru)

## 13 - 14 февраля 2020 года

Московская область, Домодедовский район, ОПК «Бор-Пансионат»





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

# ОПТИМАЛЬНЫЙ АУТСОРСИНГ ДЛЯ НЕБОЛЬШИХ И СРЕДНИХ БАНКОВ

О ЕДИНОЙ ПЛАТФОРМЕ НА БАЗЕ  
АССОЦИАЦИИ БАНКОВ РОССИИ

**П**роблема информационной безопасности небольших банков с каждым днём становится всё острее. Тем более, что ущерб грозит и другим игрокам рынка, взаимодействующими с ними. Эксперты уже неоднократно отмечали, что небольшие расходы на безопасность и высокая уязвимость маленьких банков — комплексная проблема, требующая решения уже сейчас. Аутсорсинг в этом контексте становится заметным трендом как для организаций, так и для поставщиков услуг.

Согласно исследованию Ассоциации банков России (АБР) за 2019 год, банки — лидеры цифровизации выделяют значительные бюджеты на работу с малым и средним бизнесом. Они активно трансформируют свои бизнес-модели: внедряют технологии больших данных и искусственного интеллекта, используют ИТ для обучения и нефинансовых услуг МСБ, смелее отдают на аутсорсинг решение отдельных задач.

Ассоциация уже продолжительное время ведёт активный диалог с Банком России относительно проекта по аутсорсингу для небольших и средних банков, в том числе услуг информационной безопасности. Вице-президент АБР Алексей Войлуков, модератор сессии «Аутсорсинг услуг информационной безопасности для средних и малых банков» XII Уральского форума, рассказал важные подробности проекта.

## СОЗДАТЬ ПРИЕМЛЕМОЕ РЕШЕНИЕ

Крупные банки и часть средних относительно легко справляются с реализацией требований Банка России к обеспечению информационной безопасности. У них значительно более широкое поле деятельности, им намного проще открыть дополнительный штат и найти квалифицированных профессионалов. Крупные банки могут выделять достаточные ресурсы, чтобы выполнять требования регулятора, поскольку заинтересованы обезопасить значительные ресурсы, включая предоставленные их клиентами.

Для небольших банков, где общий штат не более 30 сотрудников, нанять ещё 2–3 человек для обеспечения информационной безопасности — существенные дополнительные затраты. Независимо от используемой бизнес-модели. К тому же для этих новых штатных работников нет достаточного объёма работ для полной загрузки.

Поэтому небольшие и средние банки обратились с просьбой к Ассоциации помочь решить эту проблему. Либо просить Банк России диф-

ференцировать нормативы для банков разной величины, либо выработать приемлемый формат передачи банками некоторых функций на аутсорсинг.

Возможное решение — кооперация небольших банков, чтобы поручить выполнение некоторых задач внешнему исполнителю. Аутсорсинг является оптимальной бизнес-моделью, делающей приемлемыми затраты на обеспечение информационной безопасности для малых и средних банков.

## МОДЕЛИ ВНЕДРЕНИЯ АУТСОРСИНГА

Идя навстречу пожеланиям банков, Ассоциация разработала три модели внедрения аутсорсинга:

Первая модель: компания-аутсорсер обслуживает оборудование банков — «железо» и сервера, что позволяет снизить финансовые затраты.

Вторая модель — передача на аутсорсинг и сопровождения операционного дня, а не только «железа». Этот вариант централизует, оптимизирует и унифицирует работу аутсорсера с программным обеспечением банков-заказчи-





ков. С них снимается забота о выполнении требований регулятора в этой части.

Третья модель — единое облачное решение с разделением прав доступа. Оно позволяет значительно быстрее внедрять и распространять новые решения/ проекты всем банкам-пользователям, а тем самым — оптимизировать свой штат. Аутсорсинг откроет возможность для малых и средних банков внедрять новые сервисы на основе некоего открытого интерфейса. При этом даже небольшие банки смогут успешно конкурировать по уровню ИТ и информационной безопасности с крупными. Пока что у малых банков нет возможности самостоятельно внедрять новые бизнес-продукты. Для этого чаще всего они вынуждены подключаться к сервисам крупных банков.

Когда один из участников проекта реализует свою идею, её можно распространять на других, на партнёрской или коммерческой основе. Вопрос будет только в оформлении договоров и возможности комиссионной оплаты. Технически возможность подключения реализуется в считанные часы, учитывая работу всех участников на однотипном программном обеспечении.

### КАКОЙ ВАРИАНТ ОПТИМАЛЕН

Банк России рассматривает несколько вариантов определения порядка того, как банки могут передавать на аутсорсинг функции обеспечения информационной безопасности. Предложение АБР заключается в том, что на аутсорсинг банк сможет отдать сопровождение операционного дня, которое будут осуществлять штатные сотрудники не банка, а компании-аутсорсера.

Такое решение не только улучшит качество и оперативность, оптимизирует трудовые и финансовые затраты на ИТ и обеспечение информационной безопасности. Также появится возможность объединять усилия для создания современных решений, продуктов, конкурировать с крупнейшими участниками финансового рынка.

Банк России в целом одобрил наш проект, поставив ряд вопросов, которые сейчас обсуждаются, прорабатываются и решаются. Один из существенных — о том, кто наиболее оптимален в качестве аутсорсера. Есть вариант, что эту функцию возьмёт на себя крупный банк, но у других банков могут возникнуть серьёзные опасения, связанные с конкуренцией. Возможна реализация аутсорсинга ИБ банков и на базе Банка России, но сам регулятор такого решения пока не готовит, и даже более — не заинтересован делать это у себя.

Третий вариант — создание аутсорсинговой платформы на базе АБР. Оптимальный, по мнению и Банка России, и участников рынка. Ассоциация учреждена самими банками, является их доверенным лицом, основания для конфликта интересов отсутствуют. Такая платформа позволит банкам контролировать весь поток информации, совместно определять стоимость услуг и тарифы.

Решение отвечает нормативам Банка России, данные обрабатываются надёжной небанковской организацией, выводятся из-под рисков компрометации, утраты и недоступности, сопутствующих банкам. Регулятор может быть уверен, что выполняются все нормативные требования,



обслуживаемые банки в этой части оказываются более прозрачными и открытыми.

На встрече с представителями банков с базовой лицензией Председатель Банка России Эльвира Набиуллина подчеркнула: без такой консолидации небольшим банкам будет сложно выживать. Рынок должен сам себя создавать и эту функцию должна взять на себя Ассоциация. А регулятор может помочь людскими ресурсами и участием в разработке.

Облегчит решение задачи ожидаемое введение для банков с базовой лицензией пропорционального регулирования информационной безопасности. Регулятор заинтересован в том, чтобы такие банки развивались достаточно активно и обеспечили достижение намеченных показателей для кредитования малого и среднего бизнеса.

### РЕСУРСЫ ПРОЕКТА

Для разработки проекта в АБР создана специальная рабочая группа, в которую вошли малые и средние банки, а также крупные, способные предложить другим свои проекты, модули или сервисы. В составе группы работающие с банками вендоры и интеграторы — IT-, ИБ- и телекоммуникационные компании, операторы связи. Рабочая группа составила общую схему-описание концепции проекта, требований, задач и возможностей для заинтересованных сторон.

Следующий шаг — инвестиции в предложенное решение, добровольные для всех, включая членов АБР. Банки-участники готовы поддерживать проект разными способами: участвовать в финансировании, предоставить оборудование (сервера, ЦОДы и т.п.) и обслуживающий персонал — ИБ- и IT-специалистов.

Проект является перспективным, востребованным и окупаемым за относительно короткое время. Однако для запуска этого масштабного и долгосрочного начинания нужно довольно значительные стартовые финансовые ресурсы. Поэтому сейчас ведётся поиск якорного инвестора.

### ФОРУМ — МОМЕНТ ИСТИНЫ

На XII Уральском форуме «Информационная безопасность финансовой сферы» традиционно обсуждаются не только достижения, но и актуальные задачи, перспективы будущей работы. Как расставить приоритеты, пути решений и последовательные шаги, направленные на повышение безопасности цифровых финансовых сервисов. Поэтому по договорённости с руководством и Департаментом информационной безопасности Банка России было решено вынести вопросы реализации проекта на ближайший Уральский форум.

Участники форума получают достоверную и полную информацию о проекте и о том, что уже сделано для его реализации. Будут представлены мнения малых банков о важности, востребованности и широких перспективах нашей инициативы. Обсуждение позволит «сверить часы»: проверить насколько ожидания банков соответствуют возможностям технических исполнителей. Узнать у них, какие они видят проблемы на путях реализации предложенного решения аутсорсинга ИБ для банков, и какие оптимальные пути решения.

АБР предлагает создать не просто ещё одну организацию для аутсорсинга. Проект предполагает единое комплексное решение с использованием современных решений, в том числе созданных с нуля. Поэтому для его дальнейшей оптимизации крайне важны мнения разработчиков и ИБ-специалистов.

Ни для кого не секрет: многие малые и средние банки используют в обеспечении IT старые решения, в том числе чуть ли не двадцатилетней давности. Необходимость их модернизировать и настраивать каждый раз отнимает немало сил и драгоценное время. Закупка коробочных решений по операционным дням лишь частично решает эту проблему. Поскольку приходится держать большой штат программистов и опять же тратить время на то, чтобы адаптировать и настроить его применительно к особенностям бизнес-процессов. Подобных неудобств у банков-пользователей предлагаемой единой платформы аутсорсинга ИБ не должно возникнуть.

Единая платформа аутсорсинга разом бы решила для банков основную проблему, освободив их от немалых затрат на комплексное обновление технических средств. Предлагаемое решение полностью соответствует потребностям банков в сфере IT и ИБ: обеспечивать сохранность и конфиденциальность информации, надёжность работы IT-инфраструктуры, но при этом оптимизировать затраты.

\* \* \*

Обсуждение нашего проекта на Уральском форуме поможет предвидеть возможные сложности и заранее, ещё на стадии разработки, предупредить саму возможности их возникновения. И, что особенно важно, выработать максимально привлекательные для банков условия участия в нашем проекте. Особенно ценно вовлечение в проект новых партнёров, участников. Ценен любой вклад, от эффективной методологии до привлечения крупных инвестиций.



# МИР



Карта «Мир» создана российскими специалистами на базе собственных разработок с учетом передовых достижений в области индустрии платежных карт.

Карта соответствует строгим требованиям международных стандартов безопасности.

Будьте уверены — все ваши финансовые операции по карте, как и ваша личная информация, находятся под надежной защитой платежной системы «Мир».

[mironline.ru](https://mironline.ru)



# «ПЕРЕМЕН! — ТРЕБУЮТ НАШИ СЕРДЦА»

В ОТРАСЛИ НАЗРЕЛ ПЕРЕХОД К ОНТОЛОГИЧЕСКОЙ ХОЛИСТИЧЕСКОЙ ПАРАДИГМЕ ИБ



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

**Д**ля нынешнего этапа развития информационных систем, как корпоративных, так и государственных, характерно состояние осмысления: набралась «критическая масса» проектов информатизации с таким интегральным уровнем сложности, который требует радикальных мер для снижения этой сложности. По мнению Сергея Вихорева, слияние реального мира и мира ИТ уже произошло, и теперь законы, придуманные когда-то специально для виртуального мира ИТ, работают плохо. Сергей Викторович рассказал BIS Journal, почему пришла пора пересмотреть «нишевые» законы ИБ в сторону философских, общечеловеческих, взяв в качестве примера нынешний подход к созданию модели угроз — ключевого элемента, лежащего в основе требований ИБ к создаваемым ИТ-системам.

## СЛИШКОМ ВИРТУАЛЬНАЯ СУЩНОСТЬ

— Модель угроз изначально задумывалась как некоторое комплексное описание. В чём Вы видите ограниченность принятого подхода?

— Я бы говорил, скорее, не об ограниченности модели, а о её неадекватности сегодняшним практическим задачам. Давайте вспомним, что в своё время вообще не было никаких жёстких требований, и практически каждый опера-

тор (компания, которая работает с данными) вырабатывал свои требования самостоятельно, исходя из своего понимания угроз безопасности информации. Это был, образно говоря, «индпошив» моделей для каждого оператора. Потом пришла «промышленная» эпоха: появились определённые требования к конкретным классам защищённости, классификация информационных систем. Собственно, всё множество приказов ФСТЭК России. Но там везде в них декларируется: необходимость выбора требований на основе модели угроз. Вот только процедура выбора требований не включает моделирования угроз как конкретное действие. Модель оказывается этакой «бестелесной» сущностью, которая парит над требованиями, не касаясь их своими «крыльями». Вот пример из приказа ФСТЭК № 17 (Рисунок 1).

— Вы считаете это недостатком?

— Сама идея — использовать модель угроз при формировании требований абсолютно верная. Однако, не отрицая важности самого процесса оценки угроз безопасности информации при выборе адекватных мер защиты, необходимо отметить, что многолетняя практика моделирования угроз для каждого конкретного объекта показывает свою неэффективность. Потому что у оператора, как правило, нет специалистов, которые обладают достаточной компетенцией для правильного проведения анализа факторов, влияющих на реализацию угрозы. В связи с этим процесс моделирования зачастую носит формальный характер и не отражает реального положения дел, а разрабатываемые модели угроз мало способствуют оптимальному выбору необходимых средств защиты. Они просто не находят практического применения («документ ради документа»), так как критерии выбора средств защиты слабо увязаны с критериями оценки угроз. Производители средств защиты ориентируются не на угрозы безопасности информации, а на реализацию функций безопасности, оставляя выбор необходимых функций оператору. Но на уровне практической реализации возникает ситуация, которую я называю «парадокс свободы выбора».

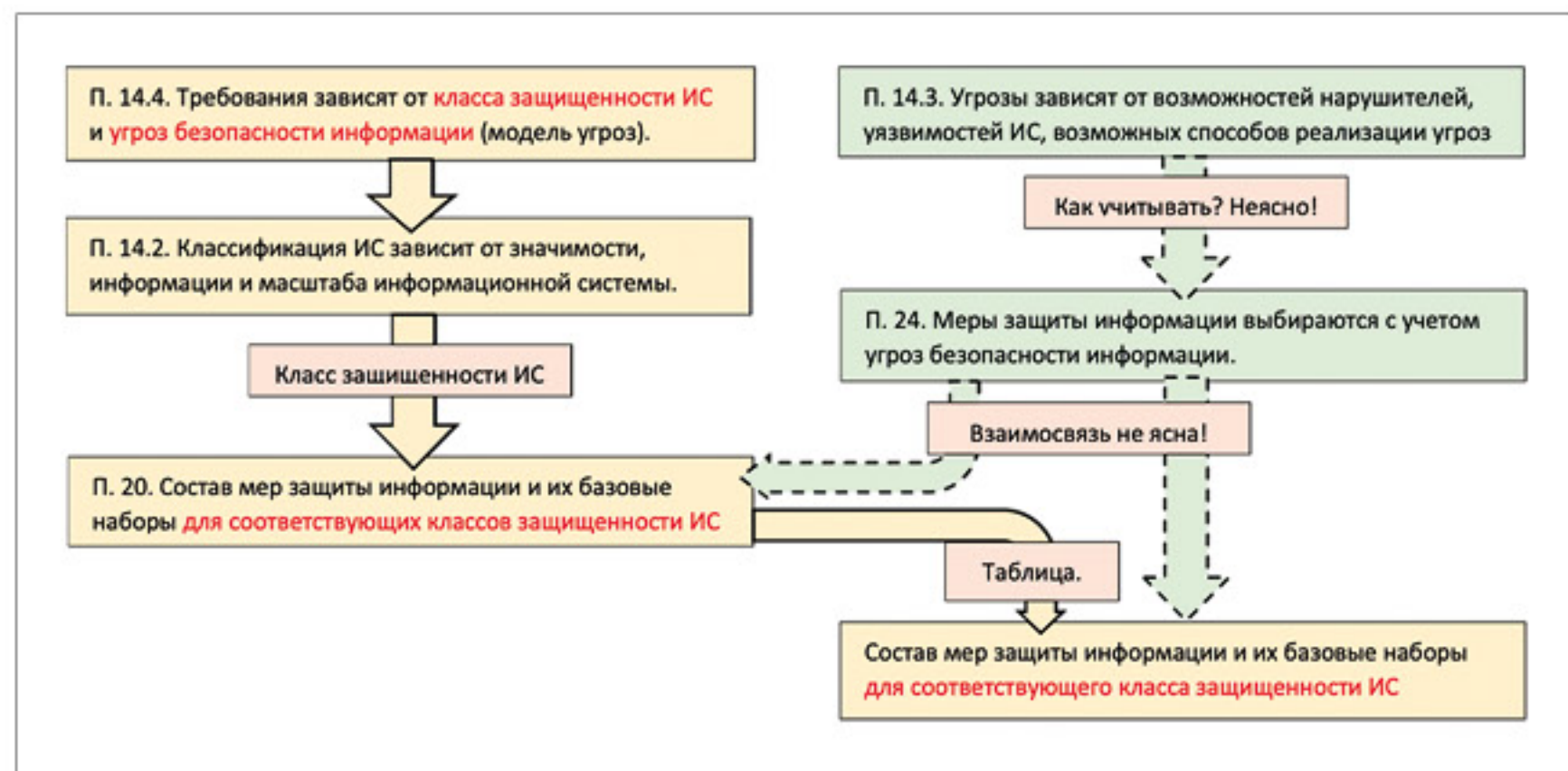


Рисунок 1. Пример из приказа ФСТЭК № 17



— В чём заключается парадокс?

— Давайте применим два философских метода: анализ и синтез. Когда я выбираю конкретные требования для определённой информационной системы, я строю модель угроз, а потом подбираю те меры защиты, которые, на мой взгляд, наилучшим образом подходят моей информационной системе. На этом этапе я провёл анализ ситуации, но затем наступает следующий, не менее важный этап — синтез, то есть конструирование системы безопасности. Для этого мне нужны инструменты, реализующие меры защиты, и за ними я обращаюсь на рынок. Но там я вижу некие универсальные средства, которые реализуют не только мои требования, но и многое другое. По факту получается, что создание системы защиты происходит буквально в форме философского закона единства и борьбы противоположностей.

— Все участники процесса, вроде, решают одну большую задачу?

— Да, в этом есть единство: все обеспечивают решение одной задачи — создание надёжно защищённой информационной системы. Но мои задачи как конструктора системы защиты и задачи вендора инструментов ИБ — диаметрально противоположны. Производители хотят максимально универсализировать задачу, снабдив продукт максимальным количеством всяческих функций. Это мы видим на рынке: появляются умные межсетевые экраны, которые уже включают не только функции фильтрации, но и DLP-систему, и систему обнаружения вторжений, и антивирусное ПО и многое другое. А у меня обратная задача — я хочу иметь конкретное средство, точно нацеленное на мои конкретные требования. Двух одинаковых информационных систем нет, каждая уникальна по-своему! Но и средств защиты, покрывающих мой уникальный набор требований защиты, тоже нет! Эту ситуацию я и назвал парадоксом свободы выбора: я должен либо построить неоптимальную систему, но которая будет соответствовать требованиям. Либо я должен построить оптимальную систему, которая не будет соответствовать требованиям.

— Стандарт общих критериев ГОСТ Р ИСО/МЭК 15408 имеет в виду, в конечном итоге, некий механизм выработки индивидуальных профилей защиты. Разве нет?

— Это так. И это правильное направление движения. Но обратите внимание, что этот стандарт предполагает свободу выбора профиля. Иными словами, декларируется в общем-то хорошая идея: пусть производитель создаст для своего продукта профиль защиты, в котором пропишет соответствующий функционал. Если

## *По факту получается, что создание системы защиты происходит буквально в форме философского закона единства и борьбы противоположностей*

все вендоры будут так поступать, у нас сформируется библиотека профилей защиты, и я как архитектор системы ИБ просто буду выбирать из этой библиотеки нужный профиль и функциональность. Идея близка к идеальной, и на практическом уровне эта идеальная модель не будет работать.

— Почему?

— Конечно, оператор не будет копаться в этой библиотеке профилей, у него также есть право создать свой уникальный профиль защиты для своей информационной системы. А потом он попросит вендора пройти сертификацию по этому профилю и придти с готовым решением. Так ведь? Но вендорам, конечно, такой путь не очень интересен: сколько клиентов — столько сертификаций, потому что профиль, который построит оператор, в большинстве случаев не совпадёт с профилем, который построит вендор. И ещё один вопрос: где во всей этой структуре модель угроз?

Она существует на уровне выработки требований. При этом процесс оценки угроз необходимо разделить по степени сложности между специалистами разного уровня квалификации. Оценку влияния угроз и выработку оптимальных методов их нейтрализации оставить наиболее квалифицированным кадрам, сосредоточенным в научно-исследовательских учреждениях, — это и будет типовой профиль защиты, а выбор конкретных мер защиты предоставить оператору, снабдив его необходимыми критериями сопоставления особенностей его информационной системы с существующими мерами защиты. Выбор необходимых мер защиты информации должен строиться по принципу «от общего к частному» из универсального набора профилей: по средствам обнаружения вторжений, по антивирусам и т.д. По сути, класс защищённости системы определяет выбор конкретного универсального профиля. Всё. Индивидуальности конкретной системы и оптимального выбора решения защиты не может быть, по определению.

Это означает, что нарушается один из базовых философских принципов построения больших систем — принцип онтологического холизма, который говорит о превосходстве общего



над частным. Мы же сейчас мыслим на уровне частного, а об общем мы вообще, по сути, пока и не задумываемся.

### **ПРИНЦИП ХОЛИЗМА И МОДЕЛЬ УГРОЗ**

— В поисках общего давайте обратимся к общей архитектуре современных ИТ-систем. Там мы видим некоторую логическую иерархию: платформа плюс дополнительные прикладные ИТ-решения. Есть целое, и отдельные частные решения, причём и целое, и частное — со своей отдельной сущностью и ценностью. Можно ли сказать, что модель угроз должна также иметь иерархическую архитектуру, скажем, более общая модель всей системы в целом и частные модели — для отдельных прикладных систем?

— Принцип холизма здесь ярко проявляется. Сейчас происходит именно так: например, для каждой системы, обрабатывающей персональные данные (а их у оператора может быть несколько), строится своя отдельная модель. А теперь давайте посмотрим на архитектуру ЦОД: на одной инфраструктуре сидит несколько различных информационных систем. Причем, каждая использует одно и то же серверное оборудование, одни и те же коммутаторы и средства сегментирования. Работаем с частным, не видим общего!

Способы сегментирования сети стремительно развиваются: сначала использовались мосты, потом маршрутизаторы (коммутаторы третьего уровня), дальше на смену подходу, основанному на физическом ограничении сетей и применении маршрутизаторов для организации связи между сегментами, пришла технология построения виртуальных сетей VLAN. Более того, виртуальные конструкции типа контейнеров вообще являются чисто логическими объектами, физически относящимися к одному и тому же оборудованию. Имеет ли смысл создать различные модели угроз, относящиеся к различным ИС, если, по сути, все они — лишь виртуальные семантические сущности?

А если они такие, то зачем мы будем строить для каждой этой сущности свою отдельную модель? Нужно минимизировать порождение моделей.

— Но для этого, прежде всего, нужно понять, где в нынешней ИТ-инфраструктуре у нас целое, а где — частное. Что здесь целое, а что частное?

— На одном гипервизоре может быть развёрнуто N-ое количество информационных систем. Что тогда мы должны защищать? В каждом конкретном случае — гипервизор, но по-своему? Абсурд. Получается, что надо защитить инфра-

структуру, на которой развёрнут этот гипервизор, это в философском смысле целое. Кстати, это направление прослеживается в некотором смысле в новой редакции приказа ФСТЭК России № 17 от 11 февраля 2013 г. В частности, применительно к инфраструктуре ЦОД, в котором размещается ГИС, указывается, что класс защищённости ЦОД должен быть не ниже класса, требуемого для ГИС. И этот посыл очень правильный, я считаю.

Ведь если у меня, например, ЦОД соответствует требованиям класса К2, то и все системы, которые я могу в нём разместить, будут также соответствовать К2. Тогда зачем для каждой такой системы делать свою модель? Модель нужно создавать не для информационной системы, а для инфраструктуры ЦОД, включая гипервизор, то есть для общего, в философском смысле. Поскольку общее превалирует над частным, и частное наследует свойства целого, то модель угроз, созданная для всей инфраструктуры ЦОД, будет распространяться на любые информационные системы, размещённые в этом ЦОД.

### **ИТ-ИНФРАСТРУКТУРА КАК КЛЮЧЕВОЙ ЭЛЕМЕНТ МОДЕЛИ ЗАЩИЩЁННОСТИ**

— Получается, что нужно переходить к модели защищённости ЦОД?

— Инфраструктуры. Не важно, ЦОД ли это или что-то другое. Информационные технологии охватывают все ресурсы, необходимые для управления информацией, особенно компьютеры, программное обеспечение и сети, необходимые для создания, хранения, управления, передачи и поиска информации. На современном этапе развития информационных технологий нужно говорить о модели угроз инфраструктуры, на которой, в свою очередь, может размещаться N-ое количество информационных систем. И она не будет зависеть от специфики тех информационных систем, которые развёрнуты на инфраструктуре.

Если у нас будет защищена инфраструктура, мне совершенно неважно, какую информационную систему на ней разворачивать, если её класс защищённости позволяет это сделать. В этом случае получается, что модель угроз мы строим применительно именно к инфраструктуре. А требования будут предъявляться к информационным системам. Вот и все.

— Звучит парадоксально. Получается, что именно ИТ-ландшафт — это ключевой элемент системы защиты современных ИТ-систем?

— Да, похоже, что ИТ-ландшафт является тем самым ключевым элементом, на котором необходимо строить модель угроз. ИТ-инфраструк-



тура — это общее по отношению к конкретным ИТ-системам. И это ярко проявилось именно в последнее время.

Раньше мы говорили о сегментировании сети. Принцип сегментирования: разделяй и властвуй, — это, действительно, один из важнейших принципов защиты информации. И мы добивались разграничения доступа к информации именно с помощью выделения сегментов, и эти сегменты были физическими: отдельные серверы, отдельные базы данных и проч. А теперь у нас совсем другая конструкция: есть некоторая платформа, и на этой платформе работает, например, ERP-система или СУБД. Вообще-то произошла некоторая революция: мы, скажем так, разсегментировали сеть и начали оперировать некоторыми семантическими сущностями. Что теперь мы должны защищать?

— СУБД?

— Зачем защищать саму по себе СУБД? Мы защищаем информацию! Если в компьютере нет никакой информации, то сам по себе он имеет некоторую материальную ценность, но не более того.

### **«ИДЕАЛЬНАЯ» ИНФОРМАЦИЯ С ПОЗИЦИЙ ЗАЩИТЫ**

— Конечно, виртуальная информация имеет материальную составляющую. Например, она нагружена содержанием, смыслом, то есть имеет семантическую ценность. Она виртуальная, но мы можем ощутить ее ценность — она выражается, например, в конкретном количестве денежных знаков. Нужно определиться с философскими понятиями идеально-го и материального и решить, что мы защищаем: материальную ценность информации или идеальное понятие информации?

— Природа информации загадочна. Норберт Винер, отец мировой кибернетики, говорил так: «Информация — это не энергия и не материя, информация — это информация». Информация — это, действительно, уникальный предмет, который одновременно содержит в себе и идеальное и материальное начало. Этаким дуализм. С точки зрения двойственной материальной и идеальной природы информации, я бы сказал так: в философском смысле она идеальна, но проявляет свои свойства, циркулируя в определённой среде. Вот почему мы должны защищать именно ту материальную среду, в которой проявляет себя — циркулирует — информация.

### **О ТОМ, КОГДА ИС ЗАЩИЩАТЬ НЕ НУЖНО**

— Есть идеи, как к этому подойти?

— Идея так называемой доверенной среды.

— Поясните, пожалуйста, на примере. Например, я владелец бизнеса. Арендую в ЦОДе пару виртуальных серверов и размещаю там несколько своих ИТ-систем. Вы отвечаете в компании за ИБ. Как Вы будете строить систему защиты?

— Прежде всего, надо уяснить, что система защиты не может быть построена для одной отдельно взятой прикладной системы, а только для ИТ-инфраструктуры. Я начинаю строить свой контур, который отгораживает мою информационную систему от других информационных систем, развёрнутых на этом же железе. Фактически строю некий виртуальный или физический сегмент. Я ведь могу на одном сервере разместить несколько различных информационных систем, и они все будут отделены друг от друга на уровне гипервизора. Именно гипервизор знает и контролирует, что одни виртуальные машины принадлежат мне, а другие — другим арендаторам инфраструктуры того же ЦОД. Но это все виртуальные машины! И мне, по сути, достаточно знать, что гипервизор, который соответствует определённым требованиям и определённому классу защищённости, позволяет выделить эти виртуальные машины в мой отдельный сегмент.

— Как такой подход меняет весь механизм решения задачи обеспечения защищённости?

— Думаю, на уровень конкретных регламентов сейчас уходить не стоит. Это отдельная и довольно большая тема. Скажу только, что всё будет проще.

— За счёт чего?

— Меняется парадигма защиты в целом. Сегодня защита строится, в основном, по принципу периметра: мы выделяем некий периметр и пытаемся его защитить. С течением времени по ходу развития ИТ, как мы знаем, это становится делать всё сложнее, проблем появляется больше, чем удачных решений.

Информационные технологии призваны рационально использовать современные достижения и практический опыт для решения задачи эффективной организации информационного процесса. Когда мы переходим к современным

*Мы защищаем информацию!  
Если в компьютере нет никакой информации, то сам по себе он имеет некоторую материальную ценность, но не более того*



технологиям, у нас появляется некий центральный сегмент (ЦОД), в котором обрабатывается информация определённой категории. А также огромное количество удалённых рабочих мест, которые связываются с этим ЦОД и, как правило, находятся в агрессивной среде. Мы не знаем, что именно находится на том конце телекоммуникационной системы. И здесь возникает парадигма доверенной среды.

Первое, что мы должны обеспечить, это защита ЦОД. Затем — защита канала. А ещё мы должны контролировать, чтобы на конкретном рабочем месте не произошло никаких изменений без нашего ведома. Чтобы было установлено только то программное обеспечение, которое должно быть, чтобы оно вовремя об-

новлялось и всегда оставалось в полном порядке. Образно говоря, нужные порты открыты, ненужные закрыты. Всё это мы должны контролировать.

Фактически создаётся некий «коридор», который идёт от отдельного рабочего места, и мы создаём защищённую оболочку не где-нибудь, а непосредственно на рабочем месте. Плюс оболочка канала связи. Плюс центр, где идёт обработка информации. Парадигма изменилась, и мы можем обойтись вообще без контура защищённости. Кстати, на рынке уже появляются устройства, которые позволяют создавать информационные системы в этой парадигме, и бизнес-приложения смогут спокойно работать в агрессивной среде.



**Юрий ЯЗОВ**  
профессор  
кафедры «Системы  
информационной  
безопасности»  
Воронежского  
государственного  
технического  
университета, доктор  
технических наук

# ВЕРШИНА АЙСБЕРГА ВО ТЬМЕ

БАЗОВЫЕ МОДЕЛИ, ПРОФИЛИ ЗАЩИТЫ,  
ДОВЕРЕННЫЕ СРЕДЫ... СПИСОК  
ДИСКУССИОННЫХ ТЕМ В ИБ БЕСКОНЕЧЕН

**Ш**ирокое внедрение в практику новых ИТ-технологий действительно существенно меняет представление о путях обеспечения безопасности в информационных системах разного уровня. Для каждой такой системы будет своя модель угроз, если речь идёт о состоятельной модели, в которой должным образом описаны для каждой угрозы её источник, уязвимость, способ реализации и возможные последствия. Такое описание сегодня (и в этом автор прав!) весьма громоздко и может быть составлено лишь знающими специалистами. Но эта сложная работа может быть облегчена, если создать для разных классов ИС «базовые модели угроз». К сожалению, пока состав таких описательных моделей невелик, но это не означает ущербность данного подхода. Конечно, базовые модели должны разрабатываться и для ИС, реализующих новые информационные технологии, и для обеспечивающих элементов информационной инфраструктуры.

Утверждение же о том, что сегодня модель угроз «оказывается этаким «бестелесной» сущ-

ностью, которая парит над требованиями — нелепо. Подчеркну: требования безопасности определяются в ходе многошаговой процедуры, позволяющей определить меры защиты информации, обеспечивающие блокирование всех актуальных угроз, включённых в модель. Без модели угроз правильно выбрать адекватные меры защиты не удастся. Другой важный методологический вопрос, который скрыто содержится в утверждении автора, состоит в том, каким образом можно определить, какие меры парируют ту или иную угрозу и насколько. Пока это делается эмпирически и весьма примитивно: организационные меры априори полагаются всегда эффективными, а технические меры должны реализовываться только сертифицированными средствами защиты, и тогда они будут эффективны. Но никакой оценки эффективности, тем более количественной, не проводится. На мой взгляд, нужно переходить к количественным методам обоснования требований по защите информации, к количественным методам оценки эффективности такой защиты, а, следовательно, и к количественным



— Завершая разговор, скажите, на чём, на Ваш взгляд, сегодня нужно сфокусировать внимание?

— Сейчас нужно пересмотреть традиционные подходы к защите информации через призму более общих философских законов. Мир един, и нужно учиться применять к проблемам защиты информации философские законы общечеловеческого плана. Один из ярких тому примеров — модель угроз. Мы видим, что если правильно применить общие философские законы, становится очевидным: нам не нужно строить 10 или 50 моделей угроз. Нам нужна одна модель угроз — для инфраструктуры. А это означает экономию времени и средств для обеспечения защиты информации.

— За счёт того, что такая модель упрощает ситуацию?

— Да. Меняется всё окружение, и срабатывает принцип диалектического единства: модель — проще, реализация защищённости — проще. Ведь информационная система, которая находится на этой инфраструктуре, уже полностью соответствует требованиям всей этой инфраструктуры. Она изначально защищена инфраструктурно. В этом и есть философская составляющая рассматриваемой проблемы. С одной стороны — онтологический холизм, то есть верховенство целостности перед отдельными элементами. С другой стороны, закон единства и борьбы противоположностей. С третьей стороны, метод дедукции — от общего к частному.

Беседовала  
Елена Покатаева

методам оценки возможности реализации и опасности угроз.

Важнейшим вопросом, поднятым автором, является вопрос создания систем защиты информации. Я согласен с мнением, что идея создания наборов профилей защиты на практическом уровне не работает! И это вполне объяснимо, так как систем в стране уже сотни тысяч, а если создавать под них совокупности профилей защиты (под каждый класс или уровень защищённости!), то это растянется на десятилетия, при этом сами профили быстро устареют из-за внедрения новых информационных технологий. Выход из создавшегося положения, на мой взгляд, можно найти в создании так называемых многоагентных (или мультиагентных) систем защиты, которые представляют собой совокупность перенастраиваемых в динамике функционирования ИС программных агентов, реализующих одну или ограниченную совокупность функций безопасности. Но для развития этого направления нужны ещё достаточно обширные и глубокие исследования.

Что касается принципа холизма и его применения при построении моделей угроз, то в вопросе модератора уже содержится ответ. Если ИС является сложной, то есть содержит в своём составе несколько составляющих (назову их парциальными системами) и в ней есть серверы, коммуникационные элементы, базы данных, не входящие в парциальные ИС, но эксплуатируемые ими, то необходимо составлять модель угроз для ИС в целом. И эта модель должна иметь составные части — модели угроз для парциальных систем, так как в них могут быть задействованы разные программные продукты,

могут внедряться разные вредоносные программы, будут эксплуатироваться разные уязвимости, могут применяться разные способы реализации угроз, хоть это и «виртуальные сущности». Всё это справедливо и для ЦОД как надсистемы, включающей в себя совокупность парциальных систем. Защита информационной инфраструктуры — это и защита информации в ИС, это и защита самих ИС от угроз нарушения их функционирования. Предложение о защите инфраструктуры побуждено попыткой сократить количество моделей угроз. Это стремление понятно, но, на мой взгляд, решение вопроса сокращения количества моделей угроз нужно решать не таким образом, а, например, путём типизации информационных систем.

Наконец, весьма важный аспект совершенствования защиты информации — это создание доверенных сред. Я в этом отношении солидарен с автором. К этому, несомненно, нужно стремиться. Единственное, что хотелось бы отметить, что создание доверенной среды даже в одной ИС — это весьма сложная задача, а если тот же ЦОД, эксплуатируемый разными ИС, — «чужой», то уверенность в доверенности среды быстро улетучивается. Пока, к сожалению, способы формирования действительно доверенных сред — это будущее.

\* \* \*

Я затронул лишь несколько важных, на мой взгляд, вопросов. Однако это лишь «вершина айсберга», так как проблематика защиты информации весьма обширна и в ней очень много и других проблемных вопросов, которые невозможно осветить в одной дискуссии.



# СМЕНА ПАРАДИГМЫ ЗАЩИТЫ ИТ-СИСТЕМ

БЛАГИЕ ПОЖЕЛАНИЯ И СУРОВАЯ РЕАЛЬНОСТЬ



**Андрей КУРИЛО**  
глава компании  
«Реальная  
безопасность»

**А**бсолютно согласен с С.В. Вихоревым — накопились серьёзные проблемы, решать их необходимо.

## О НАЗРЕВШЕЙ СМЕНЕ ПАРАДИГМЫ ЗАЩИТЫ

Действительно, сложность ИТ-систем, как в части создания, так и в части администрирования, постоянно растёт и уже очевидна настоятельная необходимость принимать меры для упрощения этой работы. Настораживает то, что несмотря на попытки регулирования путем воздействия на среду регулирования через стандартизацию и нормативно-методические документы, продукты информатизации и безопасности и состоящие из них информационные системы упорно продолжают развиваться стохастически. Согласованных концепций и планов развития нет, что ведет к еще большей дезинтеграции среды.

Разработчики систем безопасности как открыли этот «ящик Пандоры» лет пятнадцать назад, так и идут путем создания всё более сложных продуктов. А в целом, в следствие реализации упомянутого подхода, эффективность систем не только не растёт, а вообще становится неочевидной, так как растёт сложность сопровождения продуктов, и как следствие, реальная эффективность работы систем защиты (в итоге — уровень защищенности объектов) начинает падать.

Давайте посмотрим внимательнее на тот путь, по которому страна активно движется в направлении цифровой экономики. В теории всё выглядит красиво, а на практике? Электронные сервисы работают неустойчиво, причём даже в тех ведомствах, которые считаются лидерами цифровизации. Количество отказов электронных систем с течением времени только увеличивается, причём даже у самых крупных организаций, в том числе, у банков. Одна из причин — высокая сложность создаваемых систем. При этом пользователь, как человек далёкий от информатизации, опасается взаимодействий с этими системами, а их разработчики и администраторы — не всегда справляются с задачами по причине их высокой сложности. Сложилась парадоксальная ситуация. Наш мир сегодня состоит из двух частей: реального мира и его отражения в информационном мире. Однако

надёжность действий в реальном мире сегодня гораздо более высокая, нежели отражение этих же действий в цифровом мире. А поскольку мир един, то надёжность жизни в этом симбиозе определяется самым слабым звеном.

Получается, что с помощью информатизации мы, на самом деле, не улучшаем свою жизнь, а ухудшаем её. Иными словами, мы деградируем. Парадоксально? Да. Но объяснимо. Достаточно поискать ответ на вопрос: а как системы создаются, как управляются и контролируются. В условиях материального производства в процессе создания новой продукции участвует огромное количество профессионалов: от проектного бюро до ОТК и военного контроля, если речь идёт о продукции соответствующего назначения. В результате на свет появляется изделие, которое имеет конкретные заданные характеристики и свойства надёжности. А в цифровом мире практически все сложнее и опаснее, тому пример с цифровым самолетом Боинг 737 MAX, производство которого, после ряда авиакатастроф, в конце концов прекратили. И никакой выходной контроль и куча стандартов разработки и безопасности не спасли.

Яркий пример в области ИБ: при наличии и повсеместном использовании систем защиты от НСД, DLP, антивирусов, МСЭ разного уровня, систем контроля действий пользователей, обнаружения активности, SOC и SIEM в их составе, проведения разных PEN-тестов, аудитов по специальным стандартам мы пришли к тому, что практически все БД уже украдены или докрадываются сейчас, и наша страна далеко не единственная, где это происходит. Это при том, что регуляторы выпускают все больше хороших нормативных документов и требований. Их уже настолько много, что выполнить их — отдельная и сложная задача. Часто это некому делать, специалистов сокращают. Я уже не говорю о проблеме, возникшей с неправомерным сбором и использованием биометрических данных и анализом простых фото, которые радостные пользователи выкладывают в виде частных архивов в публичные облака уважаемых компаний с мировым именем. Дело уже дошло до того, что Генеральный секретарь ООН Антониу Гутерриш, характеризуя состояние современного общества, очень



выразительно назвал «темную сторону цифрового мира одним из четырех всадников апокалипсиса», наряду с высочайшей геостратегической напряженностью, климатическим кризисом и растущим глобальным недоверием к политическим учреждениям и глобализации.

Однако представляется, что в стратегическом плане, угрозы исходящие от темной стороны цифрового мира, являются главными.

А теперь давайте порассуждаем. Наша цель — парирование известных угроз и своевременное противодействие будущим угрозам. При этом, угрозы будущего видятся нам как все более масштабные и глобальные. Таким образом и наши действия должны носить все более системный и масштабный характер. И главное — они должны быть эффективными.

В целом, методически правильный подход к работе над любой сложной системой, не только технической, но и, например, социальной, подразумевает, что вначале задаются цели (что мы хотим от системы или чего мы хотим достичь с ее помощью), затем определяются параметры системы и по ним устанавливаются требования к ней (уточняется, какие характеристики должна иметь система, чтобы соответствовать нашим целям), потом система создаётся, а затем идет анализ и контроль эффективности ее работы, заключающийся в контроле соответствия показателей (индикаторов) ее состояния заданным характеристикам. Контроль состояния системы является ключевой задачей. Не следует думать, что это эксклюзивная история, свойственная сфере ИБ. Отнюдь. Такая задача возникает и всегда возникала при управлении любой сложной системой. Чего же не хватает? А не хватает четкой идентификации угроз, эффективного управления работой по созданию высокоэффективных систем безопасности и жесткого контроля за качеством работы и реализацией требований к системе.

Фактически речь о необходимости корректировки парадигмы защиты ИТ-систем. Как правильно подойти к выбору модели этой корректировки?

### О ПОПЫТКАХ НАОЩУПЬ НАЙТИ ПРАВИЛЬНЫЙ ПУТЬ

В свою очередь, парадигмы обработки данных корректируются достаточно часто. Очевидно, что требования по безопасности к клиентским рабочим местам в условиях перехода к облачной обработке данных существенным образом снижаются и типизируются, а вся тяжесть проблем безопасности переносится на инфраструктуру ЦОД. Это логичная схема совершенствования парадигмы обработки информации. Но ей должны соответствовать новые модели защиты систем.

Они постепенно появляются. Но их развитие идёт с явными перекосами. Здесь два крупных фактора. Первый — бизнес. Он довлеет и сосредоточен исключительно на извлечении прибыли. Второй — государство. Государственные регуляторы честно исполняют то, что им поручено, — защищают интересы государства. Однако те требования, которые они выставляют, зачастую оказываются слишком серьёзными, чересчур жёсткими для коммерческого сектора или общества. В итоге иногда возникает странный компромисс. Пример: ЕПГУ-ЕСИА: можно авторизоваться, как с помощью электронной подписи, так и с помощью пары логин/пароль. По факту в правовом поле уравнивается электронная подпись — вещь очень сильная, особенно квалифицированная подпись — и обычное сочетание логина и пароля. Это правильно? Получается, что использование ЭП или УКЭП избыточное требование? Никто не знает ответа... Но инцидентов и проблем с авторизацией на ЕПГУ не видно. Приведённый пример — показательный: если мы начинаем закручивать гайки в плане формирования моделей угроз, а, значит, ужесточения требований, то эти требования становятся сложно выполнимыми обществом восприняты не будут. Готового рецепта нет, в этом С. В. Вихорев прав. Но необходимо не просто «взять и скорректировать», а проанализировать происходящее.

### НАПРАВЛЕНИЕ ОСМЫСЛЕНИЯ

Начальная точка осмысления происходящего — модель нарушителя. Вначале мы должны хорошо понять, кто нам противостоит, какими инструментами он обладает, как и с какой скоростью совершенствуется. Эта модель нарушителя должна быть адекватной каждой предметной области: одна — для происходящего внутри облака, другая — для процессов внутри платёжной системы и третья — для задачи промышленной безопасности в сфере управления умными станками. Поняв нарушителя, мы можем дать описание угроз, которые исходят от потенциального нарушителя. Однако обратите внимание: сейчас у нас в типовых рекомендациях эта модель угроз связывается с типовыми уязвимостями, которые фиксирует ФСТЭК. Но модель угроз и набор уязвимостей — это совсем разные вещи! Уязвимость — это потенциальная «дырка», через которую может что-то реализоваться только в том случае, если угроза и уязвимость совпадут.

А если они не совпадут ни во времени, ни в пространстве, тогда угроза не реализуется. Нужно чётко понимать разницу. И вот когда есть модель нарушителя и модель угроз, тогда возникает новая задача, думаю, она ключевая. Это создание нового документа: **профиля защиты объекта (системы).**



Не нужно путать с профилем защиты продукта информатизации, который описан ГОСТ 15408. Он изначально целенаправленно формируется для того, чтобы продукт (изделие) прошел сертификацию. Но система и продукт сугубо разные вещи. Думаю, что именно профиль защиты является ключевым элементом во всей этой системе, а не модель угроз, она необходима, но вторична. Потому что именно профиль защиты объекта адекватно учитывает, с одной стороны, модели угроз и модели нарушителя, атакующего объект, а с другой стороны — уязвимости объекта и компонент, из которых он состоит. И только после этого возникают требования по безопасности (в терминах ГОСТ 14508) верхнего уровня, которые определяют профиль, архитектуру, подходы, оценки уровня безопасности — практически все характеристики, которые мы обычно задаём. Но наша методология такого документа не предусматривает. Понятно, что состояние «как есть» и «как должно быть», — это две совершенно разные вещи. Только тогда, когда мы описываем профиль защиты системы, мы начинаем понимать, что нужно сделать. А далее логично возникает техническое задание на систему, адекватное перечисленным угрозам, уязвимостям и требованиям к безопасности. После реализации системы возникает вопрос приёмки, в ходе которой необходимо убедиться в том, что система работает и отвечает всем требованиям технического задания. Иными словами, мы должны быть уверены в том, что каждое требование к безопасности в системе выполнено, и мы это должны реально увидеть.

Конечная точка — эффективно управление, включая контроль выполнения требований по безопасности с опорой на экономические механизмы влияния на владельцев в случае неудовлетворительной работы. Самый эффективный механизм контроля и принуждения, созданный сейчас государством для защиты своих финансовых интересов — налоговый контроль. Хуже, но работают и другие механизмы, например, лицензирование, обеспечения правопорядка, безопасности дорожного движения. В их основе лежат не только меры административного принуждения и уголовного преследования, но и меры принуждения к выполнению требований государства через экономическое воздействие. Такую модель нужно реализовывать и в сфере информационной безопасности. Этим путем медленно, но движется ЦБ РФ.

**Государство, защищая свои интересы, должно эффективнее использовать меры принуждения к реализации установленных им требований.**

Вот такой я вижу новую конструкцию. Вопрос её практического воплощения — комплексный,

но предварительно он должен быть осмыслен и достаточно глубоко.

## ПРОБЛЕМА АНАЛИЗА

Речь идёт о корректировке парадигмы защиты, а значит, начальный этап — создание модели нарушителя — требует глубоких исследовательских поисковых работ. Нам нужно несколько заглянуть вперёд: что нас ожидает в перспективе? Кто способен выполнить такую задачу? Известно, что США прогнозирует будущее на 15 лет вперёд. Корпорация IBM пытается заглянуть в будущее примерно на 40 лет. А кто в нашей стране способен сделать такое?

Академия наук? Её роли в таком стратегическом качестве не видно. Банально, нет денег. Государевы служащие в отраслевых НИИ? У них другие цели, и решают они другие задачи, тоже важные для государства. Но там тоже нет денег на такие работы.

Есть отдельные эксперты высокого уровня — они как горсть бриллиантов рассыпаны по коммерческим компаниям. Кстати, в самих этих компаниях идёт большое количество НИР по направлению информационной безопасности. Но все они имеют сугубо прикладной характер и направления исследования диктуют интересы бизнеса, которому абсолютно всё равно, как будут защищены интересы граждан через 15 лет. А нынешние госконтракты — притча во языцех — своим принципиальным стремлением к самой низкой цене и безудержному демпингу вообще убивают всякие попытки предложить что-то наукоемкое, рассчитанное на завтрашний день.

Единственный выход — должны быть созданы некоторые «фабрики мысли», которые проводят серьёзные исследования, нацеленные на перспективу. Это государственная задача с госфинансированием. Её нельзя рассматривать как очередной грант, а только как государственную функцию национальной безопасности. И под этот функционал нужно собирать, возможно, во временные научно-исследовательские коллективы по крупицам лучших экспертов и лучшие коллективы страны. Иначе та деградация, на которую мы указали в самом начале, будет развиваться. А мы её так и не разглядим за ворохом мелких текущих задач. Нужно перестать тратить интеллектуальную энергию мелочёвку, поднять глаза вверх и увидеть за этим перелеском настоящий лес.

\* \* \*

А что касается модели угроз, то это частная задача. Она, конечно, должна решаться. Но её решение очень сильно зависит от того, какую парадигму развития систем защиты мы выберем. Вот об этом пора задуматься.



# СЛАБОЕ ЗВЕНО

## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ НА СТЫКЕ ТЕЛЕКОМА И ФИНАНСОВОГО СЕКТОРА

**К**огда употребляют словосочетание «отраслевая информационная безопасность», часто думают, что ИБ в разных отраслях — это совершенно разные сферы, регулируемые разными нормативно-правовыми актами, для этих сфер актуальны и характерны разные угрозы и атаки. До недавнего времени так и было. Однако в современном мире наблюдается тенденция к всё большей цифровизации общества и, как следствие, понятие отраслевой безопасности начинает размываться. Покажем это на примере финансовой и телекоммуникационной сфер.

### ОСОБЕННОСТИ ВОСПРИЯТИЯ ИБ В ТЕЛЕКОМЕ

Долгое время риски информационной безопасности в компаниях телеком-отрасли считались вторичными. Выполнялись только явно прописанные законодательством меры, например, по персональным данным. В то же время считалось (и сейчас кое-где считается), что телеком выполняет роль некоего пересыльщика данных, предоставляя каналы связи, а уж задачи безопасности информации, передаваемой по этим каналам, лежат целиком на совести владельца информации.

Немалую роль играют также трудности донесения до бизнеса информации о ИБ-рисках и необходимости вкладываться в средства защиты. В настоящее время, благодаря тому что телеком стал предоставлять не только каналы связи, но и иные услуги, а также массовому распространению такого явления, как «интернет-вещей», вероятность реализации рисков ИБ возросла, и бизнес начинает это учитывать.

### ...И КРЕДИТНО-ФИНАНСОВОЙ СФЕРЕ

В то же время в кредитно-финансовой сфере изначально не было недооценки рисков ИБ, поскольку именно в этих организациях сосредоточен основной интерес для атакующих — деньги. Понимали это и издатели нормативно-правовых актов, что отразилось в большом количестве как законодательных инициатив, так и распоряжений регулятора (Банк России). В целом до недавнего времени кредитно-финансовые организации были достаточно обособлены и

защищались «каждый сам за себя». Ситуация улучшилась с появлением ФинЦЕРТ, когда реализовался межбанковский обмен по технической составляющей атак.

### С ТОЧКИ ЗРЕНИЯ «БУМАЖНОЙ БЕЗОПАСНОСТИ»

С регуляторной точки зрения возник парадокс: несмотря на кажущуюся жесткость регулирования телеком-отрасли (реестры Роскомнадзора, «пакет Яровой» и т.д.), возможностей для построения систем защиты информации тут больше, нежели в кредитно-финансовой сфере, где теоретически освещено достаточно много аспектов, связанных с защитой информации, но не поясняется, как построить систему защиты, удовлетворяющую регулятора (в данном случае — конкретных проверяющих, т.к. отсутствует методика проверки для них, что даёт простор для толкования требований).

### РАЗНЫЕ ОТРАСЛИ — ОДНО БУДУЩЕЕ

Но время не стоит на месте. Активно развивается финтех, используются «большие данные», ИИ, блокчейн, облачные технологии... Цифровизация банков приводит к отказу от офисов в пользу дистанционного обслуживания. Всё большую ценность играет любая информация, начиная с данных о сотрудниках компаний и заканчивая персональными данными граждан. Понятие отраслевой безопасности стремительно расширяется, включая в себя и новые понятия, в том числе и «обеспечение информационной безопасности бизнес-процесса, затрагивающего несколько отраслей». В будущем число таких бизнес-процессов, объединяющих несколько отраслей, будет только расти.

*Понятие отраслевой безопасности стремительно расширяется, включая в себя и новые понятия, в том числе и «обеспечение информационной безопасности бизнес-процесса, затрагивающего несколько отраслей»*



**Дмитрий МАХАЕВ**  
начальник центра  
мониторинга  
и реагирования  
на инциденты ИБ  
ФГУП «Российская  
телевизионная  
и радиовещательная  
сеть»



В таком контексте телеком-компании трансформируются из «просто предоставляющих каналы связи» в полноценных участников процесса, обеспечивающих часть банковских функций, например, Единую биометрическую систему. Некоторые телеком-компании стали оказывать дополнительные услуги по обеспечению отдельных процессов кредитно-финансовых организаций. Внедряются новые стандарты телевидения (например, HBBTV — Hybrid Broadcast Broadband Television, предоставляющий телезрителям дополнительные интерактивные услуги), предполагающие взаимодействие с кредитно-финансовыми организациями при проведении платежей. Растёт количество «умных устройств», которые также могут проводить платежи и, соответственно, хранят и используют платёжную информацию. Всё это в совокупности приводит к появлению новых возможных векторов атак на стыках границ ответственности двух отраслей.

В части случаев телеком-компании обеспечивают в той или иной степени аутсорс информационной безопасности для банков, например, через коммерциализацию своих SOC. Также и телеком пользуется услугами кредитно-финансовых организаций, предоставляя возможности оплаты своих услуг непосредственно через «личные кабинеты» и используя финансовые инструменты в своей работе (например, при расчётах с контрагентами).

Как следствие идёт размывание чётко очерченных границ ответственности между «банковскими безопасниками» и «телекомовскими безопасниками». Сотрудники компаний начинают искренне считать, что «это не их зона ответственности», а какие-либо договорённости, не говоря уж о совместно выстроенных процессах реагирования на инциденты ИБ, отсутствуют. Т.е. отсутствует как таковое осознание общности выполнения одной задачи — обеспечения безопасности конкретного бизнес-процесса, а не просто отраслевой безопасности.

### А ЧТО ДЕЛАЮТ АТАКУЮЩИЕ?

Атакующим уже не обязательно «пробивать» хорошо защищённую кредитно-финансовую организацию или организацию телеком-отрасли. Чтобы попасть в сеть банка или телеком-организации им проще сосредоточиться на слабо защищённой цели, которую обе стороны «не считают своей».

Кроме того, не стоит забывать и о мотивации атакующих: при цифровизации общества возрастает роль доступности услуг, соответственно становятся выгодными утечки разных данных — ввиду возросших возможностей их монетизации.

Верхнеуровнево можно выделить следующие мотивации:

1. **Личное обогащение.** Тут цель традиционная — банки и хранящиеся в них деньги. Обычно такие злоумышленники не бьют в стык межотраслевых бизнес-процессов, поскольку берут количеством, а не качеством. Против таких вполне успешно работают обычные отраслевые меры безопасности.

2. **Политические мотивы («State-Sponsored Hacktivism»).** Целью может быть как банк, так и телеком: недоступность услуг автоматически поднимает раздражение населения, а в некоторых случаях может вызвать панику. Вопросы личного обогащения здесь отходят на второй план. Хотя, если целью атаки всё же является получение денежных средств (пример — атаки группы Lazarus), то истинная её цель — именно кредитно-финансовая организация, просто атаку на неё осуществили через «слабое звено». Здесь риски целенаправленного выявления уязвимых мест очень высоки.

3. **Хактивизм** (выступают за свободу информации либо как «разоблачители»). Обычно цель атаки — любая информация, которая даёт возможность понять структуру компании, сотрудников, её внутренние процессы. В явном виде не преследуют цели личного обогащения, напротив, распространяют похищенную информацию любыми методами, добиваясь максимальной огласки. Пример — группа «Цифровое сопротивление» (Digital Resistance, DigiRev). Такие группы будут искать «слабые места» и с большой долей вероятности найдут их как раз в межотраслевых взаимодействиях. Основные риски для обеих сторон — репутационные, а также, впоследствии, и финансовые (при хищении ноу-хау компаний либо данных, дискредитирующих компанию).

4. **BountyHunters** или «охотники за наградами». Многие высокотехнологичные компании практикуют программу «BugBounty», т.е. вознаграждение за найденные уязвимости. Многие люди ищут уязвимости с целью получить награду за неё. Обычно они не ориентируются на какую-то конкретную компанию, а случайно или по стечению обстоятельств находят предпосылки для уязвимости, после чего «раскручивают» эту уязвимость. Несмотря на то, что они, как правило, исполнены благих намерений и обычно честно сообщают о найденной уязвимости владельцу, последний в силу разных причин либо игнорирует сообщение, либо отделяется общими фразами. Как результат, уязвимость получает массовую огласку на популярных тематических ресурсах («хабрахабр», «]акер» и т.д.), после чего её начинают эксплуатировать хактивисты, преследующие свои цели.





### ПРОБЛЕМА ПРОТИВОДЕЙСТВИЯ АТАКАМ

Несмотря на понятные мотивы и средства достижения целей злоумышленников, эффективно им противодействовать не получается. Почему? Потому что, несмотря на взаимное проникновение экосистем, в большинстве случаев отсутствует какое-либо масштабное взаимодействие между представителями отраслей — как при обмене индикаторами компрометаций (индикаторами атак), так и обмене опытом в построении систем защиты. Что и даёт возможность атакующим найти то самое «слабое звено».

Тут кроется корень проблемы, из-за которой могут возникнуть глобальные инциденты: одна сторона видит проблему другой, но не считает нужным или не имеет возможности сообщить об этом, что впоследствии приводит к ненужным рискам (как финансовым, так и репутационным) для обеих сторон. Причем, в случае осознания того, что существуют общие бизнес-процессы, безопасность которых должны обеспечивать обе стороны, данных рисков можно было бы избежать.

В текущих реалиях эта проблема уже осознаётся отдельными специалистами по ИБ или CISO организаций, которые в порядке личной инициативы предпринимают попытки по своевременному оповещению или межорганизационному реагированию. Но без фиксации такого опыта на официальном уровне дело с места не

сдвинется. В случае ухода такого инициатора с работы канал оповещения и реагирования, который может спасти деньги и репутацию компании, элементарно перестаёт существовать. Более того, такие взаимоотношения никак не защищены юридически, поэтому инициаторы рискуют как «разборками» внутри организации с последующими «оргвыводами», так и несением административной/уголовной ответственности за нарушение текущего законодательства.

Установлению же официальных отношений (на уровне договоров между организациями различных отраслей) зачастую мешают соображения как политического характера, так и опасения за возможную утечку данных, составляющих коммерческую тайну.

Свою роль тут играет и отсутствие нормативной базы, учитывающей современные тенденции межотраслевых взаимодействий.

\*\*\*

Выход видится только один: создание независимого межотраслевого центра компетенции и наделение его соответствующими полномочиями по разработке как нормативной базы, так и организации и проверке технических мер защиты информационной безопасности. Возможно, таким драйвером смогла бы стать Ассоциация «ФинТех».





**Дмитрий УЛЫБИН**  
директор проекта  
«Единая биометри-  
ческая система»  
ПАО «Ростелеком»

# СРЕДСТВО ОТ БОЛИ

## РЕШЕНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОТ ОПЕРАТОРА ЕБС

**К**омпания «Ростелеком» одной из первых создала облачное типовое решение по информационной безопасности для работы с Единой биометрической системой. Облачное решение, разработанное «Ростелекомом», предоставит малым банкам возможность осуществлять полноценную регистрацию биометрии и удалённую идентификацию клиентов. Работа над созданием Единой биометрической системы началась в 2017 году. Это — важный национальный проект, связанный с хранением и обработкой биометрических данных граждан.

### ВЫПОЛНЕННЫЕ ТРЕБОВАНИЯ

Платформа Единой биометрической системы соответствует требованиям, предъявляемым к «Ростелекому» регуляторами в области информационной безопасности: ФСБ и ФСТЭК России.

Основные положения по обработке персональных и биометрических данных сформулированы в федеральных законах № 152-ФЗ от 27 июля 2006 года «О персональных данных» (ограничивает использование биометрических данных) и № 115-ФЗ от 7 августа 2001 года «О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма» (определяет требования по сбору, обработке, хранению биометрических персональных данных).

Применение удалённой идентификации клиентов в финансовой сфере регламентировано федеральным законом № 482-ФЗ от 31 декабря 2017 года, который вносит изменения в № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма» и № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Для нейтрализации угроз, сформулированных Банком России на основании требований регуляторов, каждый банк должен установить программно-аппаратный криптографический модуль (Hardware Security Module, HSM) соответствующего класса защищённости, с помощью которого банк проверяет и подписывает для Единой биометрической системы биометрические данные. Помимо этого, банки должны обеспечить защиту внутренних каналов передачи информации между филиалами и дата-центром банка, а также обеспечить защиту рабочих мест операторов, осуществляющих сбор биометрических данных. Из-за сложности работы, которую предстоит проделать банкам, ЦБ РФ дал им отсрочку по внедрению средств информационной безопасности до 31 декабря 2019 года.

Важный этап работы происходит в банках — именно там регистрируются биометрические данные. Для того чтобы избежать возможных угроз при регистрации и обработке биометрической информации внутри инфраструктуры кредитной организации, 9 июля 2018 года Банк России выпустил «Указание банка России о перечне угроз биометрической информации при регистрации и обработке её в кредитных организациях». В документе содержатся ссылки на приказ ФСБ России № 378 от 10 июля 2014 года с описанием того, какими средствами и способами защиты эти угрозы можно нейтрализовать.

Часть угроз, которые признаны актуальными, требует серьёзных и комплексных мер для защиты биометрических данных граждан. Кроме того, для создания решения, соответствующего заявленным требованиям безопасности, необходимо согласовать системный проект, а после создания решения — провести ряд тематических исследований созданного продукта.

Исследования должны подтвердить, что средства защиты:

- ◆ правильно встроены в решение;
- ◆ правильно используются банком;
- ◆ обеспечивают нужные меры защиты и класс защищённости компонентов решения;
- ◆ соответствуют требованиям методических рекомендаций регулирующих органов.

### ПРЕДПОСЫЛКИ ДЛЯ СОЗДАНИЯ ТИПОВОГО РЕШЕНИЯ

Выполнение всех требований по защите информации предполагает серьёзную работу со сторо-

*Выполнение всех требований по защите информации предполагает серьёзную работу со стороны кредитных организаций, но не у всех есть ресурсы, время и специалисты для реализации таких мер*



ны кредитных организаций, но не у всех есть ресурсы, время и специалисты соответствующей квалификации для реализации таких мер. Поэтому регуляторы предложили рынку создать типовые решения, которые бы соответствовали всем нормативным и техническим требованиям, были согласованы с ФСБ России, прошли все тематические исследования и не требовали бы дополнительных исследований на стороне кредитной организации.

Сначала «Ростелеком» разработал системный проект на типовое решение, потом — системный проект облачного решения. Оба этих документа были согласованы с ФСБ России. Итогом работы стал типовой продукт по информационной безопасности, созданный по согласованному ранее системному проекту. В конечном счёте решение, разработанное Ростелекомом, получило положительное заключение ФСБ России, которое на основе анализа результатов тематических исследований подтвердило соответствие всем необходимым требованиям по информационной безопасности. Помимо этого, также был создан и согласован комплект эксплуатационной документации на решение.

## МЕТОДИЧКА БАНКА РОССИИ

Для того чтобы облегчить обеспечение информационной безопасности при обработке биометрических персональных данных для кредитных организаций, 14 февраля 2019 года Банк России выпустил «Методические рекомендации по нейтрализации банками угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия представленным биометрическим персональным данным гражданина Российской Федерации».

В соответствии с этим документом у банка есть три варианта реализации требований по информационной безопасности:

- 1) разработать собственное решение;
- 2) использовать типовое решение;
- 3) использовать облачное решение.

То есть у банка есть выбор: использовать корпоративные и облачные решения вендоров или самостоятельно заниматься всем процессом разработки (Рисунок 1). При этом каждому направлению предъявляются свои требования и рекомендации.

При разработке собственного решения банку предстоит самостоятельно пройти весь путь разработки согласования:

- ◆ согласовывать системный проект;
- ◆ разработать решение в соответствии с согласованным ранее системным проектом;
- ◆ провести тематические исследования;

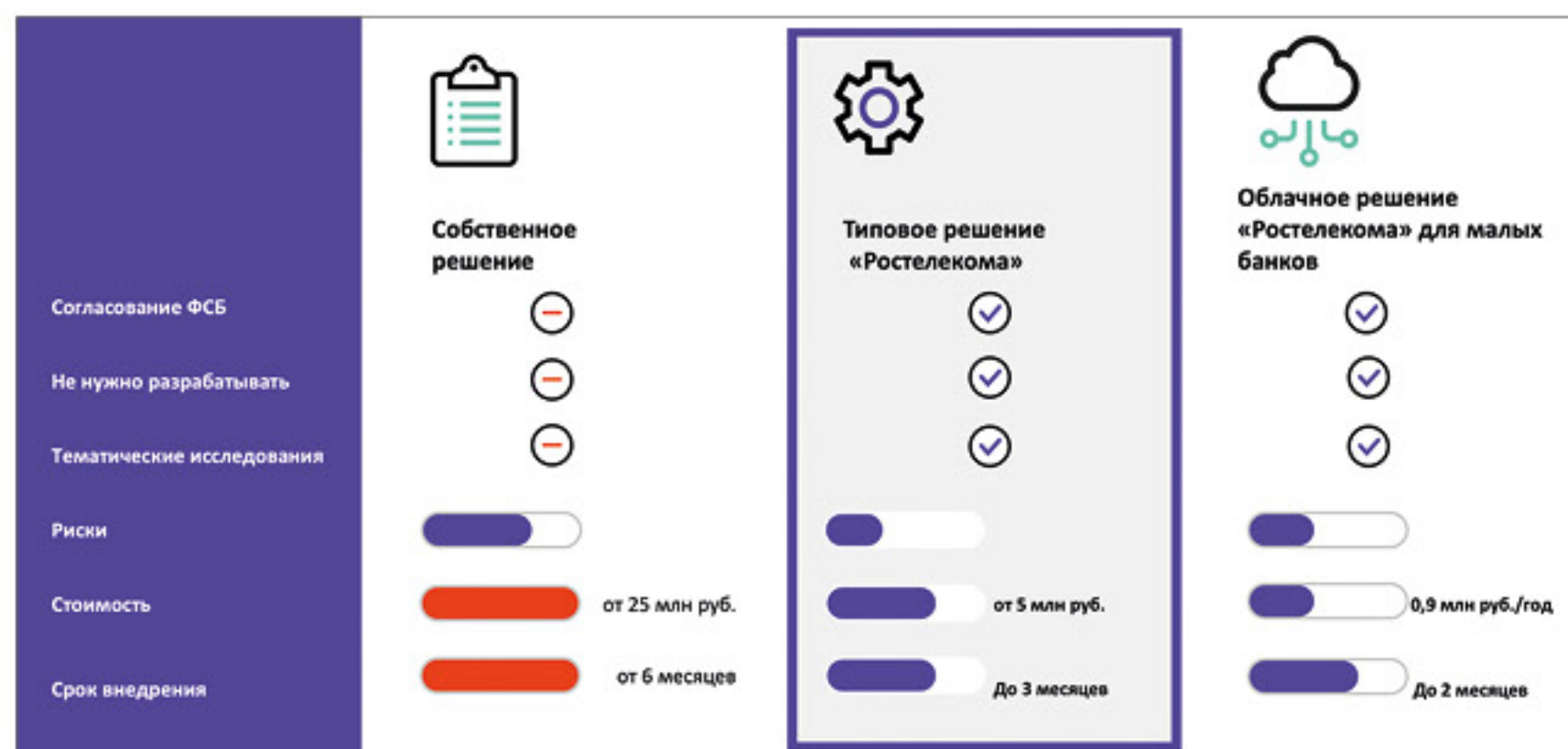


Рисунок 1. Пути выполнения требований по ИБ в банке

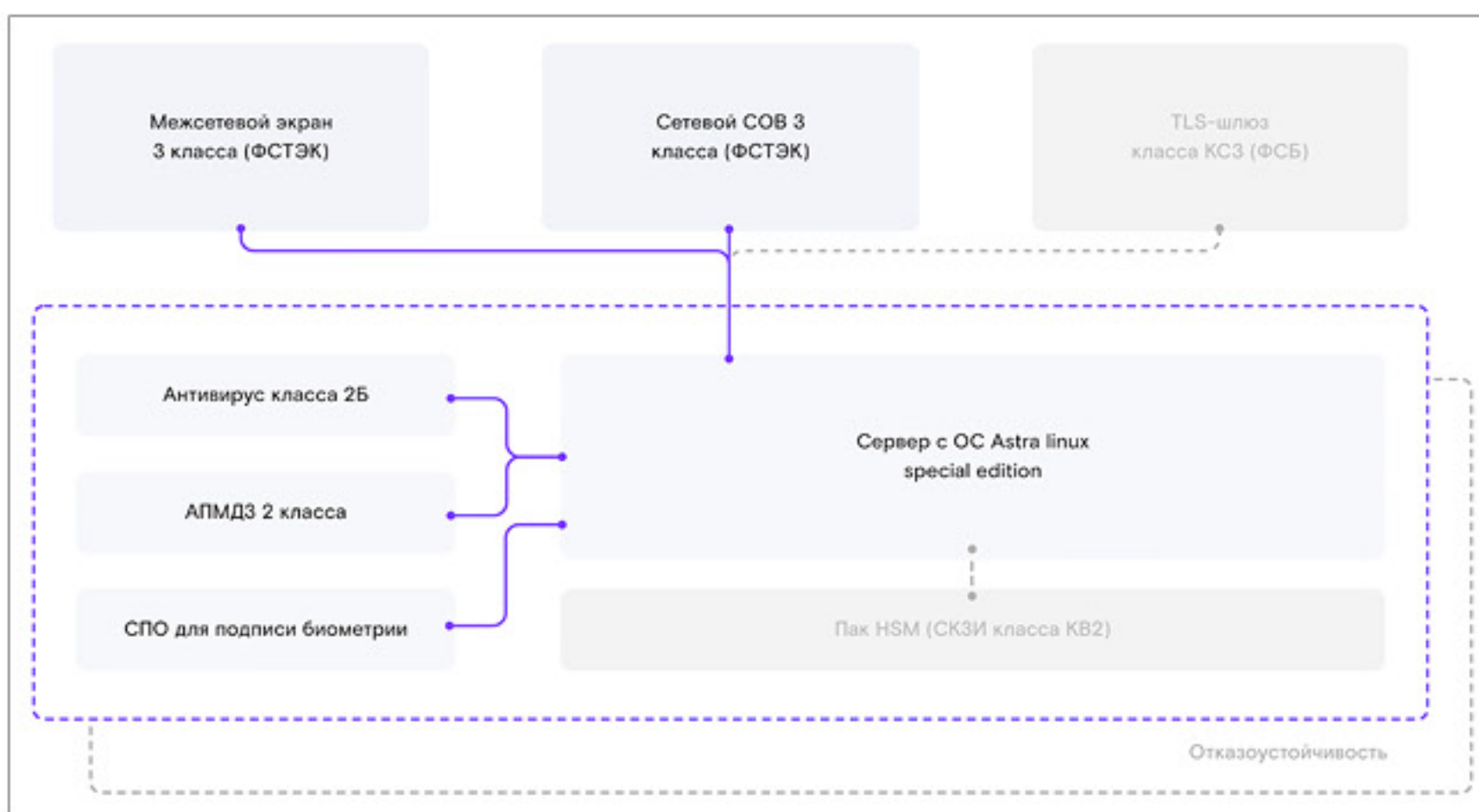


Рисунок 2. Как это работает?

- ◆ получить отчёт лаборатории и заключение ФСБ России;
- ◆ согласовать комплект эксплуатационной документации;
- ◆ внедрить решение.

## СТРУКТУРА ТИПОВОГО РЕШЕНИЯ

Типовое решение «Ростелекома» — это программно-аппаратный комплекс, в который включены средства электронной подписи класса КВ2 и сервер со специальным программным обеспечением, который взаимодействует со средством подписания. Для этого программного обеспечения проведены все необходимые исследования, которые исключили угрозы, связанные с недекларированными возможностями. ПО соответствует всем требованиям методических рекомендаций, а также согласованному ранее системному проекту, отсутствует негативное влияние на средство электронной подписи, кроме того выполнена оценка уровня доверия (Рисунок 2).

В типовой продукт «Ростелекома» также входят средства защиты информации, которые расположены вокруг сервера с HSM и обеспечивают защищённый периметр решения. В про-



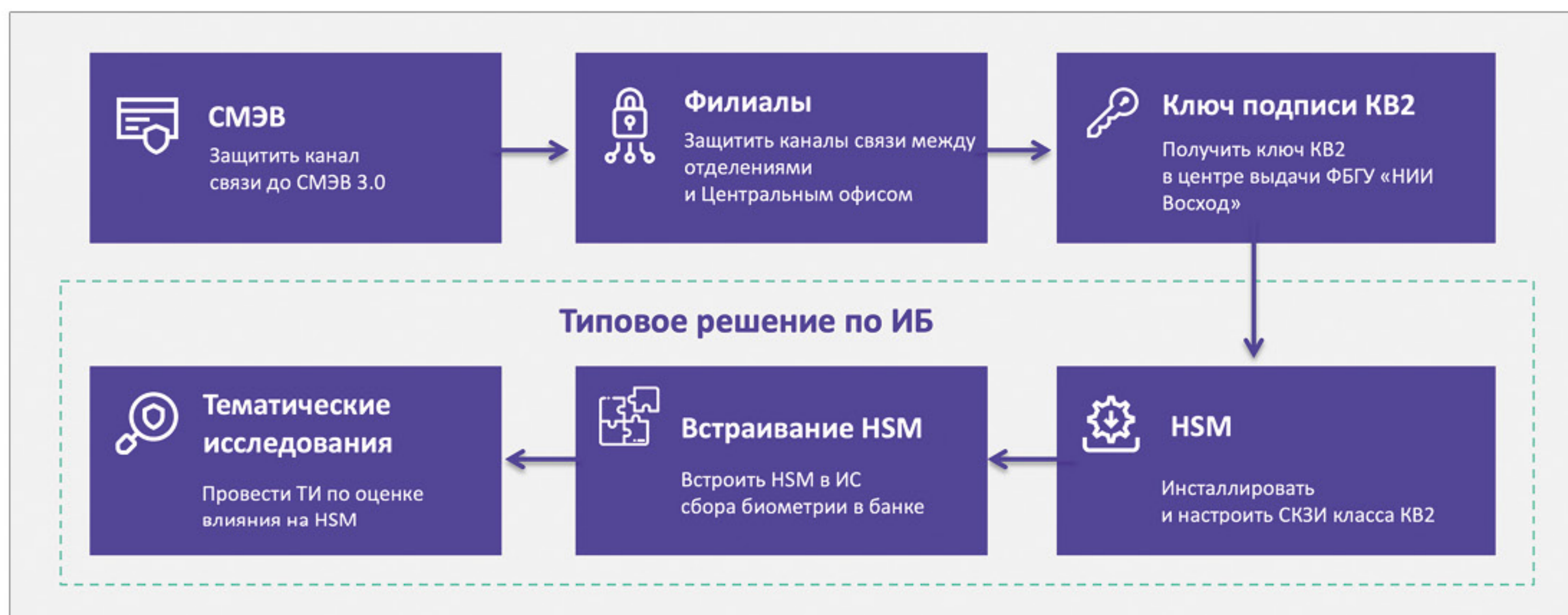


Рисунок 3. Задачи обеспечения ИБ сбора биометрии

граммно-аппаратный комплекс «Ростелекома» входит набор эксплуатационной документации, согласованный с ФСБ России. Проведены тематические исследования и получено заключение ФСБ России о соответствии требованиям информационной безопасности (Рисунок 3).

### ТИПОВОЕ РЕШЕНИЕ В ОБЛАКАХ

Облачное типовое решение — это сервис, который представляет размещённое на стороне «Ростелекома» оборудование для подписания биометрических данных и отправки их в Единую биометрическую систему. В решение входит сервер подписания, который должен быть расположен на стороне банка. Сервер упрощает интеграцию с информационными системами кредитной организации, а также избавляет от необходимости проведения тематических исследований силами организации.

Таким образом, при использовании облачного продукта банку не нужно содержать высококлассных специалистов для администрирования средств электронной подписи, а также другие средства обеспечения информационной безопасности биометрических данных, нет необходимости и выделять отдельные стойки для средств защиты информации соответствующих классов.

Облачное решение «Ростелекома» может работать как с разработанным компанией «АРМ Биометрия», так и предоставляет открытые интерфейсы для интеграции с другими АРМ сбора биометрических данных или собственными разработками банка (Рисунок 4).

### ДРУГИЕ РЕШЕНИЯ

Типовое решение разрабатывает не только «Ростелеком», но и другие компании. Их можно по-разному реализовать, однако, для того чтобы

использовать все преимущества Единой биометрической системы, оно должно поддерживать как возможность сбора биометрических образцов, так и удалённой идентификации пользователя.

На данный момент только в типовом решении «Ростелекома» реализованы оба этих процесса: и сбор биометрических данных, и удалённую идентификацию. Остальные вендоры лишь собирают биометрические данные. «Ростелеком» первым получил заключение ФСБ России о соответствии всем нормативным требованиям по безопасности и методическим рекомендациям.

Остальные типовые решения сильно отстали технически — они лишь согласовали системные проекты, им ещё предстоит пройти тематические исследования и получить заключения регуляторов. Так как системные проекты других вендоров реализуют только сбор данных, кредитная организация, которая выберет такое решение, не сможет получить новых клиентов с помощью удалённой идентификации. То есть не будет реализовано главное преимущество от использования Единой биометрической системы. Кроме того, в дальнейшем оказание услуг в удалённом канале с помощью верификации пользователей в Единой биометрической системе может стать обязательным для кредитных организаций. В таком случае решения, в которых не реализован этот бизнес-процесс, не будут соответствовать требованиям регулятора.

### КАЖДОЙ ФИНАНСОВОЙ ОРГАНИЗАЦИИ — СВОЁ РЕШЕНИЕ

Так как кредитная организация подключается к провайдеру облачного решения по защищённым каналам связи, производительность сервисов сбора и удалённой верификации в составе облачного решения может столкнуться с огра-



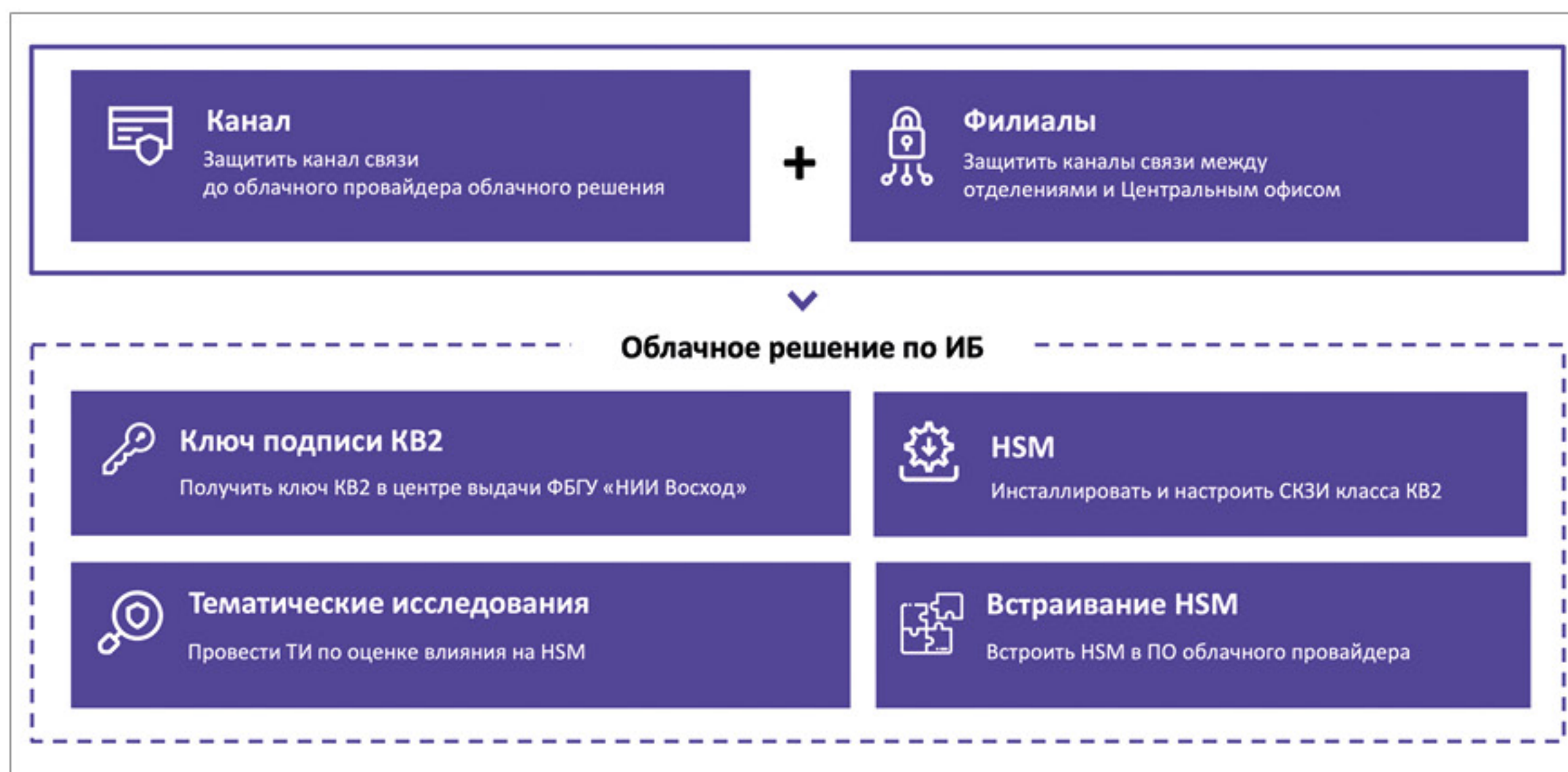


Рисунок 4. Задачи кредитной организации при использовании «облака»

ничениями каналов связи. У типового продукта, который размещается в инфраструктуре банка, таких ограничений нет, и его производительность практически неограничена. Кроме того, в случае необходимости типовой продукт может быть масштабирован для удовлетворения соответствующих потребностей кредитной организации.

Облачный продукт ориентирован на малые и средние банки, а также другие организации с небольшим потоком биометрических данных. Типовой продукт с размещением в инфраструктуре организации подойдет тем банкам, которые рассчитывают на серьезный поток биометрической информации.

Покупка типового продукта влечёт за собой единовременные капитальные расходы, а облачное решение — ежегодные операционные затраты организации. При этом на горизонте планирования 5 лет затраты на внедрение типового и облачного решения будут приблизительно равны.

«Ростелеком» как крупнейший телекоммуникационный оператор и оператор Единой биометрической системы гарантирует стабильную работу типового продукта и облачного решения. Оба решения поставляются под ключ и включают в себя логистику, настройку в инфраструктуру банка и поддержку со стороны оператора и партнёров.

На данный момент к Единой биометрической системе подключено свыше 200 банков и более 12 000 отделений.

## СТАТУС СОЗДАНИЯ ОБЛАЧНОГО РЕШЕНИЯ

«Ростелеком» создал и развернул программный код облачного решения. Сегодня ком-

пания проводит тематические исследования облачного решения, которые завершатся через несколько месяцев. Облачное решение будет размещаться на территории защищённой площадки «Ростелекома». После проведения исследований отчёт будет направлен в ФСБ России и в ФСТЭК России. После получения соответствующих заключений и сертификатов «Ростелеком» начнёт работы по аттестации объекта информатизации, где будет размещено решение. Это нужно для того, чтобы получить аттестат о соответствии требованиям информационной безопасности на объект, который представляет из себя совокупность программных мощностей, площадки и соответствующих средств защиты. Рассчитываем, что к концу II квартала 2020 года облачный продукт «Ростелекома» получит заключение ФСБ России, сертификат ФСТЭК России и аттестат соответствия требованиям информационной безопасности на объект информатизации.

## НА ЧТО ОБРАЩАТЬ ВНИМАНИЕ

В банковской сфере наиболее важный критерий выбора того или иного биометрического решения — надёжность поставщика и технологии, а также подтверждение соответствия требованиям регуляторов. Поэтому значимым является опыт внедрения в других крупных организациях аналогичной или смежной отрасли, рекомендации других банков. Важным фактором выбора поставщика решения является простота интеграции с информационными системами банка и возможности дальнейшей поддержки. Ключевые требования: поставщик должен быть из РФ, а продукт / решение должно соответствовать законодательным нормам.



Директор по цифровой идентичности «Ростелекома» Иван Беров:

«Мы заботимся о том, чтобы банки смогли выполнить требования регулятора в установленные законом сроки. Решения «Ростелекома» могут использоваться в инфраструктуре банков и позволяют финансовым организациям взаимодействовать с Единой биометрической системой в полном соответствии с требованиями безопасности».





**Антон СВИНЦИЦКИЙ**  
директор по консалтингу  
АО «ДиалогНаука»



**Ксения ЗАСЕЦКАЯ**  
старший консультант отдела  
консалтинга АО «ДиалогНаука»

# НОВЫЙ ВЕКТОР

## В РАЗВИТИИ РЕГУЛЯТОРНЫХ ТРЕБОВАНИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ

**С** момента выхода первой редакции Стандарта СТО БР ИББС-1.0 прошло 16 лет. За это время Банком России совместно со специалистами в области защиты информации проведена огромная работа по стандартизации требований по информационной безопасности для финансовых организаций. Но «рекомендательный» статус СТО БР ИББС не позволял создать единую, измеримую и применимую ко всем финансовым организациям методологическую основу для реализуемых систем обеспечения информационной безопасности.

Подходы, заложенные как в СТО БР ИББС-1.0, так и в методику оценки соответствия СТО БР ИББС-1.2, не позволяли для финансовых организаций разного «масштаба» проводить сбалансированную политику в области защиты информации по нескольким основным причинам:

- ♦ *слишком большая обобщённость требований* — большинство требований имело формулировку «должны быть документально определены и утверждены руководством, должны выполняться и контролироваться процедуры...», позволяющую организациям самостоятельно выбирать глубину реализации с целью получения «положительной» оценки соответствия в ущерб качеству реализации и соответствию актуальным угрозам безопасности информации;

- ♦ *отсутствие градации требований* в зависимости от уровня значимости

организации для финансового рынка в целом (нельзя подводить все организации под одни требования, которые могут быть легко реализованы в инфраструктуре крупных участников рынка, но невыполнимы с экономической точки зрения в маленьких организациях);

- ♦ СТО БР ИББС ориентирован в первую очередь на кредитные организации.

Двигаясь от СТО БР ИББС с добровольной областью применения (выбираемой кредитной организацией самостоятельно) к текущим Положениям Банка России с несколько это возможно в официальных документах формализованной областью применения (Положения 382-П, 672-П, 683-П и 684-П) появилась необходимость создания единой методологической основы к формализации требований к защите информации. Такой основой стали первые документы из серии Национальных стандартов ГОСТ Р 57580.1–2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» (требования) и ГОСТ Р 57580.2–2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценка соответствия».

Вчитываясь в положения Национального стандарта ГОСТ Р 57580.1–2017, мы видим преемственность:

- ♦ необходимость построения сбалансированной, основанной на оценке ри-

сков и моделировании угроз безопасности информации, экономически обоснованной системы обеспечения информационной безопасности;

- ♦ восприятие системы обеспечения информационной безопасности не как единойжды созданного и статичного продукта, а как динамической системы, представляющей собой совокупность процессов обеспечения информационной безопасности и процессов управления информационной безопасностью (цикл Plan — Do — Check — Act).

Однако, как и написано в Положениях Банка России, переводящих Национальный стандарт в область обязательных к применению документов, ГОСТ Р 57580.1 должен использоваться как базовый набор мер, необходимых к реализации на уровне ИТ-инфраструктуры финансовых организаций, а требования к мерам защиты информации на уровне технологических процессов определяются соответствующими нормативными документами Банка России.

Банк России даёт возможность финансовым организациям делать выбор мер защиты информации, основываясь на формализованных в нормативных документах критериях, проводить их адаптацию и уточнение (с учётом особенностей ИТ-инфраструктуры и результатов моделирования угроз), а также предоставляет возможность применения компенсирующих мер (экономическая целесообразность). При этом Банк России уходит от «самооценок» в сторону внешних независимых аудитов.



Такой подход должен позволить получать повторяемые результаты, как один из критериев независимости аудита, и отслеживать состояние информационной безопасности финансовых организаций по единой методологии.

Изменился и подход к формированию базовых требований:

- ♦ градация требований исходя из выбранного уровня защиты информации: «минимальный», «стандартный» или «усиленный»;

- ♦ переход от общих требований «должно быть определено, выполняться и контролироваться» к детальным требованиям по основным процессам защиты информации;

- ♦ определение уровня реализации требований (организационные меры или технологические) и смещение в сторону необходимости технической реализации, особенно в контурах безопасности соответствующих усиленному уровню;

- ♦ расширение перечня требований, которые должны быть реализованы на уровне автоматизированных систем;

- ♦ применение PDCA-модели к каждому процессу защиты информации, а не к финансовой организации в целом;

- ♦ отсутствие дублирования требований, описанных в соответствующих документах других регуляторов, например, в ГОСТ Р 57580.1 отсутствуют требования к процессам применения средств криптографической защиты информации.

В ГОСТ 57580.1 отсутствуют требования о необходимости обязательного применения сертифицированных средств защиты информации, однако дана отсылка к результатам моделирования угроз (по аналогии с Приказом ФСТЭК России от 18 февраля 2013 г. № 21 и Постановлением Правительства Российской Федерации от 01.11.2012 № 1119):

**Необходимо обеспечить применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия в случаях, когда применение таких средств необходимо для нейтрализации угроз безопасности, определённых в модели угроз и нарушителей безопасности информации финансовой организации.**



Методика оценки соответствия определена положениями ГОСТ Р 57580.2–2018, однако описание самого процесса проведения аудита информационной безопасности лучше раскрыто в документе СТО БР ИББС-1.1–2007 года. Данный подход может использоваться как при проведении оценки соответствия требованиям Положения 382-П, так и при проведении оценки соответствия требованиям ГОСТ Р 57580.1.

Ключевые отличия от подхода, применяемого в Положении Банка России 382-П:

- ♦ отсутствуют корректирующие коэффициенты, возникающие при невыполнении установленных требований;

- ♦ использование среднего арифметического как основного метода вычисления оценок по направлениям;

- ♦ введение «штрафов» за выявленные нарушения.

Единственное, на что стоит обратить внимание финансовым организациям — в разных нормативных документах определена разная периодичность оценки:

- ♦ для сегмента сбора и обработки биометрических персональных данных — 1 раз в год в соответствии с Приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 25.06.2018 г. № 321);

- ♦ для других контуров безопасности в соответствии с требованиями Банка

России, например, в соответствии с Положением Банка России 683-П — 1 раз в два года.

\* \* \*

Рассматривая развитие нормативной базы по защите информации на территории Российской Федерации в первую очередь обращаешь внимание, что растёт не только количество необходимых к реализации мер, но и увеличивается глубина проработки этих требований по отдельным направлениям, регулятор реагирует на изменяющиеся тренды и актуальные угрозы информационной безопасности. Поэтому стандартизация требований для организаций финансового рынка это логичное и прогнозируемое направление развития. Однако без должной поддержки и вовлечённости руководства и всех подразделений компаний, без корректного отношения компаний к аудиторам и выполнения аудиторами взятых на себя обязательств, таких, как соблюдение «аудиторской этики», обеспечение достоверности и независимости результатов аудитов, все попытки Банка России через регулирование донести до финансовых организаций актуальность текущих проблем информационной безопасности всё равно останутся «бумажной безопасностью».





**Алексей НОВИКОВ**  
директор экспертного  
центра безопасности  
Positive Technologies  
(PT Expert Security Center)



**Наталия КАЗАНЬКОВА**  
продуктовый маркетолог  
Positive Technologies

## SOC БЕЗ АНАЛИЗА ТРАФИКА = ЦЕНТР НЕДОСТАТОЧНОГО РЕАГИРОВАНИЯ

**З**а последние несколько лет все так или иначе поняли, что такое SOC (Security Operation Center), «с чем их едят» и даже начали их массово строить. Правда, в большинстве случаев стройка только начата: куплен SIEM, сформированы первая и вторая линии и т.д.

Но здесь как в поговорке про партизан, стремительно толстеющих по мере углубления в лес: чем активнее ведут себя SOC-строители, тем очевиднее становится, что данных, требуемых для эффективного мониторинга и выявления угроз, недостаточно. SIEM-системы выявляют некоторые виды атак только по косвенным признакам, от антивирусов легко спрятать вредоносное ПО, а решения по защите конечных точек (EDR) крайне непросто установить на все узлы.

### КОГДА SIEM НЕ ПОМОЩНИК

Да, SIEM-системы могут многое, но, тем не менее, не всё: эксплуатацию некоторых уязвимостей, использование инструментов и техник атак сложно выявить, пользуясь только анализом событий. Это актуально при необходимости детектировать использование хакерских инструментов, создающих огромное количество событий. Так, к примеру, чтобы обнаружить применение PowerView, инструмента для разведки в Active Directory, нужно включить журналирование события 1644 в Windows. Это событие показывает LDAP<sup>1</sup>-активность инструмента

PowerView. Таких событий может быть драматически много и «плохие» события могут затеряться в общей массе. Что делать? Детектировать в трафике по LDAP-запросам.

Также SIEM не слишком полезен в случае, скажем, DCS shadow — атаки на Active Directory, когда создаётся поддельный контроллер домена, который не отправляет события в SIEM-систему. Однако эту активность также можно увидеть в трафике: здесь отчётливо видно добавление нового объекта в схему конфигурации типа «контроллер домена».

### ОБМАНУТЬ АНТИВИРУС? ЛЕГКО!

Нельзя рассчитывать на выявление актуальных угроз, используя одни только антивирусные системы. Преступники сегодня с успехом их обходят, используя наборы специальных техник. В их числе и так называемый code signing, то есть подписывание вредоносного кода цифровым сертификатом реально существующей компании, что позволяет выдать его за легитимное приложение.

Так, к примеру, вредоносный архив с загрузчиком, подписанным корректным сертификатом, содержала одна из рассылок APT-группировки Silence. Этот же сертификат использовала также группировка Cobalt. Подобную задачу злоумышленник может решить, воспользовавшись соответствующей уязвимостью, такой, например, как критическая ошибка в библиотеке curl32.dll (CVE-2020-0601), которая используется во всех релизах ОС Microsoft. Уязвимость такого типа злоумышленник может использовать и для подделки

сертификата, и подписать вредоносный исполняемый файл, создав впечатление, что он принадлежит доверенному поставщику.

Применение различных нагрузок (скриптовых, in-memory) — ещё один классический способ обхода детектирования. Не менее популярна и обфускация, при которой злоумышленники запускают вредоносный код, что затрудняет его анализ антивирусными системами. Чтобы предотвратить деконструкцию вредоносных программ и затруднить анализ их поведения, создатели вредоносного ПО иногда сжимают (упаковывают) свои вредоносные программы, сочетая это с шифрованием файлов.

Для обхода антивирусных решений используют и внедрение вредоносного кода в память другого процесса, запущенного в системе (process injection). А техника masquerading применяется в тех случаях, когда требуется создать новый сервис, который будет тщательно замаскирован под легитимный.

### НЕ EDR'ОМ ЕДИНЫМ

Решения для защиты конечных узлов EDR (endpoint detection and response) — эволюционное продолжение антивирусов. Они используют поведенческий и эвристический анализы, благодаря чему могут использоваться для защиты не только от вирусных атак, но и от новых видов угроз.

Основная проблема решений такого типа — покрытие всех узлов в сети и выстраивание процесса контроля их работоспособности, централизованного управления и запрета появления узлов без установленных EDR-систем.

<sup>1</sup> Lightweight Directory Access Protocol — облегчённый протокол доступа к каталогам



Также всегда актуален вопрос совместимости с прикладным ПО и ОС, использующимися в организации. Не все хотят внедрять EDR из-за существенного увеличения нагрузки на серверы и рабочие станции — особенно если в компании большая утилизация ресурсов или используется устаревший парк оборудования. А значит, останутся «белые пятна» и необходимо искать другие способы мониторинга безопасности.

### ЗАЧЕМ СМОТРЕТЬ В ТРАФИК?

Системы анализа трафика (network traffic analysis, NTA) могут помочь EDR, SIEM и другим средствам мониторинга и защиты увидеть действия киберпреступников в «слепых зонах». Эксперты SANS Institute включают NTA в топ технологий для выявления угроз, работой которых довольны в SOC. Благодаря каким факторам системы такого класса стоит активнее использовать в SOC'ах?

### NTA В РОЛИ ДЕТЕКТОРА АТАК

Система NTA, установленная на периметре, сможет выявлять угрозы аналогично IDS, когда злоумышленник ещё только пытается проникнуть в сеть. Но особенно эффективной данная система будет при анализе внутреннего трафика: NTA позволяет выявлять злоумышленника, когда он уже проник внутрь периметра, перемещается по сети и приближается к критически важным для бизнеса системам.

«Под капотом» такой системы набор различных механизмов обнаружения угроз в инфраструктуре. Например, в PT Network Attack Discovery (PT NAD), системе класса NTA компании Positive Technologies, атаки выявляются с помощью машинного обучения, ретроспективного анализа, пяти тысяч правил детектирования и почти 20 000 индикаторов компрометации. Это позволяет системе покрыть большую часть техник из матрицы MITRE ATT&CK<sup>2</sup>,

<sup>2</sup> MITRE ATT&CK — база знаний, разработанная и поддерживаемая корпорацией MITRE на основе анализа реальных APT-атак. Представляет собой структурированный набор тактик атаки, для каждой из которых указан список возможных техник. Помогает ИБ-специалистам структурировать знания об APT-атаках, категоризировать действия злоумышленников и выбирать эффективную стратегию реагирования.

которые применяются атакующими при первоначальном доступе (initial access), разведке (discovery), горизонтальном перемещении (lateral movement), взаимодействии с командным центром (command and control).

При работе NTA вместе с SIEM-системой степень покрытия техник из матрицы ATT&CK возрастает. SIEM-системы сильнее в детектировании техник выполнения (execution), повышения привилегий (privilege escalation) и обхода защиты (defence evasion), а NTA — в техниках получения первоначального доступа (initial access) и взаимодействия с командным центром (command and control).

**1. Хранение данных, необходимых для расследования инцидентов и threat hunting.** Некоторые NTA-системы работают только с NetFlow, а другие умеют анализировать сырой трафик. Вторые могут хранить копию трафика, и когда происходит инцидент, это помогает понять, что и как произошло. Например, PT NAD хранит сырой трафик и 1200 параметров сетевых сессий.

**2. Сетевой комплаенс.** Часто в организациях во внутреннем трафике можно увидеть учётные записи или почтовые сообщения в открытом виде. При анализе защищённости мы выявляем подобные проблемы в среднем в 44% обследуемых организаций. Нарушения сетевой безопасности снижают эффективность используемых средств защиты и увеличивают шансы злоумышленников на быстрое и беспрепятственное развитие атаки.

PT NAD определяет более 50 распространённых протоколов и 30 из них разбирает на уровнях L2 — L7. Система видит и сетевые взаимодействия и может заметить передачу учётных записей и почтовых сообщений в открытом виде, использование утилит для удалённого доступа, инструментов сокрытия активности в сети и широко-вещательных протоколов.

Скомпрометировав сеть, злоумышленник может в пассивном режиме перехватить учётные данные (что в том числе может позволить злоумышленнику повысить свои привилегии в той или иной системе атакуемой организации), закрепить своё присутствие в инфраструктуре и пр. Поэтому важно

контролировать соблюдение элементарного сетевого комплаенса и оперативно устранять ошибки и нарушения.

Например, чтобы выявить учётные данные, передаваемые по сети в открытом виде, в PT NAD достаточно отфильтровать сетевые сессии по признаку передачи пароля. В карточке сессии есть информация, которая поможет в устранении ошибки: адреса узлов отправителей и получателей.

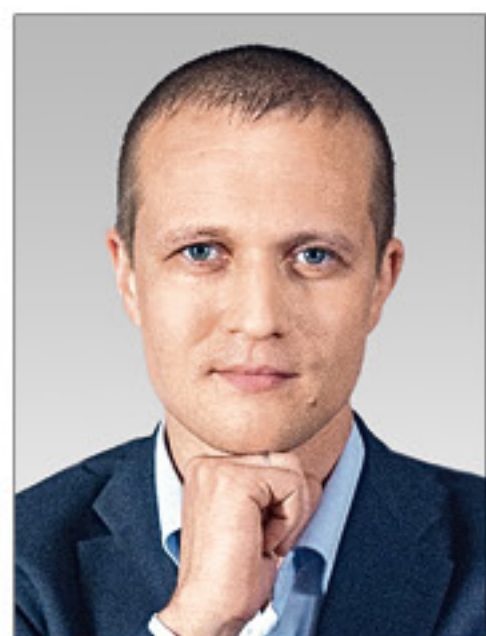
### УРАВНЕНИЕ С ТРЕМЯ ИЗВЕСТНЫМИ: NTA, ANTIВИРУС И ПЕСОЧНИЦА

Зловредное ПО, распространяющееся по сети, не всегда выявляется антивирусными средствами защиты. Для его обнаружения в передаваемых по сети файлах можно интегрировать NTA-систему с антивирусом и песочницей. Песочница в этом случае будет запускать файлы в изолированной виртуальной среде и по поведению файла делать вывод о его вредоносности. Например, PT NAD (NTA-решение) умеет извлекать файлы из трафика и автоматически передавать их на проверку в систему защиты от вредоносных программ PT MultiScanner. PT MultiScanner проводит антивирусную проверку и анализ файлов в песочнице и выдаёт вердикты об их безопасности. В случае обнаружения вредоносной программы передачу файла можно заблокировать. Использование песочницы также позволяет обезопасить электронную почту и файловые хранилища.

\* \* \*

NTA и SIEM — взаимодополняющие системы, которые совокупно покрывают большую часть известных техник атак и дают высокую видимость сети. Например, заметив подозрительную активность в NTA, в SIEM-системе можно узнать, что именно атакующие делали на конкретном узле, какие процессы при этом были задействованы, и проследить дальнейшие действия злоумышленников. Исследовательское агентство Gartner включило их вместе с EDR-решениями в триаду SOC, которые вместе значительно снижают шансы атакующих на достижение целей в вашей инфраструктуре.



**Антон АФАНАСЬЕВ**руководитель направления  
информационной  
безопасности компании СТИ

# АНАЛИЗ ТРАФИКА

## КАК СРЕДСТВО ПРОАКТИВНОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Н**и для кого уже не секрет, что информационная безопасность должна развиваться практически непрерывно, чтобы обеспечить защиту от современных и будущих угроз. На текущий момент уровень технической грамотности злоумышленников существенно вырос и становится всё более высоким с каждым днём, а различные атаки на ИТ-инфраструктуру стали более изощрёнными, целенаправленными. Этап случайных атак закончился, хакинг практически перестал быть развлечением — сейчас это полноценный бизнес. Многие государства имеют собственные кибервойска. В связи с этим, обеспечение информационной безопасности (далее — ИБ) ИТ-инфраструктуры компании становится крайне важным аспектом её полноценного, бесперебойного и эффективного функционирования.

### ВСЕ СИСТЕМЫ ХОРОШИ, ОДНАКО...

В основном, для обеспечения ИБ компаний используется следующий набор средств, по отдельности или в комбинации:

- ♦ межсетевой экран (Firewall);
- ♦ система предотвращения/обнаружения вторжений (IPS/IDS);
- ♦ встроенный функционал управления межсетевым доступом (ACL);
- ♦ системы защиты конечных точек (Antivirus/Anti-Malware/HIDS/HIPS/DLP);

♦ система контроля доступа к сети (NAC);

♦ система управления событиями ИБ (SIEM).

Все эти системы хороши как по отдельности для решения поставленных задач, так и в комплексе. Однако существуют различные задачи, такие как выявление и предотвращение комплексных угроз и целевых кибератак, которые данные системы решить не в состоянии, поскольку в современных реалиях сетевой периметр любой компании размыт благодаря использованию облачных технологий и мобильности сотрудников. Не стоит забывать о существенном росте объёмов передаваемого зашифрованного трафика, а также возможности инкапсуляции трафика приложений в другие протоколы (туннелирование), что существенно сказывается на сложности выявления комплексных угроз, поскольку для сотрудников службы ИБ данный трафик будет выглядеть как легитимный.

### ОСНОВНАЯ ПРОБЛЕМА

В качестве основной проблемы, препятствующей выявлению и предотвращению комплексных угроз, можно обозначить отсутствие полноценной, детальной видимости и автоматизированного поведенческого анализа сетевого трафика. Обнаружение комплексных угроз в сетевом трафике и проактивное реагирование на них становится возможным благодаря использованию систем Network Traffic

Analysis (сетевой анализ трафика, далее — NTA), которые выявляют угрозы, выполняя глубокий анализ сетевого трафика вплоть до 7-го уровня сетевой модели OSI (уровень приложений), предоставляя таким образом возможность раннего обнаружения злоумышленников, оперативного выявления атак, локализации угроз и анализа выполнения требований регламентов ИБ компаний в сегменте сетевого функционирования.

### STEALTHWATCH

Системный интегратор СТИ (Communications. Technology. Innovations.) в своих проектах для анализа сетевого трафика чаще всего применяет Cisco Stealthwatch Enterprise (далее — Stealthwatch). Это решение использует телеметрию из существующей сетевой инфраструктуры, повышает эффективность обнаружения угроз, ускоряет реагирование на них и упрощает сегментацию сети с помощью многоуровневого машинного обучения и усовершенствованного поведенческого моделирования. Одной из ключевых особенностей, крайне незначимой для ИБ, является интеграция Stealthwatch с каналом глобальной аналитики угроз, разработанным Cisco Talos, который обеспечивает дополнительный уровень защиты за счёт сопоставления подозрительной активности в сетевой среде с обширной базой известных индикаторов компрометации (Indicators of Compromise, IOC), благодаря чему обеспечивается высокая



точность обнаружения угроз и высокая скорость реагирования на них. Cisco Talos выявляет 1,5 млн уникальных образцов вредоносного ПО и блокирует порядка 20 млрд угроз в день.

### ОТВЕТЫ НА ВОПРОСЫ

— Возможно ли выявить несанкционированный сбор информации об ИТ-инфраструктуре компании с использованием различных техник сканирования (по протоколам ICMP/UDP/TCP) как вне, так и внутри периметра?

— В случае использования традиционных средств ИБ выявить несанкционированный сбор информации об инфраструктуре будет достаточно сложно. Зачастую злоумышленники проводят сканирования, маскируя их в общем потоке трафика, например, проводя практически атомарные сканирования, которые выглядят как единичные неудачные попытки установления соединений. В результате ИБ-службы не уделяют им должного внимания. Стоит понимать, что традиционные системы в целом не предоставляют какого-либо поведенческого анализа трафика, в результате чего крайне сложно определить, является ли данное поведение трафика (необычные IP-адреса/протоколы/потоки/объёмы) отклонением от типового поведения. В случае использования Stealthwatch от администратора не потребуется каких-либо действий, поскольку система автоматически производит детальный анализ получаемых данных сетевой телеметрии, формирует модели поведения потоков трафика, вплоть до учёта взаимодействия конечных точек, в результате чего предоставляется информация по проведённым атакам типа «разведка» (сканирование).

— Если пользователь сети, имеющий разрешения на работу с конфиденциальной информацией, обычно скачивал около 10 Мб в день, вдруг скачал с сервера 100 Гб. Как служба информационной безопасности может узнать об этом?

— Системы класса Data Leak Prevention (DLP) чаще всего контролируют движение информационных потоков, но при этом у таких систем есть технические ограничения по переч-

*NTA системы могут централизованно мониторить передаваемые данные по объёму, направлению, протоколу и другим параметрам вне зависимости от типа ИТ-актива и способа работы пользователей с ним*

ню контролируемых сетевых протоколов. Также есть много различных систем контроля работы пользователей с ИТ-ресурсами, такие как системы аудита файловых серверов, Data Base Monitoring и другие. NTA системы могут централизованно мониторить передаваемые данные по объёму, направлению, протоколу и другим параметрам вне зависимости от типа ИТ-актива и способа работы пользователей с ним. NTA системы в процессе сбора и анализа данных формируют поведенческую модель в контексте протоколов, IP-адресов, приложений и объёмов трафика с использованием машинного обучения для конечных точек и потоков трафика. Они автоматически выявляют и уведомляют о нелегитимных, подозрительных фактах передачи и получения данных как внутри, так и из сетевого контура компаний, в отличие от традиционных систем. В этом заключается их ценность.

— Пользователь заразил свой ноутбук сетевым червём за пределами корпоративной сети и принёс его на работу с дальнейшим подключением к внутреннему защищённому контуру компании. Как службы информационной безопасности узнают об этом?

— Традиционные системы, конечно, могут это выявить. Сетевой червь будет стремиться реплицировать себя на все доступные хосты в сетевом окружении, создавать подключения, в том числе и к другим хостам подсети. Такие активности можно отследить NTA системами за счёт сбора сетевой телеметрии с устройств уровня доступа (коммутаторы, беспроводные точки доступа). Конечно, не всё оборудование обладает возможностью передачи сетевой телеметрии, но можно собирать и анализировать как копии трафика, так и данных syslog и SNMP.

— При попытке извлечь из сети компании конфиденциальную информацию, злоумышленники используют, например, DNS или UDP/53 протоколы путём туннелирования. Как система поможет выявить инцидент и сообщить ИБ об этом?

— Помимо DNS злоумышленники также используют протоколы NTP, SSH и SSL, сейчас начинается процесс перехода на TLS 1.3. Шифрование вредного трафика существенно усложняет процесс выявления атак и вредоносного ПО в сетевом трафике. Опираясь исключительно на традиционные средства обеспечения ИБ неэффективно именно по причинам использования сигнатурного подхода. Тот же Stealthwatch позволяет выявлять подобные инциденты путём анализа объёма передаваемых данных в привязке с используемым типом протокола, порта, источника, получателя и направления трафика.

\* \* \*

NTA системы — неотъемлемая часть многоуровневой, современной системы обеспечения ИБ, позволяют получить полноценную видимость и аналитику не только сетевого трафика, но и общего состояния защищённости ИТ-инфраструктуры в целом. Эксперты СТИ в своих проектах всегда рекомендуют использовать NTA системы, поскольку их наличие в СОИБ позволяет выявить как текущие, так и потенциальные, скрытые угрозы, получить подробную и ясную картину по текущей ситуации с защищённостью ИТ-инфраструктуры заказчика, существенно сократить время расследования инцидентов, обеспечить всесторонний контроль сегментации сети и функционирования политик межсетевого взаимодействия.





**Павел КОРОСТЕЛЕВ**  
эксперт компании  
«Код безопасности»

# КОНЦЕПЦИЯ НУЛЕВОГО ДОВЕРИЯ

## ОСНОВА СИСТЕМЫ ЗАЩИТЫ ИТ-ИНФРАСТРУКТУРЫ

**И**сторически, при создании инфраструктуры, любая организация подходила к вопросу защиты информации, условно, как к крепости, т.е. существовал периметр, окружённый стеной, всё что находилось внутри: сервера, рабочие станции — доверенное. Ещё десять лет назад этот подход прекрасно справлялся с поставленными задачами. Проблемы начали появляться, когда потребовалось обеспечивать доступ к приложениям из Интернета, а также удалённый доступ пользователей к внутренним сервисам. Для решения вопросов защиты инфраструктуры появилась концепция «демилитаризованной зоны», когда существовало некоторое количество приложений доступных из Интернета, но отделённых от внутренней инфраструктуры. Если такие приложения были скомпрометированы, они никак не могли повлиять на безопасность внутренней инфраструктуры в целом.

### СЕГМЕНТАЦИЯ — ЗАМЕЧАТЕЛЬНО, НО ДОРОГО...

С приходом в нашу жизнь новых технологий появилась необходимость удалённой работы пользователей, которые находятся за пределами нашего периметра и им необходимо получать прямой доступ к своим приложениям. Были созданы VPN-шлюзы и VPN-

клиенты — системы защищённого удалённого доступа, обеспечивающие доступ внутрь периметра. Также появилась концепция сегментации, при которой сетевая инфраструктура разделялась на несколько частей по критерию значимости, например, пользователи отделяются от серверной инфраструктуры. Однако, если снаружи поставить межсетевой экран стоило сравнительно недорого, потому что пропускная способность интернет-канала не должна быть высокой, то внутренние требования к пропускной способности межсетевого экрана очень высокие, его же стоимость вырастала экспоненциально. Именно поэтому концепция сегментации, при всей её очевидной необходимости, далеко не всегда реализовывалась. Компания «Код безопасности» недавно проводила исследование, по которому 68 % респондентов утверждает, что сегментация — это один из ключевых подходов к обеспечению безопасности ИС, но при этом очень дорогой, опасной и снижает надёжность современных ИТ-инфраструктур.

### РАЗРУШЕНИЕ ПЕРИМЕТРА

Ещё один сложный момент заключался в том, что часть приложений перемещается из корпоративных ЦОДов в публичное облако, а значит концепция, когда мы доверяем всему, что находится внутри и не доверяем всему, что находится снаружи, больше не работает. Разрушение периметра сети вызвало

много изменений и стало необходимо разработать новые подходы к кибербезопасности.

### КАК ОБЕСПЕЧИТЬ ДОВЕРИЕ?

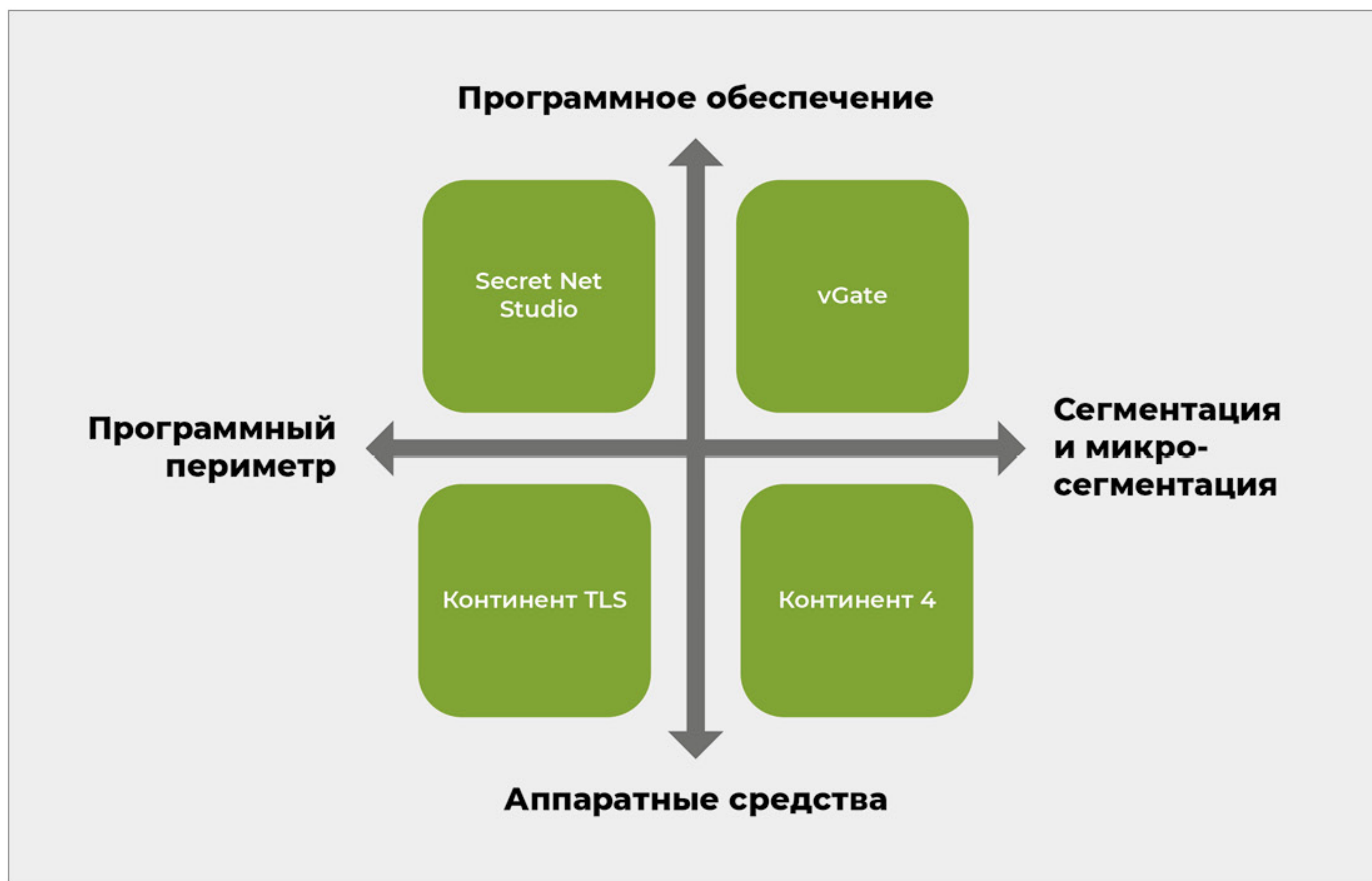
Концепция нулевого доверия как раз и стала одной из самых популярных технологий безопасности, демонстрирующая растущий интерес в отрасли. Данная концепция предлагает способ проектировать безопасность в сердце бизнес-процессов, увязывая человека с технологией. Использование концепции нулевого доверия создаёт прочную основу для проектирования безопасной ИТ-инфраструктуры. Эта основа состоит в том, чтобы обеспечить доверие путём проверки ваших пользователей и устройств, а также динамического анализа их состояния. Таким образом, отсутствие периметра не имеет значения, поскольку создаётся новый микропериметр, который более точно отражает современное движение данных.

Принадлежность к тому или иному периметру в этом случае определяется не сетевым адресом, а совокупностью успешных проверок на соответствие требованиям безопасности.

### ЧЕТЫРЕ СЦЕНАРИЯ

Нулевое доверие основано на предпосылке, что злоумышленники существуют как внутри сети, так и за ее пределами, поэтому автоматически нельзя доверять ни одному пользователю или устройству, и здесь можно выделить четыре сценария.





Реализация концепции нулевого доверия с помощью продуктов «Кода безопасности»

**Первый** — защита внешнего периметра сети. В этом сценарии необходимо защитить сеть от атак из интернета, обеспечить контроль доступа пользователей в интернет и защитить их от вредоносных сайтов. К этому же сценарию относится создание защищённых каналов связи с использованием российских алгоритмов.

**Второй** — внутренняя сегментация сети. Здесь необходима очень высокая производительность и способность работать с очень подробной политикой безопасности без падения производительности.

**Третий** — микросегментация виртуализированной сети. Это отдельный кейс, связанный с высокой изменчивостью виртуальной среды и необходимостью создавать виртуальные сегменты на «атомарном уровне» — уровне одной или нескольких виртуальных машин. И, опять же, без влияния на пропускную способность или топологию сети. Высокая изменчивость инфраструктуры приложений в этом кейсе требует исключительно высокой гибкости при управлении доступом.

**Четвёртый** — на уровне пользователей имеет смысл реализовать механизм нулевого доверия при подключении к серверу. В этом случае на уровне рабочих станций перед разрешением подключиться к серверу приложений мы проверяем пользователя, компьютер, с которого он подключается и приложение, которое он использует. Если хотя бы одно из этих условий не соблюдается — пользователь не получит доступа к серверу.

Комбинация этих сценариев значительно затруднит проникновение, а также горизонтальное распространение злоумышленника в локальной сети. Чем сложнее будет злоумышленнику проникать из сегмента в сегмент, тем больше шансов у компании его остановить.

Все эти сценарии можно реализовать с помощью набора продуктов компании «Код безопасности». Континент 4 — Первый российский многофункциональный межсетевой экран (UTM) с поддержкой шифрования по российским алгоритмам ГОСТ, Secret Net Studio и ПАК «Соболь» — комплексное

решение для защиты рабочих станций и серверов от несанкционированного доступа со встроенным межсетевым экраном уровня хоста и авторизацией сетевых соединений, а также vGate — средство микросегментации сегментации частного облака, контроля активности администратора виртуальной среды и контроля соответствия настроек безопасности частного облака требованиям регуляторов.

\* \* \*

На самом деле нулевое доверие — это динамический анализ уровня безопасности и адаптивная настройка политики доступа в зависимости от этого уровня. Внедрение этого подхода обеспечивает защиту ИТ-инфраструктуры, минимизирует количество инцидентов ИБ и повышает скорость локализации все же случившихся инцидентов. В свою очередь, это является залогом безопасной цифровой трансформации финансовых организаций.





**Яна АНДЖЕЛЛО**  
менеджер по продукту  
Центра управления сервисами  
Группы компаний Angara

# КАК ВЫБРАТЬ ПРОВАЙДЕРА MSS?

**Э**волюция угроз неминуемо ведёт к необходимости защиты активов компании. По данным Всемирного экономического форума<sup>1</sup>, кибератаки входят в ТОП-5 глобальных рисков с точки зрения вероятности их реализации, наряду с мошенничеством и кражей данных. Финансовые потери от реализации рисков информационной безопасности (ИБ) растут ежегодно, не говоря уже о репутационном ущербе. Согласно статистике компании International Data Corporation<sup>2</sup>, расходы на ИБ в мире растут со скоростью, примерно равной 9–10 % в год, и это неслучайно.

## ЧТО ТАКОЕ MSSP?

Параллельно с усложнением угроз, средства защиты информации (СЗИ) переживают серьёзную эволюцию. Современные СЗИ содержат в себе разнообразные механизмы — от продвинутых способов анализа данных до телеметрии и искусственного интеллекта. Теперь, чтобы организовать действительно надёжную защиту, нужно иметь в своём штате высококвалифицированных специалистов, глубоко разбирающихся в типах и способах настройки СЗИ, которые отличаются большим разнообразием. Компании решают эту проблему по-разному. Крупные игроки рынка предпочитают создать свой

«центр компетенций» и сознательно «играют в долгую», инвестируют в современные СЗИ и развитие сотрудников. Небольшие компании используют MSS (Managed Security Service) — услуги провайдера или аутсорсинг для решения задачи ИБ, а часть компаний только начинает задумываться над этим вопросом.

Согласно статистике<sup>3</sup>, средняя заработная плата специалиста по ИБ составляет 80 000 рублей в Москве и около 50 000 рублей в других городах России. А теперь давайте представим, что таких специалистов для обслуживания средней компании (от 100 до 500 человек) нужно как минимум трое. Ландшафт угроз требует квалифицированных специалистов и наличия опыта в области ИБ, однако существует большая сложность в поиске таких кадров.

В связи с этим, последнее время различные организации чаще обращаются к услугам управляемых служб безопасности. Следует отметить, что большинство сервис-провайдеров предоставляет услуги в режиме 24×7×365 — далеко не каждая компания способна собственными силами организовать круглосуточную работу даже ИТ, не говоря уже об ИБ-специалистах.

Впервые сталкиваясь с MSSP (Managed Security Service Provider), кажется, что это современный тренд. Но история MSSP началась в далёком 1997 году, когда компания US West, Inc. вывела на рынок услугу по VPN-шифрованию,

основанную на решении Check Point Firewall-1. До вывода услуги на рынок компания около года занималась её тестированием. Современные MSSP не менее тщательно подходят к выпуску своих сервисов.

## ПРИВЛЕКАТЕЛЬНЫЕ ОСОБЕННОСТИ

Какие же есть особенности у MSSP, что делает использование услуг провайдеров особенно привлекательным? Почему эта модель становится всё более и более популярной?

### Характерные особенности MSSP:

#### 1. Высокие требования к обеспечению безопасности.

Все устройства и технологии, которые хранят и передают конфиденциальные данные компании, требуют повышенных мер обеспечения ИБ. Сегодня ведущие облачные провайдеры инвестируют в передовые инструменты и процедуры безопасности, например, двухфакторная аутентификация или даже биометрический доступ, организация пропускного режима и резервные источники питания. Эти инвестиции предназначены для защиты данных и бизнеса. Могут ли внутренние центры обработки данных иметь такой же уровень безопасности?

#### 2. Проактивный подход к ИТ-задачам.

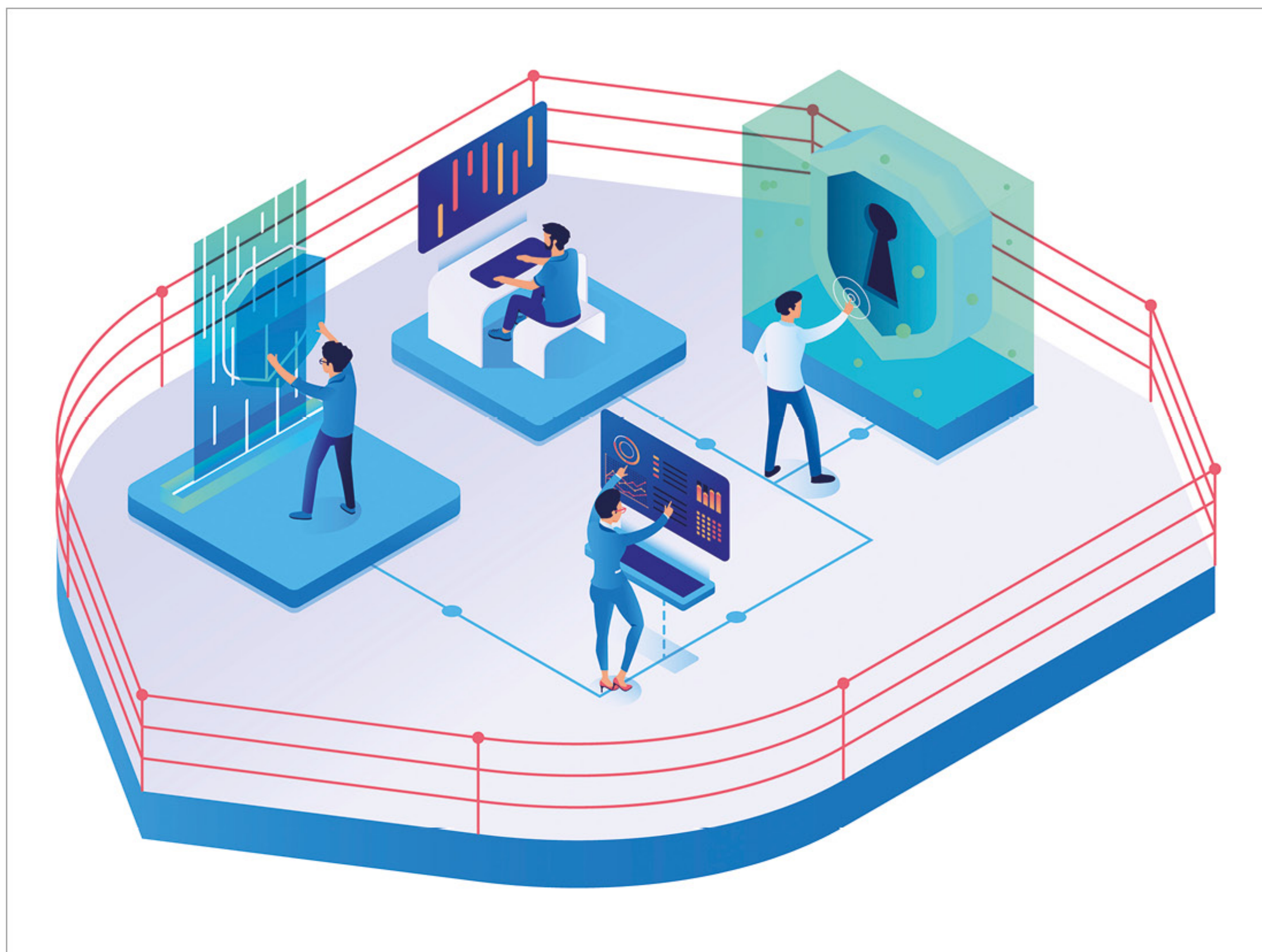
Для обслуживания, резервного копирования и мониторинга сред приложений требуются дорогостоящие ИТ-ресурсы и опыт. А если эти приложения критичны для бизнеса? С партнёром

<sup>1</sup> <https://bcs-express.ru/novosti-i-analitika/top-5-global-nykh-riskov-v-2019-godu-po-mneniiu-vsemirnogo-ekonomicheskogo-foruma>

<sup>2</sup> <https://www.idc.com/getdoc.jsp?containerId=prUS44935119>

<sup>3</sup> <https://ru.indeed.com/salaries/cneцyалuцm-по-информационной-безопасности-Salaries-Москва-MOS>





вы получаете доступ к ряду сертифицированных инженеров и архитекторов, что позволяет сосредоточиться на более важных задачах, которые непосредственно влияют на рост бизнеса и доходов компании.

**3. Максимальное время безотказной работы.**

В условиях постоянно меняющегося мира компании нуждаются в непрерывности бизнеса, потому что каждое прерывание деятельности стоит денег. Роль MSSP включает в себя выявление и предотвращение событий, влекущих простой систем заказчика.

**4. Доступ к самым новым технологиям и оптимальный выбор продукта для сервиса.**

Бизнес-модель управляемых услуг хорошо подходит, если в компании имеется ряд областей, в которых внутренние службы, а именно ИТ и ИБ-отделы, пытаются «играть в догонялки» или за-

*Большинство сервис-провайдеров предоставляет услуги в режиме 24×7×365 — далеко не каждая компания способна собственными силами организовать круглосуточную работу даже ИТ, не говоря уже об ИБ-специалистах*

нимаются «перетягиваем каната». Провайдер может проконсультировать и предложить клиентам новейшие технологии, обеспечивающие бесперебойную работу и рентабельность. В некоторых случаях замена продукта, на котором оказывается услуга, может происходить совершенно бесплатно для клиента, так как всё обслуживание берёт на себя сервис-провайдер. Кроме того, компании не придётся ждать, если у неё внезапно появились новые требования. Как правило, провайдер может

помочь изменить уровень предоставления услуги без каких-либо проблем.

**5. Рентабельность инвестиций и экономия средств.**

Самая большая ценность для бизнеса — это экономия затрат. При росте бизнесу не нужно думать, как масштабировать мощности или сколько и каких новых сотрудников нанять в отдел ИБ. Расширение услуг сервис-провайдера происходит для клиента легко и только тогда, когда эта необходимость назрела.



## НО ЕСТЬ И РИСКИ

Вместе с плюсами есть ряд рисков, связанных с MSSP:

### 1. Неспособность оценить свои «сильные» и «слабые» стороны в обеспечении безопасности.

Компания должна, с одной стороны, понять свои собственные возможности, чтобы обоснованно выбрать подходящего MSS-провайдера, который действительно сможет помочь устранить пробелы. С другой стороны, необходимо оценить сильные и слабые стороны MSSP, чтобы убедиться, что провайдер соответствует предъявляемым требованиям. Например, не стоит дублировать функции уже существующих ИБ-специалистов. С другой стороны, если ваш специалист, например, по WAF, тратит на его настройку 50% рабочего времени, то, возможно, провайдер смог бы снять с него эту ответственность, а компания получила бы возможность решать более важные задачи ИБ.

### 2. Предполагать, что провайдер знает, как работают ваши внутренние системы, или моментально в них разберётся.

Иногда компании совершают ошибку, слишком полагаясь на MSSP. Чтобы понять внутреннюю ИТ-среду компании и то, как она работает, потребуются время и опыт. Если компания не будет управлять своими бизнес-процессами, проводить оценку рисков и периодически пересматривать проводимую работу, то есть шанс, что всё пойдёт наперекосяк.

Например, MSSP вряд ли узнаёт о планируемых изменениях, если компания сама об этом его не проинформирует. Более того, часто отсутствие доступа и информации о ключевых системах или отдельных лицах препятствует быстрому подключению MSSP и может резко снизить эффективность провайдера в целом. Именно поэтому важно

наладить постоянное взаимодействие между клиентом и поставщиком услуги. Не задействовать ИТ-команду при подключении к MSSP также является ошибкой, так как области ИТ и ИБ тесно связаны. Особенно, если на команду ИТ были возложены задачи по обслуживанию систем ИБ.

### 3. Не понимать, на что вы подписались.

Иногда услуги MSSP описаны таким образом, что клиент не сразу понимает, как будет фактически предоставляться услуга. Например, как будет отслеживаться использование облачных сервисов? Возможно ли подключение дополнительных опций или услуг у текущего провайдера? Если компания планирует развитие в сторону расширения договора с сервис-провайдером, ей стоит заранее узнать состав услуг MSSP и их планируемое расширение или изменение.

### 4. Не принимать во внимание ограничения по интеграции и аналитике.

Если у компании уже имеются средства общей аналитики, то стоит заранее уточнить возможности MSSP по интеграции с ними. Часто у клиента может возникнуть потребность «подружить» технологии, но на практике он может столкнуться с ограниченными возможностями интеграции. Эта же проблема может возникать при взаимодействии с экосистемой MSSP-поставщиков. Как обеспечить интеграцию двух или трёх сервис-провайдеров? Об этом стоит подумать заранее.

Кроме того, в таких сложных сервисах как SOC (Security Operations Center), при отсутствии достаточной интеграции, многие предупреждения MSSP могут не иметь контекста или значения и могут вынуждать сотрудников заказчика проводить дополнительные работы, проверяя и перепроверя каждое полученное предупреждение о потенциальной угрозе.

### 5. Не проверять безопасность MSSP.

Не исключено, что злоумышленники могут попытаться проникнуть в MSSP-системы и сети, чтобы затем получить доступ к системам клиентов провайдера. В некоторых из подобных инцидентов атакующие использовали «слабые» места в средствах удалённого администрирования, которые MSSP используют для получения доступа к своим клиентским системам. Одним из наиболее известных примеров является китайская кампания APT10 threat group Operation Cloud Hopper, ориентированная на сотни провайдеров по всему миру.

Злоумышленники знают, что компрометация одного управляемого поставщика услуг достаточна для получения доступа ко многим клиентским сетям. Ввиду того, что MSSP могут являться «точкой входа» для злоумышленников, они должны соответствовать самым высоким стандартам безопасности.

## РИСКИ УСТРАНИМЫ

Многие из перечисленных рисков можно устранить на этапе оценки провайдера, но необходимо хорошо понимать, что именно нужно проверить. Вопросы для такой проверки должны касаться инструментов и процессов, которые использует провайдер, уровня квалификации сотрудников провайдера, принятой системы повышения квалификации. Также целесообразно выяснить, как провайдер планирует снижать тот или иной риск ИБ в условиях работы вашей компании.

\* \* \*

Опрос Forrester Research показал, что лучшие результаты взаимодействия с MSSP достигаются, когда компания имеет чёткое представление о своих собственных возможностях и предъявляет конкретные требования к поставщику услуг. При этом важно, чтобы эти требования были установлены заранее и оперативно пересматривались в зависимости от изменений, происходящих в области ИБ, а также в работе компании и провайдера услуг.

*Компания должна понять свои собственные возможности, чтобы обоснованно выбрать подходящего MSS-провайдера, который действительно сможет помочь устранить пробелы*





**Алексей КУРСКИХ**  
руководитель направления  
Pre-sale по ИБ, ARinteg

*«Здесь, знаешь ли, приходится бежать со всех ног, чтобы только остаться на том же месте. А чтобы попасть в другое место, нужно бежать в два раза быстрее»  
Л. Кэрролл, «Алиса в Зазеркалье»*

# ОЧЕВИДНЫЕ И НЕОЧЕВИДНЫЕ

## ПРЕИМУЩЕСТВА СЕРВИСНОЙ МОДЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**К**огда возникает вопрос об управлении, модернизации или поддержке систем информационной безопасности на предприятии, как правило, за этим следует закономерный второй вопрос — кто это будет делать? Что в итоге выбрать заказчику — выполнение работ внутренним сотрудником или внешним подрядчиком? Рассуждать на подобные темы лучше всего, основываясь на практике.

Когда мы приезжаем к заказчику и предлагаем ему сделать что-либо внешними силами, то есть нашими сотрудниками, обычно я слышу: «Да, это здорово. Это очень здорово, но...». Далее следуют типичные «но»:

### «НО ЭТО НЕНАДЁЖНО / НЕТ ОТВЕТСТВЕННОСТИ»

Кажется, что внешний сотрудник — это не очень надёжно. Вернее, очень ненадёжно. Здесь обычно сравнивают своего сотрудника, специалиста в штате компании, и конкретного исполнителя, который придёт лично выполнять работу или будет делать её удалённо. Сравнение совершенно некорректное. В случае с внутренним сотрудником ответственность за выполненную работу несёт именно он, т.е. ваш внутренний специалист. В случае заключения договора с аутсорсинго-

вой компанией ответственность несёт не человек. В том смысле, что не тот человек, который пришел к вам что-то делать. Это очень важный момент. Ответственность несёт юридическое лицо, то есть фактически директор или тот, кто подписал договор об аутсорсинге или выполнении сервисных работ со стороны этого юридического лица. Он и только он несёт настоящую ответственность. Она гораздо круче и сильнее, чем, если за это отвечает простое физическое лицо, которого вы взяли на работу. Это не стоит недооценивать.

Если вы повысите голос на штатного сотрудника или перегнёте палку, или ему надоест работа, он посчитает, что у него недостаточно высокая зарплата, или еще что-то, то он напишет заявление, и через две недели этот сотрудник у вас не работает. Этим ваши с ним отношения закончатся. Ничего существенного вслед ему вы сделать не сможете. Если ваш специалист устанавливал или настраивал какое-то дорогостоящее оборудование и сломал его, никто не возместит вам расходы. Вы просто вынуждены будете докупить это в организацию. С физического лица практически невозможно что-либо взыскать, чтобы компенсировать убыток от его деятельности. В случае договора с юридическим ли-

цом возместить можно — финансово, дополнительными работами, сервисами и т.д. Это важно. При заключении правильного договора возможно практически всё.

### «У НАС СВОЯ СПЕЦИФИКА. ВЫ НИЧЕГО НЕ СДЕЛАЕТЕ»

Своей специфики не бывает в принципе. Компьютеры и сети везде одинаковые. Серверы делают на одном и том же заводе в одной и той же стране. Бывает, когда «мы так исторически построили инфраструктуру». Вот это, действительно, бывает часто и повсеместно. Вы так строили инфраструктуру потому, что не подразумевали, что она будет обслуживаться внешним специалистом. Вот и всё. Давайте переделывать.

### «ЭТО НЕВЫГОДНО»

Тут вообще всё просто, без гипотез и эмоций, это обычный экономический расчёт. Предположим, у нас есть три сотрудника с зарплатой 50 000 рублей, и мы им платим в месяц суммарно 150 000 рублей, тогда мы на них тратим в год 2 400 000 рублей.

Если мы платим те же самые 150 000 рублей в месяц внешней компании за её услуги, мы тратим 1 420 000 рублей в год. Получается разница в миллион в пользу аутсорсинга.



50 000 рублей — это средняя зарплата сотрудника ИБ по стране, общедоступная информация из открытых источников.

### **«У НАС ПОЯВИЛСЯ НОВЫЙ ОБЪЁМ РАБОТЫ, МЫ НАЙМЁМ ЕЩЁ СОТРУДНИКОВ»**

На самом деле они у нас, как у поставщика услуг, уже есть. Не надо никого искать, надо просто оценить объём работ и добавить в договор.

В договорах на аутсорсинг можно и нужно прописывать работы по заявкам. Если у вас, как у заказчика, в течение года возникает что-то неожиданное или требующее новых сотрудников, как правило, это заканчивается суетой с участием отдела кадров, сайтов по подбору персонала, выделением рабочих мест или оборудования, сбором коммерческих предложений, попыткой протестировать компанию, выяснить компетенции сотрудников. В случае заключения договора на аутсорсинг в нём достаточно указать возможность работы по заявкам и заранее оценить час работы соответствующего специалиста. Когда договор заключён, вы при необходимости оформляете заявку, и через два дня у вас всё сделано.

### **«МЫ ИХ ОБУЧИМ»**

Да, без обучения в ИБ вообще никак. Если специалист ИБ не учится, он отстаёт. Он как бы ничего не делает, но при этом движется назад. Мы, как системный интегратор, постоянно обучаем сотрудников. Это бесконечный и необходимый процесс. В случае аутсорсинга вы сразу получаете обученных специалистов.

### **ЮРИДИЧЕСКИЕ АСПЕКТЫ**

Здесь вообще одни плюсы. Заключение договора с юридическим лицом закрывает вопрос с ответственностью. В трудовом договоре практически нереально подписать SLA (ServiceLevelAgreement — соглашение об уровне сервиса), или это будет выглядеть очень бедно. Трудовой кодекс вкупе с гражданским довольно сильно ограничивают возможности работодателя по составлению трудовых договоров. Даже если работодатель впишет в трудовой договор пункты, ко-

торые ему очень нравятся, в случае противоречия с ТК РФ есть вероятность признания их ничтожными.

NDA (Non-disclosure agreement) — соглашение о неразглашении конфиденциальной информации) обычно заканчивается коммерческой тайной. Без правильной правовой поддержки режим коммерческой тайны в компаниях обычно выглядит совершенно неправильно. Как пример, первое, что нужно делать при режиме коммерческой тайны, — это как минимум менять устав организации. Об этом все забывают. А комплекс мер должен быть довольно большим. В случае с физическим лицом всё, что вы сможете взыскать с сотрудника, который нарушил вашу коммерческую тайну и что-то где-то разболтал, — это по факту ничего. Это просто бумажка.

### **СТРАХОВАНИЕ РИСКОВ**

Тут нам, как поставщику услуг, проще смотреть на мир. У нашей компании есть возможность застраховать работы, сделки и пилотные проекты. Мы с нашим партнёром — страховой компанией можем застраховать нашу деятельность на приличную сумму — от 10 млн рублей, чего нельзя сделать в работе с физическим лицом. С человеком можно максимум застраховать его здоровье.

### **БОЛЕЕ ОТВЕТСТВЕННЫЙ АУДИТ**

Аудит внешней компанией — это всегда здорово, потому что именно этот аудит является непредвзятым и более независимым. Мы не создавали вашу IT-инфраструктуру, поэтому мы можем проверить её непредвзято. В случае со штатным сотрудником это называется «самооценкой». Она всегда грустная. Человеку приходится отчитываться за то, что он сделал. А после этого там ещё работать. Давайте посмотрим правде в глаза, когда мы сами отчитываемся за нашу работу, мы её частенько приукрашаем. А вот если есть желание получить неприукрашенный аудит, надо звать кого-то со стороны.

### **КАК ВЫБРАТЬ КОНТРАГЕНТА**

Допустим, вы согласились со всеми предыдущими пунктами, пришли к тому, что, да, надо попробовать аутсорсинг.

Понимаете, что работы будут осуществлять более квалифицированные и опытные специалисты, чем у вас сейчас есть. Вы определились с бюджетом. Теперь надо найти контрагента. Правильно выбрав контрагента, вы сможете получить необходимый уровень ответственности, а вместе с этим уровень обслуживания, гарантию неразглашения коммерческих и прочих тайн. Обратите внимание, что контрагент — это не торговая марка компании, зарегистрированная на всех билбордах, а «ООО», с которым вы будете заключать договор. Вот тут надо внимательно смотреть, чтобы ему было больше, чем 3 дня, чтобы оно сдало хотя бы пару годовых отчётностей, чтобы за ним не было большого количества профильных судов. Понятно, что если юридическое лицо осуществляет коммерческую деятельность, то оно в какие-то тяжбы будет попадать. Корректную оценку контрагента по множественным параметрам, необходимую для принятия решения, как правило, дают сотрудники внутренней службы безопасности.

Именно директор выбранного вами юридического лица, с большим количеством договоров, выручкой, известным именем, будет очень сильно переживать за выполнение договора. Это не просто рядовой сотрудник. В договоре с этим юридическим лицом можно прописывать штрафы и неустойки. Тогда в случае судебного разбирательства оно закончится правильно для вас. Всё становится в разы лучше по сравнению с ответственностью физического лица, которого вы берёте на работу по трудовому договору, и которое уйдёт в течение двух недель, если ему что-то разонравится.

### **УСЛОВИЯ ДОГОВОРА**

Вы просите потенциального аутсорсера прислать форму договора для заполнения, а получаете что-то аналогичное договору на обслуживание с крупным банком. Читаете и понимаете, что в случае чего вы совершенно бесправны, и другая сторона может сделать всё что угодно. Конечно, такой договор не стоит подписывать, а с такой компанией, наверное, дальше не стоит иметь дел. Это будут совершенно неравные условия, несущие риски для бизнеса заказчика.





### РЕАЛЬНОСТЬ ИСПОЛНЕНИЯ ДОГОВОРА

Естественно, договор после подписания не нужно пускать на самотёк и предусмотреть некую систему отчётности, реперные точки.

Есть одна немаловажная особенность. Обычно почему-то подразумевается, что заказчик всегда классный и непогрешимый, а исполнитель всегда пытается обмануть. Смею заверить, заказчики тоже бывают разными. Как правило, стороны, выбрав друг друга, всё же стараются придерживаться исполнения договора, ведь изначально его заключение ведёт к взаимному получению выгоды для обеих сторон. Но иногда что-то идёт не так. Если по вновь открывшимся обстоятельствам исполнение договора будет вести к убыткам для одной из сторон, акцентирую внимание — для любой, то договор должен быть пересмотрен. Именно поэтому в нём следует прописать условия расторжения, указать срок действия и условия пролонгации. Это всегда мотивирует.

### КАК ПРАВИЛЬНО ПЕРЕВОДИТЬ РЕКЛАМНЫЕ ОБЪЯВЛЕНИЯ

Поделюсь своим мнением о некоторых рекламных ходах, используемых для привлечения внимания к аутсорсингу ИБ.

♦ «ИБ/ИТ-аутсорсинг используют только зрелые компании» — обычная техника манипуляции. Когда вам это заявляют, то подразумевается, что вы себя признаёте зрелой компанией и что-то купите.

♦ «Вам нужно аутсорсить именно это» — предлагающая сторона умеет только это. По-хорошему, системный интегратор не должен предлагать «локутное» решение какой-то одной проблемы. Мы стараемся получить больше информации, т.к. одну и ту же задачу можно решить различными методами, двигаясь от запросов бизнеса, а не от локальных задач ИТ/ИБ.

♦ «SOC — это круто» — у компании есть SOC, она старается его продвигать, чтобы окупить. Не факт, что он вам вообще нужен. SOC — это всегда дорого и сложно. Это не антивирус поставить.

♦ «Ответственность будет на нас» — сразу надо смотреть в договор. Там написано, у кого какая ответственность.

### КОГДА БЕЗ ШТАТНОГО СОТРУДНИКА НЕ ОБОЙТИСЬ

Ситуаций, когда всё-таки нужен постоянный сотрудник в штате, довольно немного.

Пожалуй, в основном — это требования регуляторов. Компании, попадающие под их действия, обязаны иметь

штатного специалиста по ИБ с соответствующим профильным образованием и стажем работы.

Разумно иметь своих специалистов на ключевых постах. Конечно, внешними силами можно сделать довольно много. Однако, у организации должны быть свои постоянные сотрудники, которые как минимум создают общую стратегию развития компании и управляют внешними контрагентами. Нанять компанию, которая будет следить за работой других компаний, — идея утопичная с точки зрения прозрачности и надёжности ведения бизнеса.

Когда заказчик использует специфические продукты и технологии, то экономически целесообразно развивать и поддерживать свои компетенции, так как найти подобные услуги на рынке бывает затруднительно.

\* \* \*

Также необходимо брать в штат сотрудников, если вы полностью уверены, что они от вас никогда не уйдут, будут выкладываться на 110%, не будут приукрашивать данные в отчётах, будут совершенно незаменимы, и не станут просить прибавки к зарплате.





**Николай ФОКИН**  
руководитель направления  
противодействия  
мошенничеству BI.ZONE

# ЦИФРОВОЙ ПРОФИЛЬ: ИНФОРМАЦИЯ НА СТРАЖЕ ДЕНЕГ

BI.ZONE CLOUD FRAUD PREVENTION — КОМПЛЕКСНЫЙ ПОДХОД К ЗАЩИТЕ ОТ БАНКОВСКОГО МОШЕННИЧЕСТВА

**Т**ехнологии в наши дни развиваются стремительно, всё глубже проникают в повседневную жизнь, а вот киберграмотность распространяется гораздо медленнее, и этот дисбаланс успешно используют мошенники. Они предпочитают идти по пути наименьшего сопротивления, а в финансовом секторе легче всего получить доступ к деньгам, атакуя отдельных клиентов, а не сам банк. Одним из самых действен-

ных инструментов в арсенале киберпреступников становится социальная инженерия.

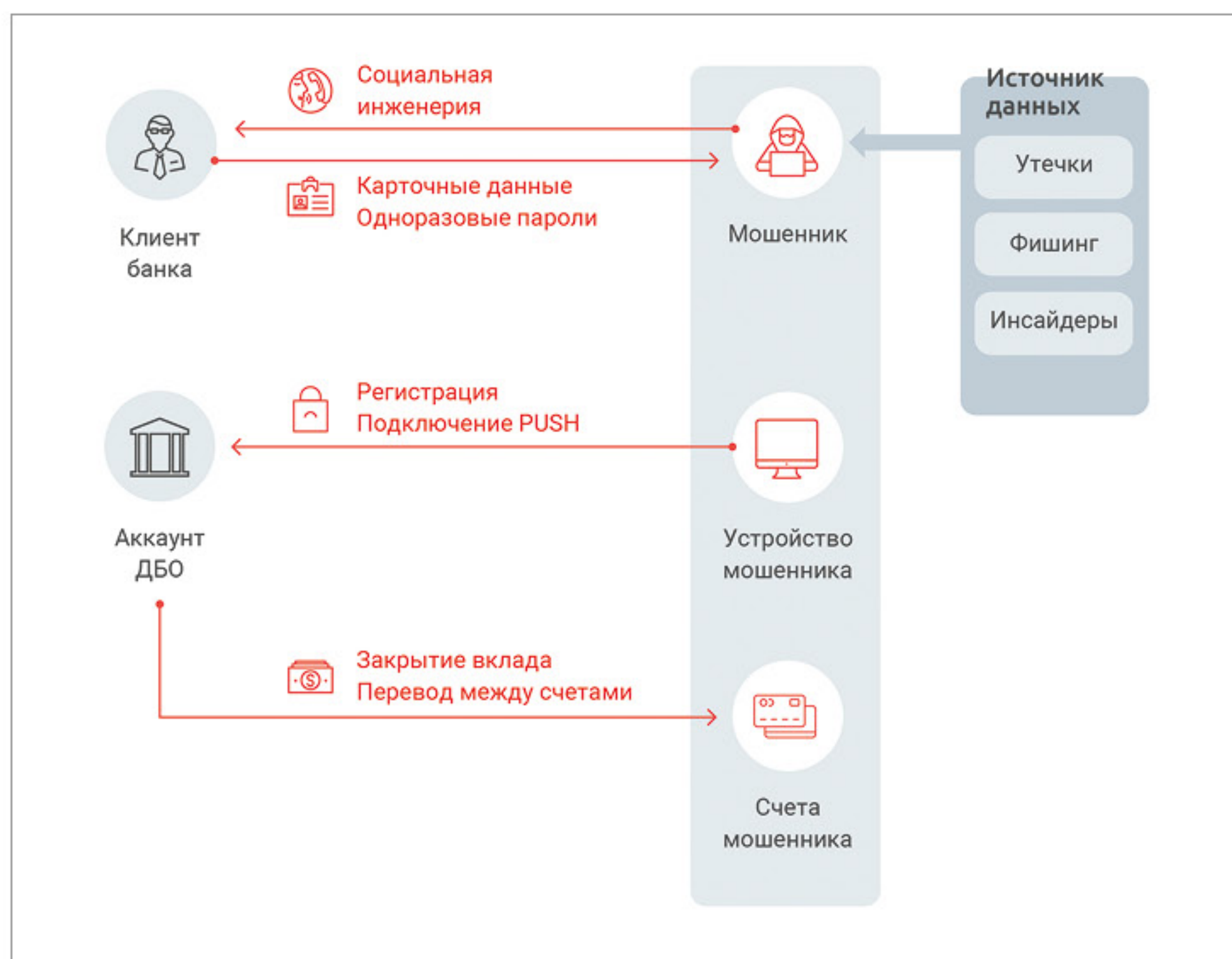
По данным исследования Threat Zone '19, в России она используется при 80% атак на клиентов банков. В большинстве случаев жертвы поддаются на уловки мошенников, передают им свои персональные и платёжные данные, и даже сами переводят средства на счета злоумышленников. Также играет на руку киберпреступникам и повсемест-

ное распространение мобильных платежей, которые, с одной стороны, удобны для клиентов банков, а с другой — делают возможными новые мошеннические схемы.

## КАК ПРОИСХОДИТ АТАКА

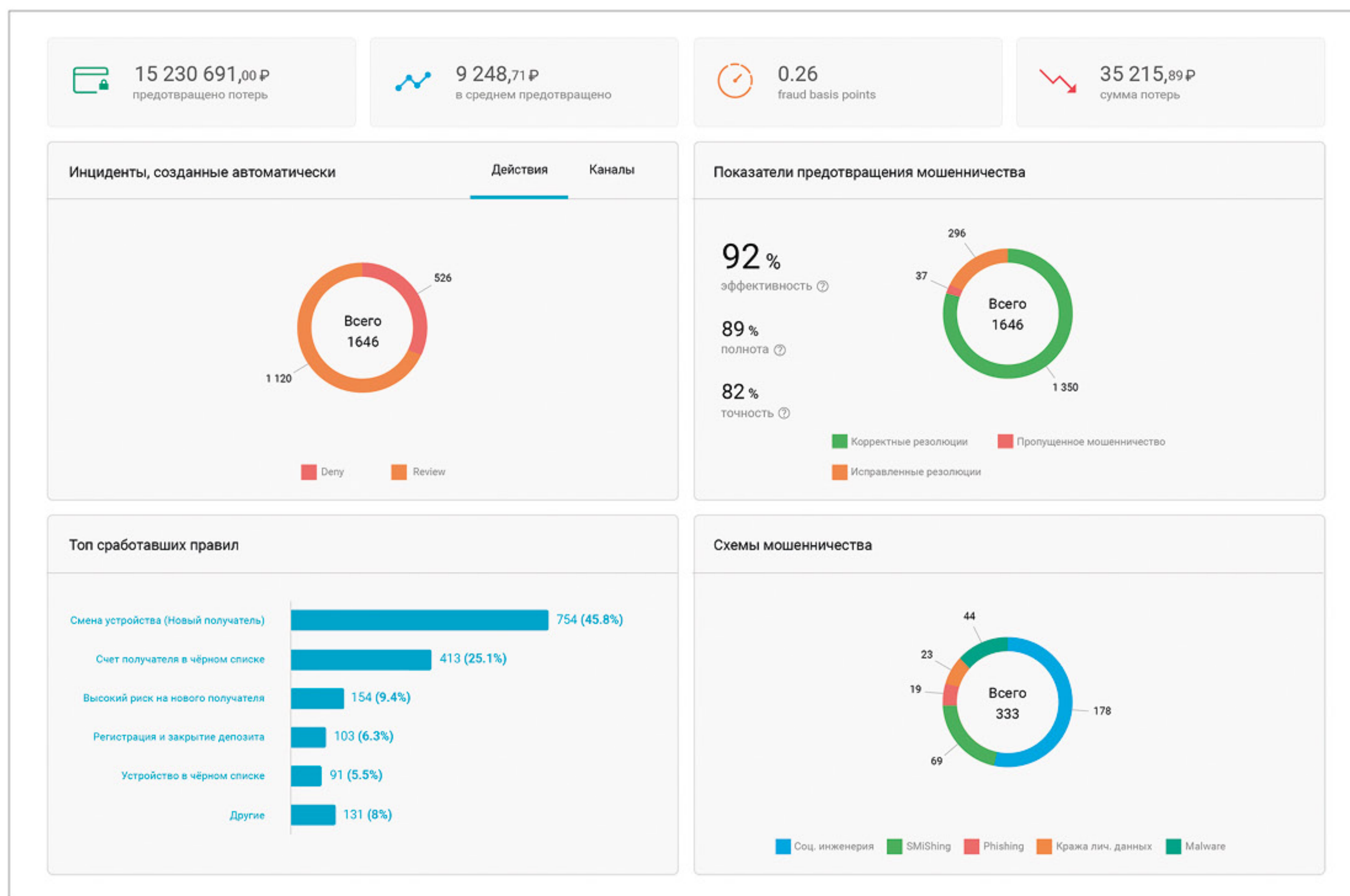
Главное для злоумышленников — втереться к жертве в доверие, для чего они используют самые разные подходы. В последнее время мошенники всё чаще представляются сотрудниками банка, в котором у их собеседника есть счёт. Чтобы сделать общение с «клиентом» максимально реалистичным, киберпреступники нередко используют личную информацию, купленную в даркнете. За неё, между прочим, просят не такие уж большие деньги: обширную подборку данных о человеке, включая сканы паспортов, водительского удостоверения и других важных документов, можно приобрести всего за \$50.

Вооружившись необходимой информацией, мошенник способен довольно правдоподобно замаскироваться под сотрудника банка. После этого конкретные сценарии обмана могут быть различными. Например, жертве сообщают о подозрительной транзакции, которую кто-то якобы пытался совершить с её счёта, и советуют немедленно перевести деньги на «резервный счёт». Естественно, на самом деле доверчивый клиент собственными руками отдаёт средства мошенникам.



Типовой сценарий мошенничества





Пример статистики по угрозам в BI.ZONE Cloud Fraud Prevention

Иногда злоумышленники звонят жертве и, представляясь сотрудниками службы безопасности банка, под различными предлогами просят установить на компьютер или смартфон программу для получения удалённого доступа к устройству. Позже она позволит мошенникам перехватить пользовательскую сессию в онлайн-банкинге и завладеть деньгами.

Заручившись доверием жертвы, можно убедить её раскрыть информацию о банковской карте и одноразовый код подтверждения из СМС. Это даёт злоумышленникам возможность вывести средства, либо токенизировать карту в Apple Pay или другой системе, а затем использовать для покупок. По такой схеме, к примеру, часто крадут деньги у продавцов на торговых онлайн-площадках.

Вариантов обмана множество, и тут всё ограничивается только фантазией мошенников. Жертве могут сообщить про выигрыш в лотерею, предложить удалённую работу в интернете и

т.д. Нередки и случаи, когда социальная инженерия используется в сочетании с фишингом.

### КАК ЗАЩИТИТЬ КЛИЕНТА ОТ МОШЕННИЧЕСТВА

Чтобы защищаться от киберпреступников, финансовым организациям необходимо не только повышать среди клиентов киберграмотность, но и вооружиться современной антифрод-системой. Это решение, которое проверяет все пользовательские операции, оценивая при помощи различных аналитических механизмов степень риска того, что транзакцию на самом деле пытаются провести злоумышленники.

Если оценка риска слишком высока, банку следует приостановить операцию, чтобы связаться с клиентом и получить от него дополнительное подтверждение. Уже по результатам общения с клиентом сотрудник контакт-центра принимает решение, разрешить проведение транзакции или отклонить её как мошенническую.

Именно такой подход мы используем при разработке BI.ZONE Cloud Fraud Prevention (BCFP). В то же время наша система обладает рядом дополнительных и уникальных функций. Это, например, омниканальный мониторинг: в список поддерживаемых каналов обслуживания входят интернет- и мобильный банк как для физических, так и для юридических лиц, а также платёжные карты — эмиссия, торговый эквайринг, электронная коммерция.

Для анализа транзакций применяются не только заранее настроенные правила, но и модели машинного обучения. Важная роль в функционировании BCFP отводится и людям: работу системы сопровождают опытные аналитики и специалисты по data science. Наконец, система наглядно визуализирует основные показатели эффективности своей работы, помогает отслеживать актуальные тренды угроз и видеть объём предотвращённых убытков.

BCFP — это облачная система, что значительно снижает затраты на её вне-



дрение и сокращает операционные издержки на обслуживание и эксплуатацию, а также даёт возможность более оперативно получать данные об угрозах и экспертную поддержку.

### КАК ПРИМЕНИТЬ ДАННЫЕ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Одна из ключевых особенностей ВСФР — построение для каждого клиента цифрового профиля, в котором учитывается множество факторов. К примеру, система отслеживает цифровые отпечатки устройств, с которых производятся операции, то есть совокупность параметров, которые можно использовать как уникальный идентификатор устройства.

При этом ВСФР обращает внимание на окружение пользователя, отслеживает изменения и оценивает, насколько типичны характеристики каждой пользовательской онлайн-сессии, такие как сетевое соединение и геолокация. ВСФР принимает в расчёт репутационные характеристики пользовательских атрибутов: реквизиты, устройства, IP-адреса. Но этим дело не ограничивается, так как система отслеживает паттерны поведения клиента при совершении операций, чтобы выявлять нехарактерные для пользователя действия.

В течение пользовательской сессии система в реальном времени анализирует данные, чтобы выявлять аномалии, которые могут свидетельствовать о мошеннической активности. Здесь речь идёт в том числе об атаках с использованием вредоносного ПО (эмуляторы, средства удалённого управления и т.д.). Важно отметить, что ВСФР работает только с обезличенными данными в соответствии с требованиями законодательства. Профили создаются и для торговых точек, что даёт понимание, насколько для каждой из них характерна та или иная операция.

Обладая таким количеством данных о клиенте и его цифровом окружении, банки могут не только усложнять жизнь мошенникам, но и упрощать её честным пользователям. К примеру, если при обнаружении каких-то аномалий можно добавить дополнительные шаги для верификации, то в обратной ситуации, когда клиент ведёт себя абсолютно

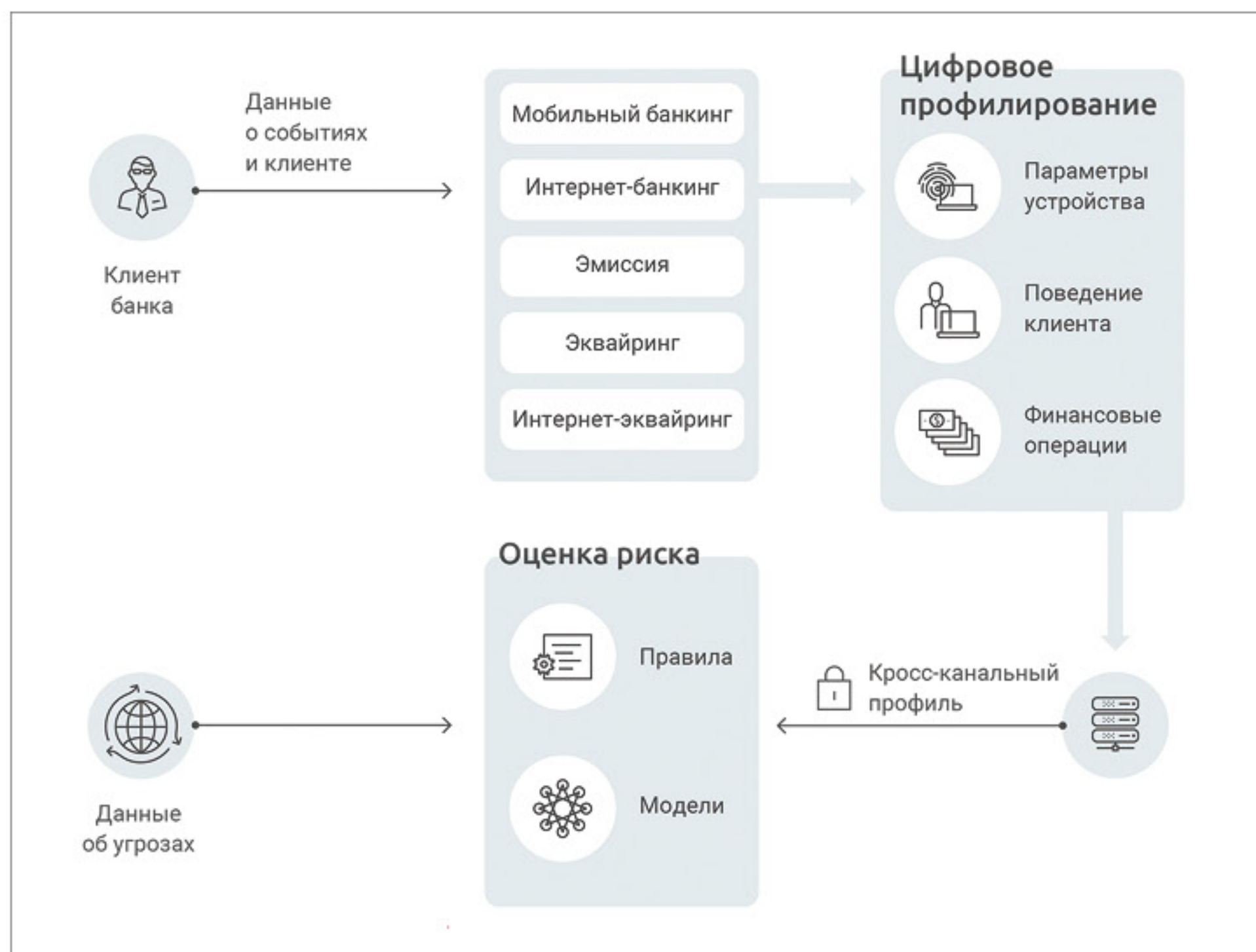


Схема обработки данных в ВСФР

типично, ничто не мешает исключить некоторые этапы проверки. Скажем, пропустить СМС-подтверждение при входе в онлайн-банк или позволить провести операцию без верификации через 3-D Secure.

Всё это делается на базе тех же технологий анализа информации и оценки рисков. Подобный подход можно использовать практически в любом онлайн-сервисе, упростив работу с ним с точки зрения обычного пользователя и повысив таким образом лояльность клиентов.

### ИСТОЧНИКИ ДАННЫХ ОБ УГРОЗАХ

Важной составляющей эффективной работы системы являются данные об актуальных угрозах. ВСФР всё время обучается на результатах обработки операций, а также на информации, поступающей в систему и полученной по итогам расследования инцидентов. Руководствуясь этими данными, система ежедневно корректирует собственную работу, чтобы добиться максимальной эффективности.

Одним из источников актуальных угроз служит модуль BI.ZONE Fraud Intelligence (BFI), в который постоянно поступает информация об активности киберпреступников. Она формируется

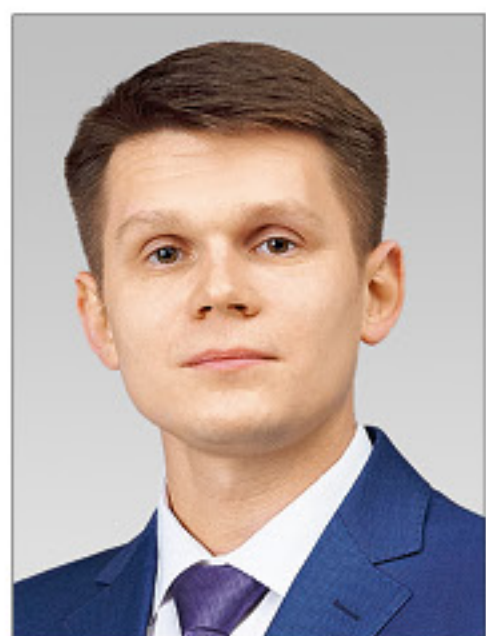
на основе работы аналитиков и ВСФР при отслеживании операций в различных платёжных каналах. Кроме того, значительную роль играет экспертная работа специалистов BI.ZONE, которые непосредственно занимаются расследованиями и проводят постоянный мониторинг даркнета, наблюдая за площадками, где общаются создатели вредоносного ПО, торговцы персональными данными и другие злоумышленники.

\*\*\*

Используя различные системы борьбы с мошенничеством в разных каналах, непросто бывает получить цельную картину. Гораздо удобнее и эффективнее, когда все данные, необходимые для обеспечения безопасности платежей, собраны в одном продукте. Это позволяет проводить более полный и оперативный анализ, точнее оценивать риски каждого действия пользователя.

В идеальном мире все эти предосторожности и сложные системы были бы, конечно, излишни. Пока же не все пользователи знают даже базовые принципы кибербезопасности и готовы им следовать, банкам придётся брать борьбу за безопасность клиентов в свои руки.





**Леонид БОНДАРЕНКО**  
директор департамента  
поддержки продаж  
Сикрет Технолоджис

# ФОТОГРАФ ЭКРАНА МОНИТОРА УЖЕ НЕ АНОНИМ

ПОПУЛЯРНЫЙ В 2019–2020 ГОДАХ КАНАЛ УТЕЧЕК  
ТЕПЕРЬ ПЕРЕКРЫВАЕМ

**В** начале каждого года принято говорить либо о годе ушедшем, либо о прогнозах на предстоящий. В настоящей статье я, как представитель разработчика программного обеспечения в области информационной безопасности, компании Secret Technologies, хочу рассказать о проблеме, которую нам активно транслировали заказчики в 2019 году, и которая будет актуальна и в 2020 (как минимум). Эта проблема — фотографирование данных с экрана монитора.

Проблема широко известная и актуальная, ведь у практически любого сотрудника есть смартфон, а сделать фото — дело нескольких секунд, и про услуги «пробива» тоже слышаны все. Инструментов, которые позволяют снизить этот риск, не так уж и много. Несмотря на то что работодатель вправе ограничить использование мобильных телефонов на рабочем месте, далеко не каждая компания пойдёт на такие запреты. И ввод соответствующих локальных нормативных актов не гарантирует, что они не будут нарушены. В любом случае нужны какие-либо инструменты контроля.

Самый очевидный способ контроля — изъятие телефона при проходе сотрудника на работу. Этот способ дол-

жен быть тщательно обоснован с правовой точки зрения, вопрос очень неоднозначен юридически. Ещё один способ — анализ изображений с видеорекамер. Но обрабатывать видео вручную очень трудозатратно, а использовать современные технологии компьютерного зрения и машинного обучения для решения этой задачи активно пока не начали. Контролировать может также руководитель, но это точно негативно скажется на его непосредственных задачах и рабочем процессе и не эффективно при большом количестве сотрудников в подразделении.

Нашим предложением для снижения рисков фотографирования данных с монитора является нанесение на окна приложений идентификационной информации в виде водяных знаков.

Снижение, при нанесении водяных знаков, количества утечек через фотографирование экрана обусловлено тем, что сотрудник будет видеть, что ведётся контроль. Понимать, что если он сделает фото, то на нём будет явно видно дату, имя компьютера, имя пользователя и другие атрибуты, которые позволят идентифицировать его как источник утечки. Информация из водяного знака также поможет в расследовании инцидента, если несанкционирован-

но сделанное фото попадёт в службу безопасности.

Решение, применяемое для нанесения водяных знаков поверх окна приложения для эффективности контроля, должно удовлетворять ряду требований. Мы сформировали их по итогам взаимодействия с заказчиками:

- ♦ возможность работы с любым содержимым любого приложения (графическое, консоль, чертёжные инструменты, банковское и специальное ПО);
- ♦ динамическое определение ценной информации или приложений (скрытие на не конфиденциальном содержимом);
- ♦ возможность гибкой настройки отображаемого содержимого водяного знака;
- ♦ лёгкое масштабирование, низкая стоимость администрирования;
- ♦ без больших затрат человеческих ресурсов;
- ♦ низкая нагрузка на рабочую станцию.

\* \* \*

Команда Secret Technologies разработала собственный инструмент, удовлетворяющий сформированным требованиям, — решение Screen Guard.





**Сергей ДОБРУШСКИЙ**  
директор по разработке  
системы защиты баз данных  
ООО «Гарда Технологии»

# АКТУАЛЬНАЯ АРХИТЕКТУРА ЗАЩИТЫ ОТ ИНСАЙДЕРА

«ГАРДА БД» — ВОСТРЕБОВАННОЕ АВТОМАТИЗИРОВАННОЕ РЕШЕНИЕ ДЛЯ БАНКОВСКИХ БИЗНЕС-СИСТЕМ, БАЗ ДАННЫХ И ПРИЛОЖЕНИЙ

**Б**азы данных — наиболее ценный источник конфиденциальной информации банковской сети в сравнении с теми же серверами и ПК. Поэтому защита баз данных становится одним из приоритетных направлений работы службы информационной безопасности в финансовых организациях.

## АКТУАЛЬНЫЕ УГРОЗЫ ДЛЯ БАЗ ДАННЫХ В БАНКАХ

Есть два ключевых фактора, влияющие на безопасность баз данных — это привилегированные пользователи с неограниченным доступом к данным и недостаточный аудит доступа к данным.

Как правило, корпоративная сеть считается защищённой межсетевыми экранами и другими сетевыми средствами защиты периметра. Но обнаружить атаки на данные со стороны легитимного пользователя-инсайдера, который успешно авторизовался в базе данных, такой подход не позволит.

Как показывают исследования аналитического центра «Гарда Технологии» (входит в «ИКС Холдинг»), 91 % утечек баз данных, оказавшихся в свободной продаже на чёрном рынке, — дело рук инсайдеров. Как правило, в формате го-

товой базы продаются выгрузки, обычно в формате xml, полученные в результате выгрузки из АБС банка или CRM-систем. С такими ситуациями сталкиваются даже банки из ТОП-10 страны.

## КАК СНИЗИТЬ РИСК УТЕЧЕК БАЗ ДАННЫХ?

Это комплексная задача, включающая постоянный анализ привилегий пользователей баз данных, настройку аудита и мониторинг действий пользователей в базах данных.

Регулярный анализ привилегий даёт возможность службе безопасности ограничить доступ пользователей к конкретным базам данных, а аудит и мониторинг — увеличить эффективность расследования инцидентов по фактам мошенничества и предотвратить аналогичные инциденты и реализацию мошеннических схем.

**1. Встроенный аудит баз данных.** Этот функционал существенно влияет на производительность сервера, что вынуждает многие организации ограничивать или полностью отключить аудит. Большинство собственных механизмов аудита уникальны для платформы сервера баз данных. Например, журналы Oracle не такие как PostgreSQL, а жур-

налы PostgreSQL отличаются от Teradata. Для крупной банковской сети с гетерогенными средами баз данных это препятствие для реализации единых масштабируемых процессов аудита, мониторинга и отчётности.

**2. Контроль действий привилегированных пользователей.** Пользователи, обладающие административным доступом к базе данных либо законно, либо преднамеренно могут отключить встроенный аудит базы данных, поэтому нужна система независимого аудита действий пользователей баз данных со стороны службы информационной безопасности.

**3. Аудит пассивных операций.** Прикладной аудит не позволяет отслеживать операции «пассивного» просмотра конфиденциальной информации в базах данных со стороны пользователей — одной из основных составляющих в мошеннических операциях. Примеры «пассивных» операций: просмотр остатков по счётам VIP-клиентов и организаций, данных по учредителям и другой ценной информации, используемой инсайдерами для перепродажи.

**4. Выявление аномалий в поведении пользователей и приложений.** Для выявления мошеннических схем



также требуется анализ данных аудита баз данных. Разблокировка банковских карт клиентов, операции по ним, блокировка банковской карты, движение средств с «малоподвижных» счетов. Сами по себе такие операции не свидетельствуют об угрозе вывода денежных средств со счетов клиентов. Но анализ событий во времени и с привязкой к другим событиям позволяет раскрыть мошеннические схемы.

Для непрерывного аудита доступа к базам данных, оперативного выявления аномалий, расследования и предотвращения мошеннических действий со стороны сотрудников банков применяются автоматизированные решения по защите баз данных и веб-приложений класса DAM (Database Activity Monitoring — Мониторинг активности базы данных).

### КАК РАБОТАЕТ АВТОМАТИЗИРОВАННАЯ СИСТЕМА ЗАЩИТЫ БАЗ ДАННЫХ И ВЕБ- ПРИЛОЖЕНИЙ БАНКОВ?

Аппаратно-программный комплекс «Гарда БД» российского производителя систем информационной безопасности «Гарда Технологии» (входит в «ИКС Холдинг») осуществляет аудит и мониторинг баз данных крупных банковских сетей. Для высоконагруженных автоматизированных процессинговых систем, когда недопустимо влияние на вычислительные ресурсы серверов, применяется безагентское решение, основанное на анализе копии трафика с сетевого оборудования. Для остальных систем применяется агентское решение, позволяющее отслеживать локальные подключения к базе данных, решая задачу контроля администраторов БД.

«Гарда БД» позволяет анализировать большинство сетевых протоколов СУБД для обмена между клиентами и серверами баз данных, используемых в банке. Для связи событий баз данных между собой и с другими источниками используется инструменты поведенческого анализа, интегрированные в АПК, и SIEM системы, для которых DAM-система — один из источников данных.

Большинство современных банковских систем строит свою работу по принципу трёхзвенных подключений, где между клиентом и сервером БД

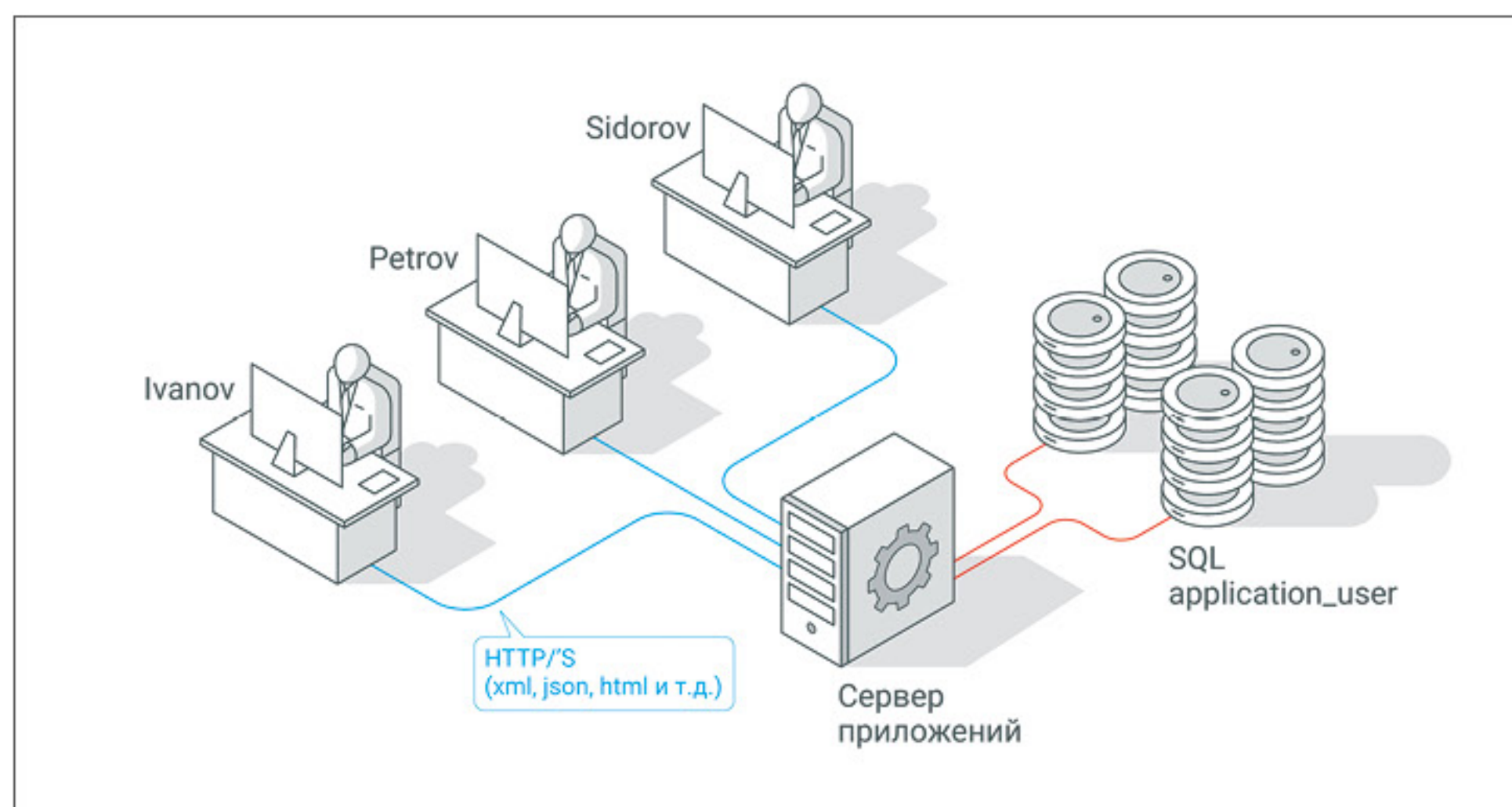


Рисунок 1. Схема трёхзвенной архитектуры

используется дополнительное звено — сервер приложений (рис. 1).

При трёхзвенной архитектуре приложения все подключения к базе данных совершаются от технологических учётных записей, так как соединение с базой данных устанавливает не клиент, а сервер приложения. По этой причине, анализируя только SQL-трафик к базе данных, возможность определить пользователя, инициировавшего запрос, существует далеко не всегда.

Для решения задачи персонификации действий пользователей в трёхзвенных приложениях можно использовать разные подходы, зависящие от логики работы приложения:

**1. Выделение информации о конечном пользователе исключительно из SQL-трафика.** Такая возможность появляется, когда сервер приложения передаст информацию о конечном пользователе в SQL-трафике. Это может быть передача учётной записи в инициализирующем запросе, в переменных или же возвращение с ответами на запрос.

**2. Взаимосвязь HTTP и SQL-трафика.** Способ требует подачи на DAM-систему сегмента HTTP-трафика, из которого выделяется учётная запись пользователя. При этом гарантированный результат при персонификации будет только в случае передачи сервером приложения некоторого уникального идентификатора сессии пользователя в SQL-трафик.

**3. Использование только сегмента HTTP-трафика для задач персонификации и аудита доступа и проведения расследований.** Этот подход

может применяться для критичных систем, так как кроме определения пользователя, он позволяет вести аудит всех ответов на запросы, то есть той информации, которую пользователь получает в веб-браузере.

«Гарда БД» позволяет решить задачу защиты трёхзвенных приложений всеми тремя способами.

Построенная таким образом система безопасности бизнес-систем, позволяет вести архив действий сотрудников. При этом не нужно вносить изменения в архитектуру приложения, устанавливать агентские решения на сервера приложений или на пользовательские компьютеры. Система не оказывает никакого влияния на работу приложения и базу данных.

Система позволяет с высокой эффективностью проводить расследования по фактам мошенничества с участием персонала банка, а также независимую экспертизу действий ИТ-персонала при возникновении инцидентов в ИТ-инфраструктуре банка.

\* \* \*

**«Гарда БД» решает задачи по аудиту и мониторингу пользователей в базах данных даже при большом объёме обрабатываемой информации в автоматизированных системах банковского сектора, поддерживая разнородную инфраструктуру и высоконагруженное оборудование, и становится важной составляющей защиты данных в компании.**





**Виктория ЧИРВА**  
PR-менеджер  
компании «Актив»

# РУТОКЕН — СТАНДАРТ ДЕ-ФАКТО

## НА СТРАЖЕ БЕЗОПАСНОСТИ ДБО ЮРИДИЧЕСКИХ ЛИЦ

**С**егодня мы наблюдаем увеличение масштабов киберпреступности. Бурное развитие цифровых финансовых услуг требует надёжных и проверенных решений. Продукция Рутокен стала стандартом де-факто для аутентификации и защиты транзакций в системах дистанционного банковского обслуживания более чем в 300 российских банках.

К 25-летию «Актива», российского разработчика и производителя программно-аппаратных средств инфор-

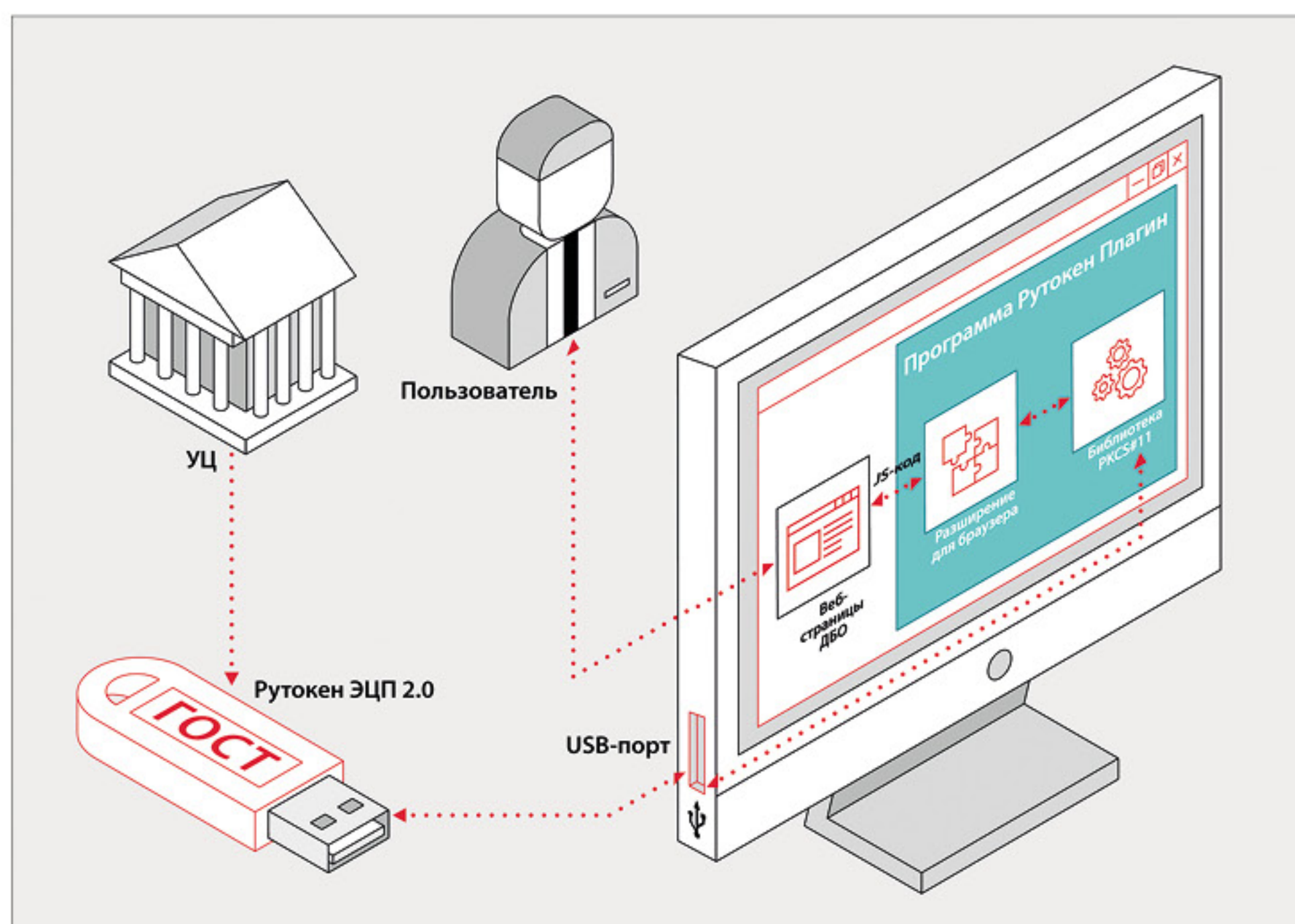
мационной безопасности, портфель компании насчитывает более 100 продуктов и решений. Среди которых — системы для защиты и лицензирования ПО, программные и программно-аппаратные средства защиты информации. В том числе полностью отечественная линейка аппаратных продуктов и решений Рутокен для аутентификации и создания электронной подписи. Также есть и решения для защиты мобильных платформ.

Технологии, разработанные компанией «Актив», позволяют финансо-

вым организациям повысить защищённость операций, осуществляемых клиентами дистанционно. Применение электронной подписи в системах ДБО позволяет повысить уровень защищённости транзакций, обеспечить целостность и неотказуемость. Использование электронной подписи (в том числе квалифицированной) в любой системе документооборота приносит новые возможности как для самой организации, так и для её контрагентов. А двухфакторная аутентификация, основанная на владении пользователем электронным идентификатором и использующая асимметричную криптографию, серьёзно повышает безопасность системы, делая её неуязвимой к краже пароля.

Линейка аппаратных ключевых носителей и программного обеспечения Рутокен предназначена для работы с электронной подписью, двухфакторной аутентификации, а также для защищённого хранения криптографических ключей, сертификатов, паролей и критически важной информации. Продукция имеет сертификаты ФСТЭК России и ФСБ России, и может быть использована для вычисления квалифицированной электронной подписи.

Программное решение Рутокен Плагин позволяет интегрировать интеллектуальные ключевые носители Рутокен в Web-сервисы, порталы и SaaS-решения с минимальными затратами (рис.1).



**Рисунок 1.** Схема работы системы ДБО, плагина и токена





Корпоративным клиентам Новикомбанка стали доступны решения Рутокен

Рутокен Плагин может быть запущен в большинстве браузеров (Google Chrome, Mozilla Firefox, IE, Edge, Яндекс, Слутник и прочие) под различными операционными системами (Windows, Linux, MacOS).

Для электронной подписи в мобильных версиях ДБО может использоваться беспроводной токен, компактный токен с разъёмом Type-C и дуальная смарт-карта с двумя интерфейсами: беспроводным NFC и обычным контактным. Для создания мобильного рабочего места с возможностью работы с электронной подписи на Рутокен, достаточно перенести модули подписания и обнаружения устройств в мобильное приложение из готовых примеров из комплекта разработчика Рутокен для мобильных платформ.

#### **РУТОКЕН УСИЛИЛ БЕЗОПАСНОСТЬ СИСТЕМЫ ДБО НОВИКОМБАНКА**

Надёжность и удобство продуктов Рутокен проверены сотнями российских банков в реальной эксплуатации. Отлично, что количество банков, использующих в системах ДБО классические аппаратные решения Рутокен, растёт.

Не исключением стал Новикомбанк, опорный банк Госкорпорации Ростех.

Новикомбанк запустил новый интернет-банк для корпоративных клиентов. В конце 2019 года банк представил релиз новой интернет-версии системы дистанционного банковского обслуживания для корпоративных клиентов на платформе BSS. Новая версия ДБО представляет собой современный высокотехнологический формат дистанционного банковского обслуживания.

Пользователям доступны такие преимущества, как улучшенный интерфейс, функционирование на множестве операционных систем (в том числе MS Windows, Mac OS) и мультибраузерность (возможна работа в MS Internet Explorer, Google Chrome, FireFox, Safari, Opera). Также для работы новой системы не требуется установка никакого банковского ПО.

«Новикомбанк успешно решил задачу по переходу на новую современную платформу интернет-банка для корпоративных клиентов. У нас есть понимание, что, стремясь предложить клиентам максимум возможностей в удалённой среде, мы не должны забы-

вать о безопасности новых решений. Поэтому мы выбрали решения от компаний BSS и «Актив», которые полностью соответствуют требованиям регуляторов и гарантируют максимальный уровень защищённости в удалённой среде», — отметил заместитель Председателя Правления Новикомбанка Игорь Дубоносов.

В целях обеспечения безопасности и сохранности денежных средств в новой версии ДБО применяется целый набор защитных механизмов, в том числе шифрование канала между Банком и Клиентом, сертифицированные средства криптографической защиты информации и носители ключевой информации — ключевые носители Рутокен ЭЦП 2.0. Кроме того, предусмотрено самостоятельное изготовление клиентом своих ключей электронной подписи сроком действия 3 года, а также SMS-оповещение клиента о каждой совершенной операции.

В новой системе ДБО доступно использование усиленной квалифицированной электронной подписи, сертификаты для которой выпущены сторонними аккредитованными удостоверяющими центрами.





Для электронной подписи в мобильных версиях ДБО может использоваться компактный токен с разъёмом Type-C и дуальная смарт-карта

После внедрения продуктов Рутокен в системе ДБО Новикомбанка решены следующие задачи безопасности:

- ♦ Двухфакторная аутентификация при входе в интернет-банк — гарантия, что доступ к личному кабинету клиента банка может получить только он.
- ♦ Повышение уровня защищённости финансовых транзакций.
- ♦ Использование электронной подписи, в том числе квалифицированной, позволит перевести документооборот в электронный формат, упростить и обезопасить взаимодействие клиента с банком.

Помимо сохранения всех функциональных возможностей по удалённому взаимодействию с Банком и совершению полного перечня платёжных операций, новая версия ДБО предлагает актуальные возможности системы интернет-банкинга последнего поколения. При внедрении новой системы ДБО для корпоративных клиентов заложены возможности активного наращивания функционала и модификации интерфейса. В ближайшее время поль-

зователям станет доступно мобильное приложение для систем iOS и Android.

\*\*\*

«В банковском секторе усиливается регулирование, финансовые институты вынуждены быть более консервативными, уделять больше внимания информационной безопасности. Существенный пересмотр отношения к рискам подталкивает банки к более широкому использованию классических проверенных технологий. Рутокен, устройство с отечественной

криптографией «на борту», как нельзя лучше вписывается в эти реалии. Большинство российских банков в системах ДБО для юридических лиц используют интеллектуальные ключевые носители Рутокен с неизвлекаемыми ключами электронной подписи.

Мы ценим доверие Новикомбанка к опыту BSS и к нашей продукции. Применение Рутокен позволит повысить защищённость и снизить затраты на поддержку клиентов банка», — подчеркнул Дмитрий Горелов, управляющий партнёр и коммерческий директор компании «Актив».



Контакты:

[www.aktiv-company.ru](http://www.aktiv-company.ru)  
[www.rutoken.ru](http://www.rutoken.ru)  
[www.guardant.ru](http://www.guardant.ru)  
[info@rutoken.ru](mailto:info@rutoken.ru)

#### ТЕХНОЛОГИИ РУТОКЕН ПОМОГАЮТ:

- ♦ сохранить удобство использования ДБО для клиентов банка;
- ♦ снизить затраты банка на внедрение и использование электронной подписи;
- ♦ исключить риск хищений у клиентов;
- ♦ упростить прохождение аудита безопасности банка.



16–17 апреля

Москва,  
LOFT HALL #2

OFF  
ZONE  
2020

# OFFZONE 2020

Третья международная конференция  
по практической безопасности

**2000**

**участников**

специалисты по кибербезопасности,  
разработчики, инженеры, преподаватели  
и студенты

**60+**

**докладов**

экспертов из России, Европы, Азии  
и Америки

**11 тематических  
зон**

от глобальных исследований  
до уникальных практических активностей

**10 сильнейших  
команд**

сразятся за 10 000 \$ и место  
на DEF CON CTF

Никаких пиджаков, никакого бизнеса —  
только hardcore research

info@offzone.moscow

offzone.moscow







**Дарья СУТОРМИНА**  
начальник отдела анализа  
защищённости  
АО НИП «ИНФОРМЗАЩИТА»

# «БЕЛЫЕ ХАКЕРЫ» НА СТРАЖЕ БИЗНЕСА

КОРПОРАТИВНЫЕ КИБЕРУЧЕНИЯ RED TEAM:  
«КРАСНЫЕ» ПРОБУЮТ НА ПРОЧНОСТЬ «СИНИХ»

**К**ибератаки на банки, государства и компьютеры граждан давно не редкость. Понятие «хакер» в массовом сознании неразрывно связано с темой киберпреступлений. Тем не менее, хакер — необязательно злоумышленник: продвинутые «взломщики» умеют не только нарушить покой, но и знают, как его сберечь. Поговорим о том, как работают «белые хакеры» и чем они могут быть полезны вашему бизнесу.

## «КРУЧЕ» ПЕНТЕСТИНГА

Компании кровно заинтересованы в защите данных: утечки приводят к серьёзным денежным и репутационным потерям. Информационная безопасность — не результат и не состояние, а непрерывный процесс. Чтобы сотрудники компании, ответственные за информационную безопасность, вовремя смогли обнаружить и правильно, адекватно возникшей угрозе, отреагировать на брешь в системе, необходимо постоянно повышать профессионализм команды.

Рынок информационной безопасности предлагает несколько услуг по анализу защищённости компании, среди которых:

- ♦ анализ безопасности систем и приложений,
- ♦ тестирование на проникновение,

♦ оценка осведомлённости персонала в вопросах информационной безопасности

Самый эффективный метод, на наш взгляд, — киберучения в рамках Red Team<sup>1</sup>.

Метод этот схож с традиционным тестом на проникновение (пентестом), который используется для проверки сетей, сервисов, систем и беспроводных точек доступа, но не стоит их путать. Пентестинг — оценка пассивной защищённости информационных систем, Red Teaming — оценка активной защищённости.

Специалисты-пентестеры выезжают к заказчику со сканерами и другим оснащением и, не таясь, пытаются «взломать» систему (сразу скажу, статистика неблагоприятная). После проверки и анализа пишут отчёт о проведённой работе, о наличии уязвимостей, дают рекомендации по их устранению.

Red Team — «проверка боем». Наши белые хакеры имеют обширные знания о способах нападения. Во-первых, они накапливают опыт во время пентестов, во-вторых, изучают мировую

практику реальных хакерских атак. Во время проведения Red Team хакеры имитируют настоящую кибератаку. Естественно, «нападение» проходит по заранее оговорённым сценариям и не нарушает работоспособность критически важных информационных систем компании.

Тщательная подготовка и изучение систем позволяют провести атаку аккуратно и максимально приближенно к реальности. Это, конечно, напрямую зависит от опыта и уровня профессионализма команды Red Team. Об учениях и мнимой атаке сообщается очень узкому кругу людей, чтобы остальные сотрудники вели себя естественно.

## КОРПОРАТИВНЫЕ КИБЕРУЧЕНИЯ

Цель Red Team, «красной команды», — достичь поставленных целей, то есть проникнуть в систему, похитить данные, задокументировать процесс «взлома» и рассказать «синей команде» (стороне заказчика) о допущенных ошибках и способах их устранения. Получается, что знания и умения «синей команды», внутренних экспертов компании, растут за счёт того, что «красная» раз от раза обеспечивает всё более высокий уровень атак.

«Редтиминг» более затратен по времени и усилиям, чем пентест. Но зато позволяет решить сразу несколько задач:

<sup>1</sup> Понятие Red Team и Blue Team пришло в информационную безопасность из военной терминологии, где Red Team — команда нападающих, а Blue Team — защищающих. В контексте кибербезопасности Blue Team означает команду экспертов, задача которых — обеспечивать защиту инфраструктуры.





- ♦ проверка эффективности систем информационной безопасности, используемых в компании;

- ♦ анализ действий службы информационной безопасности и других сотрудников;

- ♦ обучение внутренних специалистов для предотвращения ошибок в дальнейшем.

Ещё одна особенность метода Red Team, которая отличает его от других способов анализа уязвимостей, — использование любых вариантов добычи нужной информации для проникновения в систему. В том числе, методов социальной инженерии.

Самое слабое звено в безопасности информационной системы, как известно, не софт и не «железо», а сами пользователи. Хакеры используют психологические приёмы и особенности поведения людей для получения информации о доступе в систему. Несмотря на то, что о социальной инженерии активно пишут СМИ и общая осведомлённость в этом вопросе растёт, на уровне

корпоративной защиты она, как правило, не обнаруживается.

Кроме того, меняются способы психологических атак: массовые письма и сообщения уступают место таргетированному воздействию. В ход идут телефонные разговоры, дружба в социальных сетях и общение в чатах. В нашей практике есть удачный кейс взлома системы с использованием информации, добытой в закрытом корпоративном чате в WhatsApp.

### ИСПЫТАНИЕ НА ПРОДВИНУТОСТЬ

О том, как злоумышленники могут выудить нужную информацию, мы рассказываем во время киберучений Red Team. Обучаем, кстати, не только специалистов служб информационной безопасности, повышаем киберграмотность всех сотрудников компании.

Кому стоит задуматься о проведении «редтиминга»? Киберучения не имеют смысла для организаций с начальным уровнем зрелости информационной безопасности, слишком рано.

Таким компаниям можно ограничиться традиционными услугами вроде пентеста или технического аудита информационных систем.

Мы рекомендуем «редтиминг» среднему и крупному бизнесу и организациям финансово-технического сектора. Тем организациям, которые традиционно являются лакомым кусочком для злоумышленников.

\* \* \*

Не стоит бояться проведения учений, особенно внутренним службам безопасности. Цель проверки — не выявить некомпетентность и недостаток экспертизы. Наоборот, помочь тем, кто занимается информационной безопасностью компании, обеспечить максимальную защиту и повысить профессионализм во время учебных боёв, чтобы всегда быть наготове и отразить реальную атаку. Как любят повторять наши белые хакеры: тяжело в киберучении — легко в кибербою.





**Никита ДУРОВ**  
технический директор  
Check Point Software Technologies  
в России и СНГ

# ЗНАЕШЬ УГРОЗЫ — ЗАЩИТА НАДЁЖНА

## АКТУАЛЬНЫЕ ОСОБЕННОСТИ БЕЗОПАСНОСТИ МОБИЛЬНОГО БАНКИНГА

**В** 2019 году, по данным Check Point ThreatCloud Intelligence, вдвое возросло количество мобильных банковских вредоносных атак. Сегодня банковские вредоносные программы — распространённая мобильная угроза. Банковское вредоносное ПО способно похитить платёжные и учётные данные, средства с банковских счетов жертв. Все новые версии вредоносного ПО готовы к массовым продажам злоумышленникам.

BIS Journal пообщался с техническим директором Check Point Software Technologies в России и СНГ Никитой Дуровым, чтобы узнать, как обеспечить безопасность мобильного банкинга от этой угрозы.

### БАЛАНС УДОБСТВА И БЕЗОПАСНОСТИ

— Как найти баланс между удобством и безопасностью мобильного банкинга?

— Банкам важно сделать максимально простой и понятный интерфейс — но при этом обеспечить безопасность

работы. В целом, по моему мнению, если смотреть на текущие мобильные банковские приложения, банки вполне справляются с этой задачей.

В прошлом году было много обсуждений применения биометрии для идентификации пользователей в банковских приложениях. Безусловно, это очень удобно для пользователей, но в то же время это несёт значительные риски. Возможно, в ближайшем будущем банки будут сосредоточены на том, чтобы эти риски минимизировать.

— Кто должен отвечать за безопасность мобильного банкинга: банк или разработчик? Что могут предложить специалисты по ИБ?

— Здесь есть две стороны: банк и разработчик. Разработчик занимается платформой приложения, а совместно с банком делает функциональную часть. На текущий момент полностью за всю безопасность отвечает сам банк. Сервисов аутсорсинга мобильного банка не так много, этими услугами пользуется совсем немного банков. И то, чаще всего их поставщиком выступают крупные банки. Большинство банков строит

собственные системы мобильного банкинга; используя продукты некоторых лидеров-разработчиков. В конечном счёте все вопросы безопасности ложатся на сам банк.

— О безопасности приложений, в том числе банковских, говорят давно. Каковы достижения в этой сфере?

— Мобильные банковские злоумышленники по-прежнему очень опасны. Главным образом потому, что могут легко обойти многие механизмы защиты, например, двухфакторную аутентификацию. Для незаметной загрузки вредоносного ПО злоумышленники могут использовать дропперы или так называемые загрузчики. Сам дроппер не содержит вредоносный код, поэтому получает разрешение пользователя на загрузку файлов и, таким образом, может установить на ПК или устройство практически любой вирус.

### ОТ КАЖДОЙ АТАКИ — СВОЯ ЗАЩИТА

— Чем отличаются атаки на приложения мобильного банкинга? Какие атаки популярны у злоумышленников, включая социальную инженерию?

— Главный вектор защиты для банков — DDoS-атаки, при которых пользователи теряют доступ к банковским сервисам. Серьёзный удар по репутации банка! Согласно отчёту Check Point

*Мобильные банковские злоумышленники по-прежнему очень опасны. Главным образом потому, что могут легко обойти многие механизмы защиты*



CyberSecurity Report 2020, в 2019 году 28% организаций по всему миру подверглись атакам ботнетов. Наиболее распространённым вредоносным ПО для ботов был Emotet.

Если говорить об атаках на пользователей, то главная проблема безопасности — человеческий фактор. Всегда проще атаковать человека, чем искать уязвимости в приложении. Злоумышленники используют социальную инженерию, психологические приёмы мошенников. Стараются собрать максимальное количество данных о пользователях во всевозможных базах данных. В том числе полученных из-за утечек из банков и других организаций, или же путём информационного взлома, кражи. Информация о гражданах собирается по всей сети, эти данные выкладываются злоумышленниками в открытый доступ для продажи.

— Иногда злоумышленники целеным образом атакуют конкретного человека. Какие каналы используют преступники в этом случае?

— Каналы могут быть как открытые, так и закрытые. Базы данных могут попадаться в выдаче поисковиков. Есть люди, которые целенаправленно ищут базы в открытом доступе. Второй вариант — Dark Web. Там есть специализированные сервисы, которые оказывают подобные услуги. Через них можно найти почти все существующие в открытом доступе базы: государственных органов, например, из налоговой службы. Часто злоумышленники имеют инсайдеров в таких организациях и могут получить по запросу информацию о конкретном человеке.

Манипулируя этими данными при помощи социальной инженерии, киберпреступники побуждают пользователя совершать те или иные транзакции. Проверять, есть ли данные о конкретном человеке в базах, мы не рекомендуем. Так можно спровоцировать злоумышленников на атаку. Сами по себе данные не дают возможности совершить кражу денежных средств с карты.

Впрочем, возможно появление новой волны фишинговых атак, когда злоумышленники, имея определённую информацию о своих жертвах, начинают

*Утечка персональных данных влечёт за собой как финансовые, так и репутационные риски для банков и их клиентов — и сейчас это одна из основных проблем кибербезопасности*

звонить им, представляясь сотрудниками банка и вынуждая совершить те или иные операции. Так как преступники обладают некоторыми сведениями, у жертвы может создаться впечатление, что звонок действительно от представителя банка.

Лучшая стратегия — не вести переговоров по телефону. Банки не звонят своим клиентам по таким поводам. Они просто блокируют карту, если подозревают неправомерные действия. Если вам позвонили якобы из банка, лучше всего перезвонить в банк самим. При подозрении, что данные вашей карты, скомпрометированы — похищены, а на ней крупная сумма, лучше оперативно выпустить её заново, заблокировав прежнюю.

— Какие методы атак на онлайн-банки можно прогнозировать?

— Банки давно увидели множество возможностей в применении последних технологий: распознавания лиц, идентификация пользователя по голосу, использование умных устройств в работе. Удалённая идентификация клиента в банке — сложный процесс, требующий совместных усилий как разработчиков самой системы, так и специалистов банка по безопасности.

С одной стороны, очень удобно, когда после однократного подтверждения клиентом своей личности в банке его в дальнейшем могут идентифицировать по голосу. С другой стороны, это сопряжено с огромным количеством рисков. Банки должны крайне серьёзно относиться к хранению личных данных пользователей. Очевидно, что сейчас хакеры активно работают над способами обхода биометрии, и вероятно, что скоро мы увидим попытки опробования новых методов взлома.

Объёмы хранящейся персональной информации растут, и хакеры заинтересованы получить её. Утечка персо-

нальных данных влечёт за собой как финансовые, так и репутационные риски для банков и их клиентов — и сейчас это одна из основных проблем кибербезопасности.

Если мы говорим о рисках биометрии, эти риски будут снижаться по мере того, как технологии такой идентификации будут становиться более зрелыми, а распознавание данных станет максимально точным. При этом необходимо в комплексе учитывать все возможные угрозы подмены данных и взлома приложений в обход механизмов идентификации.

## ПРАВИЛА КИБЕРГИГИЕНЫ

— Какие правила безопасности электронных сервисов первостепенны для банков и для клиентов?

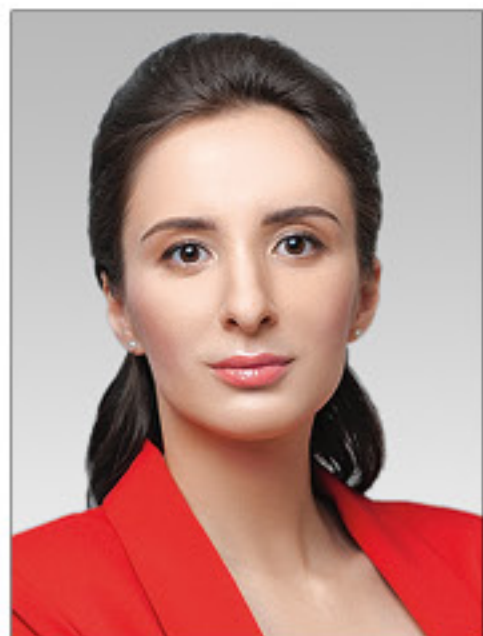
— Прежде всего банкам необходимо работать со своим персоналом, информировать его об угрозах и правилах безопасности. Зачастую сотрудники не осознают ИБ-риски, которым они подвергают организацию, не соблюдая правила цифровой гигиены.

Не рекомендуется открывать письма от незнакомых отправителей, загружать файлы с непроверенных ресурсов, даже с виду знакомые сайты могут нести угрозу. Так, хакеры могут отправлять ссылки на поддельные сайты, которые практически идентичны оригинальным. Также важно рассказывать сотрудникам о том, что подключение мобильных телефонов, планшетов и ноутбуков к непроверенной сети Wi-Fi может привести к серьёзным последствиям.

Для пользователя важно соблюдать базовые правила цифровой гигиены. Например, регулярно обновлять свой смартфон, пользоваться проверенными сетями, внимательно относиться к загружаемым приложениям.

Беседовала Анна Воробьева





**Дарья ВЕРЕСТНИКОВА**  
коммерческий директор  
компании SafeTech

# ПОДПИСЬ В СМАРТФОНЕ — ДЛЯ БЕЗОПАСНОСТИ И ДЛЯ БИЗНЕСА

КАК ЦИФРОВЫЕ КАНАЛЫ МОГУТ БЫТЬ БЕЗОПАСНЫМИ,  
УДОБНЫМИ И ДОСТУПНЫМИ

**В** последние годы экспертное сообщество непрерывно говорит о бурном развитии цифровых каналов банковского обслуживания, а также о связанных с ними проблемах: увеличением активности мошенников, использующих социальную инженерию, уязвимости кодов подтверждения операций, передаваемых в SMS и PUSH, непреодолимых ограничениях на реализацию сервисов для мобильных пользователей. О том, как решить актуальные проблемы безопасности Интернет- и мобильного банкинга, а также создать необходимые условия для самых инновационных и востребованных сервисов мы побеседовали с Дарьей Верестниковой, коммерческим директором компании SafeTech.

— Дарья, расскажите, пожалуйста, какие вопросы, связанные с информационной безопасностью, являются сейчас наиболее актуальными в области цифровых каналов обслуживания?

— На наш взгляд, самым актуальным вопросом на сегодняшний день

является проблема социальной инженерии. В частности, по информации ФинЦЕРТ Банка России, в 2018 году с использованием приёмов социальной инженерии было совершено более 97 % хищений со счетов физических лиц. А в прошедшем 2019 году ситуация усугубилась ещё больше — мошенники стали активно использовать возможность подмены исходящего телефонного номера на «реальные» номера колл-центров банков. Вы же помните, как прошедшей осенью новостные ленты пестрили сообщениями об успешных попытках злоумышленников получить данные пользователей, представившись «сотрудниками банков»? Мы в компании SafeTech уверены, эта проблема останется актуальной и в наступившем году.

Вторым важным вопросом и направлением активной деятельности экспертного сообщества в финансовых институтах является обеспечение соответствия требованиям Положения Банка России № 683-П от 17.04.2019 г. Очевидно, что в условиях увеличения числа преступлений в финансовой сфере регулятор продолжает задавать ос-

новные направления борьбы с ними. По информации МВД России в течение девяти месяцев 2019 года был зафиксирован 70 %-ый рост количества преступлений в сфере IT, в том числе с использованием банковских карт и мобильных устройств. И выполнение требований Банка России, какими бы сложными в реализации они ни казались, является в полном смысле слова, велением времени.

Третьим актуальным вопросом, связанным с информационной безопасностью, является уязвимость распространённых, но уже устаревших методов аутентификации пользователей ДБО и подтверждения проводимых ими операций по одноразовому SMS-коду. Показательным является международный опыт: за последние 6 месяцев 2019 года 6 крупнейших банков Германии посчитали такой способ подтверждения платежей небезопасным и приняли решение отказаться от него. Аналогичные сообщения поступали из ряда других стран Евросоюза и из Турции. Как известно, проблема заключается в недостатках протокола OKC-7 (SS 7). Уязвимости в этом протоколе позво-



ляют злоумышленникам «незаметно похитить» номер телефона пользователя, даже без ведома Оператора связи, а также «отслеживать» все коммуникации его владельца, и в конечном счёте — похитить денежные средства у ничего не подозревающего легального клиента банка.

— Дарья, давайте обсудим эти вопросы подробнее. Расскажите подробнее о проблеме социальной инженерии, и как с ними бороться?

— Это очень серьёзная проблема, которая настигла, прежде всего, простых граждан. Конечно же, банки активно предупреждают пользователей об опасности, но истории про то, как мошенник «выудил» у клиента код подтверждения и похитил деньги мы слышим всё чаще и чаще.

Существует несколько наиболее массовых сценариев хищений, в которых клиента просят сообщить присланный код подтверждения. Самым распространённым в 2019 году способом стал звонок «представителя службы безопасности банка» с просьбой для отмены «свершающейся прямо сейчас попытки мошенничества» срочно сообщить код из SMS или PUSH. Второй популярный способ — звонок из «кредитного отдела банка» для погашения задолженности. В условиях стрессовой ситуации продиктовать мошеннику код может даже очень осторожный клиент.

«Технологическая» сторона проблемы социальной инженерии заключается в том, что в одном SMS или Push-сообщении невозможно представить все реквизиты платежа, чтобы человек сам видел, какая операция совершается в действительности. Если же дать клиенту возможность подтверждать своё волеизъявление только после просмотра реальных реквизитов и вообще без необходимости вводить какой бы то ни было код, это кратко сократит число успешных для мошенников попыток кражи! В частности, одно из возможных решений проблемы — мобильная аутентификация и подпись в смартфоне — реализовано таким образом, что никаких кодов подтверждения нет, но есть полное отображение реквизитов операции и гарантия того, что на конкретном телефоне клиента будет исполнена именно эта операция.

— Некоторые эксперты говорят, что помимо проблемы социальной инженерии коды в SMS или Push-сообщениях обладают и собственными недостатками, прежде всего, в отношении выполнения требований Положения Банка России № 683-П от 17.04.2019 г. Вы согласны?

— Мы считаем, что сама концепция передачи уже известного банку кода на смартфон клиента через недоверенные каналы связи является порочной и не должна использоваться для подтверждения финансово значимых операций. Кроме того, такие коды только «на бумаге» можно привязать к выполнению требований 683-П о гарантии целостности и авторства подписываемого документа. И именно поэтому судебная практика в России всё чаще сводится к признанию SMS «неперсонифицированным» средством подтверждения и, как результат, банки вынуждены возвращать клиентам похищенные средства.

Но есть ещё и экономический аспект данного вопроса. Несколько лет назад удорожание SMS привело к тому, что банки начали использовать PUSH-коды. На первый взгляд, это казалось оптимальным, и многие перешли на эту технологию. Но эксперты в области безопасности справедливо называют такой вариант «профанацией электронной подписи». Судите сами: на сервере прикладной системы «сгенерировался» какой-то одноразовый пароль (ОТР), он как-то был передан клиенту на смартфон, иногда даже сам за клиента «подставился» в интерфейс и сам «подписал» транзакцию. Это же страшный сон любого специалиста ИБ!

— Итак, для решения перечисленных проблем Вы предлагаете подпись в смартфоне. Чем она отличается от

обычной, и в чём преимущество её использования для клиентов?

— Несколько лет назад мы представили рынку решение PayControl для подписи в смартфоне, призванное кардинально улучшить ситуацию с безопасностью цифровых каналов по отношению к классическим SMS- и PUSH-кодам, и позволяющее «превратить» мобильное устройство в аналог USB-токена с таким же высоким уровнем безопасности и очень простым пользовательским сценарием. Сейчас PayControl — это полноценная платформа мобильной аутентификации и электронной подписи. При её использовании обеспечивается эффективное противостояние наиболее распространённым атакам на клиентов («перевыпуск» SIM-карты, фишинг, подмена документа, социальная инженерия и т.д.). Главный принцип — клиент видит реквизиты платежа на своём смартфоне и подтверждает их одним нажатием кнопки.

Стоит отметить, что в основе PayControl лежит асимметричная криптография, а это значит, что банк не может от имени клиента подписывать какие-либо операции. Закрытый ключ «рождается», «живёт» и «умирает» в конкретном смартфоне — попытки его воспроизведения на другом устройстве ни к чему не приведут. Подпись формируется как функция от 4-х аргументов: реквизиты конкретной операции, закрытый ключ клиента, момент времени и «отпечаток» смартфона пользователя. С точки зрения удобства использования очень важно, что SDK PayControl может быть полностью встроено в мобильное приложение банка.

— А как быть с классическими пользователями Интернет-банка?

— Конечно, концепция Mobile First — это тренд, но мы никогда не забываем о других каналах. Для PayControl абсо-

*«Технологическая» сторона проблемы социальной инженерии заключается в том, что в одном SMS или Push-сообщении невозможно представить все реквизиты платежа, чтобы человек сам видел, какая операция совершается в действительности*



лютно не имеет значения, в каком канале был создан документ, который пользователь подпишет в своём смартфоне. Это может быть не только мобильный банк, но и Интернет-банк, рабочее место операциониста и даже банкомат. Важно то, что информация о совершенной операции приходит прямо в смартфон клиента, где он проверяет детали операции и подписывает её электронной подписью.

Более того, мобильная подпись для пользователей Интернет-банка предоставляет ещё и весьма интересные дополнительные возможности. К примеру — вход без логина и пароля, при помощи смартфона в личный кабинет. Совсем недавно с одним из банков из «топ 5» мы запустили самый масштабный проект для физических лиц, где реализовали не только подпись операций, но и такой вход в Интернет-банк. Работает это так: на экране компьютера вместо окна с логином и паролем отображается QR-код. Вы открываете мобильное приложение банка, считываете QR-код, и автоматически «проваливаетесь» в личный кабинет! Важно отметить, что в этом сценарии исключается перехват логина и пароля клиента, даже если он работает в недоверенной сети.

Аналогично клиент сможет работать при помощи своего телефона и с банкоматами. И для этого не требуется внедрять NFC-модули — нужно лишь обновить ПО. На экране, по аналогии с Интернет-банком, появится QR-код, который клиент сканирует своим смартфоном и получает доступ к своему карточному счёту. Все действия в банкомате, будь то перевод или снятие наличных, клиент подтвердит при помощи смартфона. Банк может даже выдать клиенту виртуальную карту, с которой клиент сможет снимать денежные средства и распоряжаться ими, не имея вообще пластикового аналога на руках. И всё это благодаря полноценной электронной подписи, которая формируется в мобильном устройстве клиента и может однозначно указать на конкретного пользователя и совершённое им действие и подписать любой тип волеизъявления.

— Можно ли с помощью мобильной подписи решить ещё и проблему организации безбумажного офи-

са и подписи договоров клиентами без бумаг?

— Конечно! Клиенты прямо со своего смартфона смогут подписывать любые договоры, которые раньше приходилось подписывать в офисе банка: от открытия новых счетов и карт, до оформления депозитов и кредитов. Сейчас банки тратят огромные средства на печать, подписание, хранение и логистику документов. А безбумажный документооборот, помимо того, что упрощает действия пользователя, ещё и значительно сокращает затраты Банка на коммуникации с клиентами.

— Говоря о подписи договора, мы вплотную подошли к вопросу о формировании на мобильном устройстве квалифицированной электронной подписи. Это возможно?

— Нам удалось предложить рынку два решения для формирования «мобильной» подписи: «облегчённую» версию, которая идеально подходит для обслуживания физических и юридических лиц, а также «полновесное» решение, востребованное в тех областях, где необходима квалифицированная электронная подпись (КЭП). Решение для формирования КЭП при помощи смартфона называется myDSS и представляет собой совместную разработку компаний «КриптоПро» и SafeTech на базе программно-аппаратного комплекса облачной электронной подписи «КриптоПро DSS» и платформы PayControl. В 2018 году на это решение был получен сертификат ФСБ России.

Выбирая из двух решений, очень важно понимать, что различным сегментам клиентов и наборам сервисов необходим разный уровень безопасности и юридической значимости. Например, при дистанционном обслуживании физлиц или небольшого бизнеса простой или усиленной неквалифицированной подписи может быть вполне достаточно, но для предприятий с государственным участием или тех, кто взаимодействует с госструктурами (сдача налоговой отчётности, регистрация юридических лиц и прочее), необходимо использовать сертифицированные средства электронной подписи и усиленную квалифицированную электронную подпись.

— Какие услуги банков уже были реализованы с использованием ква-

лифицированной электронной подписи со смартфона?

— На рынке уже представлены такие сервисы: удалённая регистрация бизнеса из интерфейса банка, сдача налоговой отчётности, дистанционный банкинг, торги и Госзакупки прямо с мобильного устройства. Таких проектов с каждым днём появляется всё больше и больше. Если у нас совместно с регулятором отрасли, совместно с удостоверяющими центрами, с ведущими производителями криптографических решений в России получится предоставить банкам технологии, которые помогут жителям страны экономить время, деньги, силы, то таких проектов станет ещё больше, и мы сможем «оКЭПить» каждого жителя страны, чтобы он стал полноценным участником безопасного электронного взаимодействия.

— В каком направлении происходит дальнейшее развитие ваших технологий мобильной аутентификации и электронной подписи?

Мы активно развиваем решение, проводим интеграцию с различными системами обеспечения безопасности, в частности, с биометрическими системами аутентификации и антифрод-системами. Это необходимо, например, для предоставления банкам возможности «адаптивной аутентификации», а также возможности ещё большего повышения уровня безопасности и удобства клиентов. Интеграция с биометрическими системами позволит добавить дополнительные факторы аутентификации при совершении так называемых «высокорисковых» операций, а использование передовых антифрод-систем позволит «на лету», в момент совершения операции, оценивать риск её подписи и работы пользователя на конкретном мобильном устройстве.

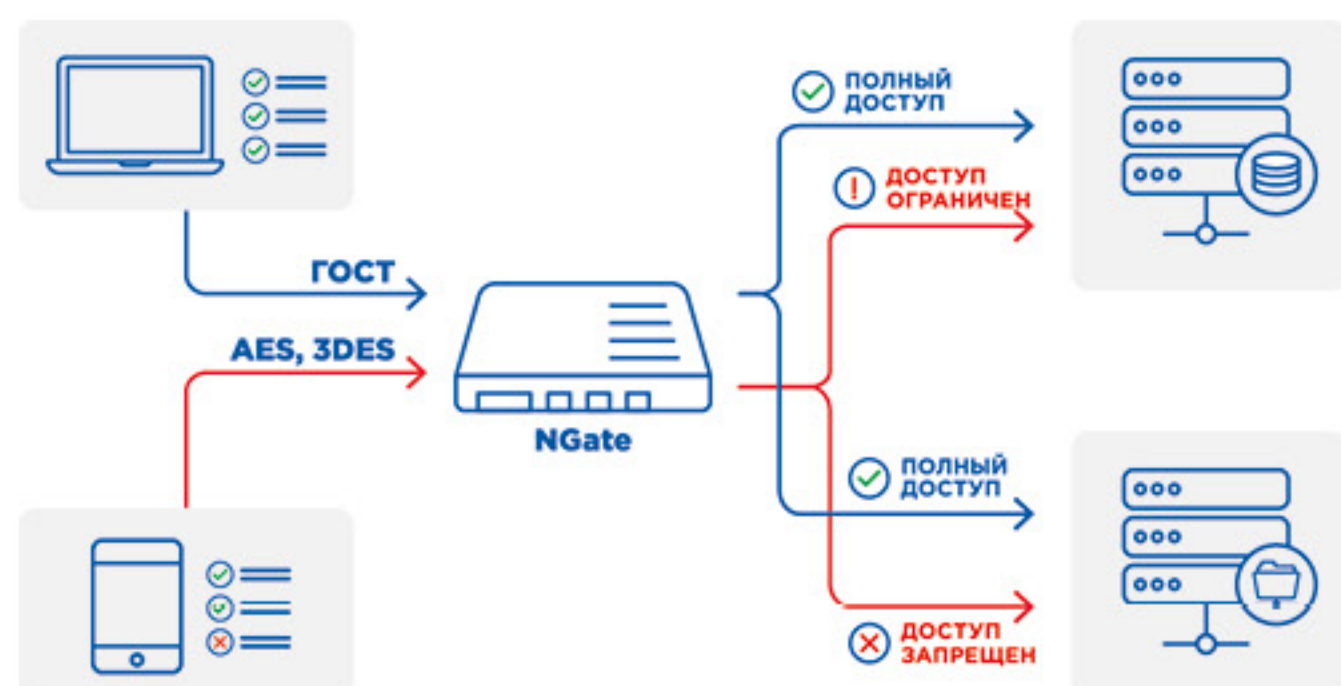
Таким образом, PayControl — это действительно полноценная платформа мобильной электронной подписи и аутентификации, которая позволит банкам, как кубики, собирать те функциональные возможности, которые им необходимо получить. Это позволяет нам говорить о новом классе систем обеспечения безопасности транзакций, которые мы сейчас выводим на рынок, и которые будут «взрывать» его в ближайшие несколько лет.





## КРИПТОПРО NGate

Универсальный высокопроизводительный VPN-шлюз, позволяющий быстро и безопасно реализовать защищённый удаленный доступ к корпоративным ресурсам и информационным системам через незащищённые каналы связи.



### Поддержка ГОСТ и зарубежных алгоритмов

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

### Выполнение требований регуляторов

Серверные и клиентские компоненты NGate сертифицированы по требованиям к СКЗИ и имеют соответствующие сертификаты ФСБ России по классам КС1, КС2 и КС3. Это позволяет использовать NGate для защиты персональных данных при передаче по незащищенным каналам связи, а также для защиты удаленного доступа к значимым объектам КИИ. Кроме этого NGate позволяет реализовать защищенные TLS-соединения при передаче биометрических ПДн в рамках соответствующих взаимодействий в ЕБС.

### Три режима работы

NGate может работать в трех режимах — TLS терминатора, портального и VPN доступа. Режим TLS терминатора используется для снятия нагрузки по обработке TLS-соединений с бэкэнд-серверов и серверов доставки данных. Режим портального доступа — для организации персонального доступа пользователей к опубликованным на портале NGate веб-ресурсам в соответствии с корпоративными политиками ИБ. Режим VPN доступа — для подключения к произвольным ресурсам с помощью VPN-клиента, поддерживающего все популярные платформы (Windows, macOS, Linux, iOS, Android, Sailfish).

### Простая реализация контроля доступа к ресурсам

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

### Масштабируемость

Один узел NGate выдерживает нагрузку до 28000 одновременных соединений с обработкой информационных потоков до 10 Гбит/с в режиме TLS терминатора. Данные характеристики легко увеличить добавлением узлов в кластер.

**КриптоПро NGate**

<http://www.cryptopro.ru/products/ngate>

## КриптоПро CSP Lite

КриптоПро CSP Lite — это новый «облегченный» криптопровайдер на базе флагманского СКЗИ КриптоПро CSP 5.0, который представляет собой новое поколение криптопровайдера, развивающее три основные продуктовые линейки компании КриптоПро: CSP (классические токены и другие пассивные хранилища ключей), ФКН (неизвлекаемые ключи на токенах) и DSS (ключи в облаке).

Преимущества продуктов этих линеек не только сохраняются, но и умножаются в КриптоПро CSP 5.0: шире список поддерживаемых платформ и алгоритмов, выше быстродействие, удобнее пользовательский интерфейс. Но главное — работа со всеми ключевыми носителями, включая ключи в облаке, теперь единообразна. Для перевода прикладной системы на поддержку ключей в облаке или на новые носители с неизвлекаемыми ключами не потребуется какая-либо переработка ПО — интерфейс доступа остается единым, и работа с ключом в облаке будет происходить таким же образом, как и с классическим ключевым носителем.

КриптоПро CSP Lite предназначен для использования в браузерах в различных операционных системах, одновременно реализует функции КриптоПро CSP и КриптоПро ЭЦП Browser plug-in и не требует установки. Его использование сводит к минимуму настройки СКЗИ для пользователя. При этом набор поддерживаемых токенов и смарт-карт может быть динамически настроен под требования конкретного веб-ресурса (электронной площадки, системы ДБО и т.д.).





**Екатерина КРЫЛОВА**  
системный аналитик  
ООО «ЦРТ-Инновации»



**Юлия ФАРАБЕ**  
руководитель проектов  
ООО «ЦРТ-Инновации»



**Иван МЕДЕННИКОВ**  
ведущий научный сотрудник  
ООО «ЦРТ-Инновации»

# GOLDEN VOICES ИЗ РОССИИ

## КАК РАСПОЗНАТЬ ДИКТОРА И ЕГО РЕЧЬ С ДАЛЬНОГО МИКРОФОНА В УСЛОВИЯХ ШУМА?

**В** 2019 году технологии искусственного интеллекта (ИИ) для распознавания речи и диктора на среднем и дальнем микрофонах, соревновались на международном конкурсе VOICES 2019. Две команды научных сотрудников российской ГК ЦРТ заняли первые места в двух номинациях. В статье описываются представленные на конкурс решения.

### НАУЧНЫЙ КОНКУРС — РИНГ ДЛЯ ТЕХНОЛОГИЙ

Международные конкурсы решений на основе искусственного интеллекта сегодня являются площадкой для демонстрации систем ведущих игроков рынка речевых технологий. Конкурс VOICES (Voices Obscured in Complex Environmental Settings — VOICES From a Distance challenge), организованный SRI International, в 2019 году прошёл впервые и стал площадкой для сравнения решений одной из наиболее сложных задач современного машинного обучения — распознавания речи в трудных условиях (с удалённого микрофона, в присутствии внешних источников шума).

Решение такой задачи — ключ к созданию технологий для биометрической идентификации и автоматического распознавания речи, надёжно работающих в различных (акустических) условиях.

Участие команды ГК ЦРТ, входящей с апреля 2019 года в экосистему Сбербанка, в VOICES 2019 обусловлено высокой востребованностью решений для автоматического распознавания речи и распознавания диктора по голосу, а также необходимостью глубоких исследований в этих сферах. С одной стороны, современные алгоритмы машинного слуха обеспечивают высокое качество работы в условиях телефонного канала, с другой, они не позволяют получать аналогичные результаты в условиях удалённого микрофона: точность их работы может снижаться на порядок.

В то же время на рынке наблюдается рост спроса на голосовые ассистенты и другие решения, работающие с использованием речевого интерфейса. Технологии, в которых голос является не только уникальным паролем, но и универсальным интерфейсом для взаимодействия, уже сегодня встраивают-

ся в мобильные устройства, медиасистемы автомобилей, становятся частью умного дома. Кроме того, решения для автоматического распознавания речи и голосовой идентификации диктора используются в умных колонках, решениях для речевой аналитики, ритейла.

Условия конкурса VOICES 2019 во многом отражали ситуацию, сложившуюся в современной науке. Соревнующимся командам было предложено решить две задачи: распознать речь и идентифицировать диктора по голосу в рамках двух категорий:

- ♦ **фиксированная категория** предполагала обучение моделей только на базах из списка, предложенного организаторами — чистой речи, записанной с расстояния до полуметра (ближнего микрофона);

- ♦ **открытая категория** предполагала возможность добавления к обучающим данным любые данные, доступные участникам.

Чтобы принять участие в конкурсе, было необходимо подготовить минимум одно решение для задачи в любой категории.

Итоговое тестирование моделей всех участников проводилось на оригинальной базе VOICES [2], которая включала VOICES development set (множество фонограмм для первоначального тестирования) и VOICES evaluation set (множество фонограмм для итогового тестирования). Фонограммы тестовых баз данных записывались с использова-

*В современной науке тип микрофона определяют условно. Считается, что микрофон, удалённый от диктора меньше чем на 0,5 м — ближний; от 0,5 до 2 м — средний, дальше 2 м — дальний*



нием 12 микрофонов (студийных, динамических, кардиоидных микрофонов SHURE SM58; всенаправленных, конденсаторных, петличных микрофонов AKG 417L; всенаправленного, динамического, петличного микрофона SHURE SM11). Все фонограммы представляли собой монозаписи, с частотой дискретизации 16 кГц и точностью представления 16 бит на отсчёт.

При записи данных, на которых тестировались участники конкурса, микрофоны располагались в определённых местах двух различных комнат. Полезный речевой сигнал проигрывался внутри комнат с использованием высококачественной системы воспроизведения. Динамик данной системы располагался на роботизированной платформе, которая имитировала поворот головы человека по отношению к множеству микрофонов. Речевой сигнал был искажён различными шумами: музыкой, звуком работающего телевизора, множественной человеческой речью на заднем плане, естественным шумом комнаты. Подробное описание условий формирования фонограмм представлено в статье [1].

Собственные разработки, подготовленные в рамках VOiCES 2019, участники представили на специальной сессии Международной конференции Interspeech 2019 в Австрии.

## РЕШЕНИЕ ДЛЯ АВТОМАТИЧЕСКОГО РАСПОЗНАВАНИЯ РЕЧИ

Распознавание зашумлённой речи, записанной на дальний или средний микрофон, — актуальная задача, для которой в современной науке пока не существует универсального решения. Именно этой задаче была посвящена номинация автоматического распознавания речи конкурса VOiCES From a Distance challenge 2019.

Российская команда участвовала в закрытой категории этой номинации. Поэтому единственными обучающими данными для созданных систем стала подвыборка корпуса LibriSpeech, содержащая 80 часов речи, записанной на ближний микрофон. Это и стало основной трудностью: обучать нейронные сети нужно было на чистых данных с ближнего микрофона, а распозна-

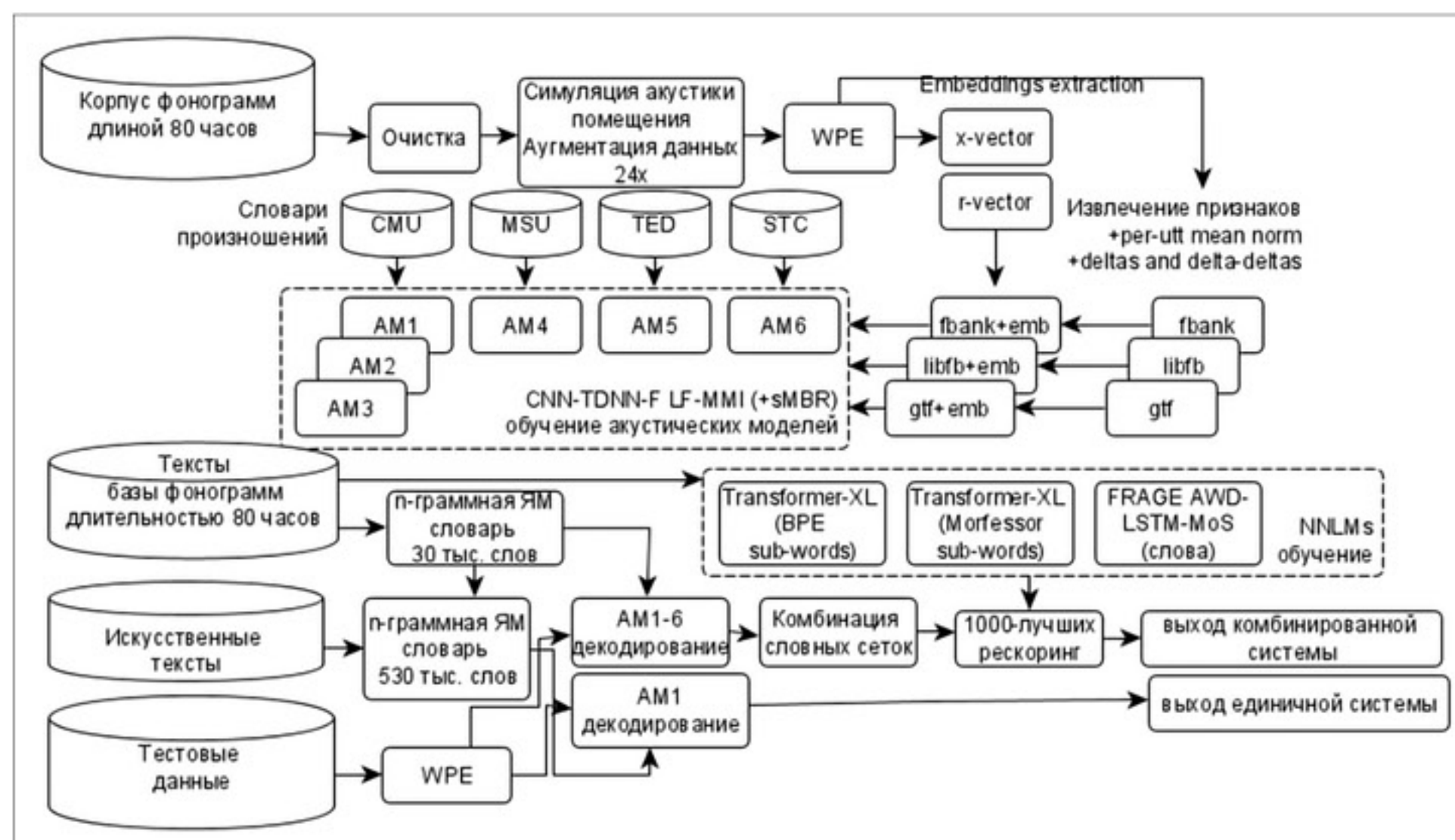


Рисунок 1. Схематичное изображение системы для автоматического распознавания речи, предложенной на конкурс VOiCES 2019 командой ГК ЦРТ

вать в итоге пришлось зашумлённые фонограммы, полученные с помощью дальнего микрофона. Для того, чтобы система работала точнее, команда расширила объём обучающих данных благодаря различным алгоритмам преобразования (аугментации). На основе предложенных обучающих фонограмм были искусственно сгенерированы новые данные, имитирующие фонограммы с удалённого микрофона с наложением шумов. Также использовалась адаптация системы к голосу диктора с помощью x-векторной системы и адаптация к акустике комнаты.

Россияне использовали комбинацию на уровне словных сеток шести акустических моделей, которые создавались на базе различных словарей произношения и входных признаков. N лучших гипотез (n-best) перевешивались тремя языковыми нейронными сетями, обученными на основе слов и подсловных единиц. Для обработки несловарных слов использовались тексты, искусственно сгенерированные с помощью нейросетевой языковой модели. Система автоматического распознавания речи, предложенная на конкурс российской командой, представлена на рисунке 1.

Созданная система на первом этапе производит очистку обучающих данных: удаляются возможные ошибки в эталонных текстовках. Затем, чтобы сделать фонограммы более разнообразными, применялась симуляция акустики помещения. С помощью

программных средств обучающие фонограммы как бы проигрывались в больших и маленьких комнатах разной конфигурации. Полученные таким образом данные очищались от помех, возникших из-за отражения звука в помещении, и использовались для получения отличительных характеристик голоса диктора (x-вектора), характеристик помещения (r-вектора), а также признаков ещё двух типов: 80-размерных блоков фильтров и гамматонных блоков фильтров.

Нормализованные признаки каждого произнесения наряду с их первыми и вторыми производными комбинировались с x-векторами и r-векторами. Применение такого набора признаков в значительной степени схоже с процессом, происходящем в акустическом центре головного мозга, где выделение целевой речи происходит как по частотным признакам, так и по их динамическим характеристикам по времени, с учётом отражения звука о стены и предметы, которая не фильтруется напрямую, но подавляется благодаря механизму внимания.

Российская команда также представила систему без использования нейросетевых языковых моделей, использующая словарь из 530 тысяч слов, включая 500 тысяч искусственно сгенерированных слов. Для того чтобы достичь сходства обучающих данных с тестовыми, речевой корпус LibriSpeech был модифицирован с помощью симу-



лятора акустики помещения с добавлением различных шумов: шума музыки, шумов из корпусов MUSAN, AURO-RA, QUT-NOISE, звуком телепередач. Предложенные организаторами 80 часов записей чистой речи были искусственно увеличены в 24 раза. В результате, было получено 1894 часа модифицированных обучающих данных. Испытания предложенной на конкурс системы на множестве данных для первоначальной проверки показали ощутимое повышение точности распознавания речи.

Адаптация акустической модели к диктору с использованием высокоуровневых дикторских признаков (эмбеддингов) — широко распространённая практика. Опыт участия научных сотрудников ГК ЦРТ в конкурсе CHiME 5 в 2018 году показал, что адаптация акустической модели к диктору повышает качество распознавания речи, записанной не только в телефонном канале и на ближнем микрофоне, но и на дальнем микрофоне. В связи с этим, было решено применить эмбеддинги, извлечённые х-векторной системой. Экстрактор х-векторов с размером 512 был обучен на данных длиной 1894 часов, полученных указанным выше способом.

Наиболее ценным научным результатом конкурса для российской команды стало изобретение г-векторов, высокоуровневых признаков, которые выделяются из речевых данных и содержат информацию об акустической обстановке в помещении. Их выделение из звукового сигнала позволяет адаптироваться к акустике помещения, что в условиях обработки фонограмм, записанных с помощью дальнего микрофона, является более полезным, чем адаптация к диктору. Предварительное сравнение результатов работы системы автоматического распознавания речи, показали, что адаптация к диктору с помощью выделения х-вектора позволяет повысить точность распознавания с 80,6% до 82,46%. Выделение г-вектора повысило точность автоматического распознавания речи до 83,01%. Наибольшего прироста точности (83,53%) удалось добиться в результате сочетания обоих типов адаптации. Проводя аналогию с нейрофизиологией, можно сказать, что

х-векторы и г-векторы в совокупности можно расценивать как паттерн говорящего в непосредственной обстановке разговора, что по всей видимости выделяется и в головном мозге при общении в конкретном случае.

Что касается языковых моделей, они были обучены на наборе текстовых расшифровок для фонограмм из обучающего корпуса. В рамках конкурса были доступны только 4 мБ обучающих текстов. Столь малый объём данных мог повлиять на обучение языковой модели, поэтому дополнительные языковые модели были обучены на двух наборах подсловных единиц, специальным образом подготовленных. Языковые модели на основе рекуррентных нейронных сетей применялись для перевзвешивания гипотез в системе распознавания речи.

Комбинация лучших языковых моделей позволила повысить точность распознавания до 87,14%. Что касается несловарных слов, которые негативно сказываются на работе систем распознавания, в описываемом конкурсе они также были. Множество данных для первоначальной проверки системы содержало 2255 уникальных несловарных слов. Чтобы предотвратить снижение качества распознавания на несловарных словах, языковые модели россиян обучались на искусственно сгенерированных текстах, содержащих более 3 миллионов новых уникальных слов. На этих текстах обучалась n-граммная языковая модель, которая затем интерполировалась с базовой языковой моделью. Словарь итоговой языковой модели был ограничен 500 тысячами наиболее часто генерируемых слов и 30 тысячами оригинальных слов. Это позволило повысить точность распознавания на базе для первоначальной проверки системы с 84,69% до 85,81% для одиночной системы.

Итоговая система автоматического распознавания речи, представленная на конкурс VOiCES 2019, продемонстрировала лучшую среди всех участников точность распознавания: 87,6% на множестве фонограмм для первоначального тестирования, 85,3% на множестве фонограмм для итогового тестирования. По итогам участия в номинации написана статья для специаль-

ной сессии конференции Interspeech 2019, в которой раскрываются подробности реализации выбранных решений [2].

*Состав российской команды: И. Меденников, Ю. Хохлов, А. Романенко, И. Сорокин, А. Митрофанов, В. Батаев, А. Андрусенко, Т. Присяч, М. Корневская, О. Петров, А. Затворницкий.*

## РЕШЕНИЕ ДЛЯ ЗАДАЧИ РАСПОЗНАВАНИЯ ДИКТОРА ПО ГОЛОСУ

Обучение моделей в рамках фиксированной категории конкурса VOiCES 2019 для системы распознавания диктора могло быть реализовано только с использованием баз SITW и VoxCeleb1 и VoxCeleb2. Эти базы данных содержат аудиофайлы, полученные путём записи речи разных дикторов в различных комнатах с разным уровнем шума на несколько видов микрофонов.

Исключением из этого правила стали только детекторы речевой активности, их разрешалось обучать с использованием любых баз данных. Искусственное увеличение объёма данных, имитирующих реальные условия, разрешалось проводить, используя любые публично доступные неречевые аудиозаписи.

В рамках фиксированной категории соревновалось более 20 команд. Решение, демонстрирующее максимальную точность распознавания диктора, разработала команда ГК ЦРТ. Особенность решения [5] заключается в использовании технологий, хорошо зарекомендовавших себя в системах идентификации диктора. При этом в основе систем, представленных в закрытой и открытой категориях номинации, — извлечение высокоуровневых признаков диктора с определённых слоёв нейронных сетей, обученных классифицировать дикторов. Для повышения их устойчивости к различным условиям эти нейронные сети были обучены на специальным образом подготовленных данных на основе баз, предоставленных организаторами. Как и у команды, готовившей систему для автоматического распознавания речи, подготовка обучающих данных включала увеличение их объёма путём имитации акустики раз-



ных помещений. В рамках подготовки финальных систем рассматривались различные подходы препроцессинга признаков, используемых в нейронных сетях. Эти подходы были основаны на применении различных детекторов речевой активности, используемых в решениях ЦРТ.

Система идентификации диктора включал в себя компоненты для удаления искажения звукового сигнала, которое появляется из-за отражения звука от окружающих объектов, для повышения качества обучающих данных. Также на этом уровне извлекались низкоуровневые признаки диктора, которые постобрабатывались скользящим окном шириной 3 секунды. Что касается высокоуровневых дикторских признаков (эмбеддингов), использовались х-векторы и предложенные научными сотрудниками ГК ЦРТ с-векторы [6].

Выделенные признаки дикторов — х-векторы и с-векторы — обрабатывались для повышения их способности разделять дикторов. Объем обучающих данных был увеличен с 1000 до 4000 часов, путем добавления различных типов шумов, для повышения качества работы моделей. Финальное решение, занявшее первое место в фиксированной категории номинации, было получено в результате слияния нескольких подсистем, принимающих решение о

принадлежности голоса тому или иному диктору.

Открытая категория распознавания диктора предполагала снятие ограничений на обучающие данные. В данной категории, команды могли использовать любые речевые базы, в том числе и предоставленные в закрытой категории. Решение российской команды для открытой категории представляло собой обобщение опыта разработки подсистем, разработанных для закрытой категории, а также подбор оптимальной стратегии их нормализации и слияния. При этом точность разделения дикторов была улучшена более чем в полтора раза по целевой метрике minDCF [4]. В открытой категории команда ГК ЦРТ заняла первое место среди четырех компаний.

Разработанные для конкурса системы показали, что х-векторная система, предложенная на конкурс командой ГК ЦРТ, превосходит с-векторную, а увеличение объема данных путём создания искусственной реверберации (отражения звука в помещении) делает систему более устойчивой к непредвиденным условиям. Детектор речевой активности, разработанный для автоматического распознавания речи в ряде случаев помогает добиться более высокого качества распознавания диктора по сравнению с детектором речевой активности на основе энергии.

По итогам участия в номинации распознавания диктора написаны статьи, команда приняла участие в специальной сессии конференции Interspeech 2019 в австрийском городе Грац [4, 5].

*Состав российской команды, победившей в номинации идентификации диктора: С. Новосёлов (руководитель группы голосовой биометрии), А. Гусев, А. Иванов, Т. Пеховский, А. Шулипа, Г. Лаврентьева, В. Волохов, А. Козлов.*

## АНАЛИЗ РЕЗУЛЬТАТОВ И ПОСЛЕДУЮЩИЕ РАЗРАБОТКИ

Несмотря на то, что в рамках конкурса VOICES 2019 от ГК ЦРТ выступали две отдельные команды (одна занималась задачей распознавания дикторов, другая — автоматическим распознаванием речи), им удалось обменяться опытом и технологиями при подготовке итоговых систем:

- ◆ применялись дикторские представления как в распознавании речи, так и в распознавании дикторов;

- ◆ в системе распознавания дикторов использовался детектор речевой активности, основанный на системе распознавания речи;

- ◆ применялся алгоритм очистки звукового сигнала от помех, возникающих в результате отражения звука в помещении, для улучшения качества работы систем распознавания речи и распознавания дикторов;

- ◆ использовались модели для построения импульсных характеристик помещений, которые затем служили для искусственного создания больших объёмов симулированных данных, имитирующих реальные условия (эта процедура необходима при обучении систем распознавания речи и распознавания дикторов).

\* \* \*

Такой подход привёл научные команды ЦРТ к успеху: золоту во всех номинациях. Синергия различных технологий рассматривается учёными компании как один из способов достижения более высокого качества распознавания речи и диктора и будет использоваться в дальнейших разработках.

## ЛИТЕРАТУРА

1. Richey C. et al. Voices obscured in complex environmental settings (VOICES) corpus // Interspeech 2018, Hyderabad, India, 2018.
2. I. Medennikov, Y. Khokhlov, A. Romanenko, I. Sorokin, A. Mitrofanov, V. Bataev, A. Andrusenko, T. Prisyach, M. Korenevskaya, O. Petrov, and A. Zatvornitskiy, «The STC ASR system for the VOICES from a distance challenge 2019,» in INTERSPEECH, 2019.
3. Y. Khokhlov, A. Zatvornitskiy, I. Medennikov, I. Sorokin, T. Prisyach, A. Romanenko, A. Mitrofanov, V. Bataev, A. Andrusenko, M. Korenevskaya, O. Petrov. «R-vectors: New technique for adaptation to room acoustics», in INTERSPEECH, 2019.
4. Novoselov S., Gusev A., Ivanov A., Pekhovsky T., Shulipa A., Lavrentyeva G., Kozlov A., Volokhov V. STC-SID team's speaker recognition system for the VOICES 2019 challenge // VOICES 2019 description, 2019.
5. Novoselov S., Gusev A., Ivanov A., Pekhovsky T., Shulipa A., Lavrentyeva G., Volokhov V., Kozlov A. STC speaker recognition systems for the VOICES from a distance challenge // Interspeech 2019, Graz, Austria, 2019
6. S. Novoselov, A. Shulipa, I. Kremnev, A. Kozlov, and V. Shchemelinin, «On deep speaker embeddings for text independent speaker recognition,» in Odyssey 2018 The Speaker and Language Recognition Workshop, June 26–29, Les Sables d'Olonne, France, Proceedings, 2018, pp. 378–385.



# «КИБЕРСТАБИЛЬНОСТЬ: ПОДХОДЫ, ПЕРСПЕКТИВЫ, ВЫЗОВЫ» 2019

## СТАРЫЙ ВАВИЛОН НОВОГО КАРИБСКОГО КРИЗИСА В КИБЕРПРОСТРАНСТВЕ

**В**ыступая на конференции «Киберстабильность: подходы, перспективы, вызовы» в декабре 2019 года, спецпредставитель Президента РФ по вопросам международного сотрудничества в области ИБ Андрей Крутских упомянул о недавнем интервью Генерального секретаря ООН, в котором тот прямо заявил о своих опасениях возникновения большого конфликта. Мол, «спусковым крючком» для этого конфликта на этот раз станет столкновение в киберпространстве. По словам Андрея Крутских, урегулирование складывающейся в мировом киберпространстве конфронтации рассматривается генсеком ООН в качестве первоочередной задачи.

Оба дня IV международной конференции «Киберстабильность: подходы, перспективы, вызовы» были сфокусированы на анализе ситуации в системе международной кибер- и информационной безопасности (К&ИБ). Кроме обсуждения вопросов ответственного поведения государств в новой среде обитания человечества — киберпространстве — состоялась и гуманитарная дискуссия о степени влияния на человека этой новой среды. Эта дискуссия вышла далеко за рамки традиционных обсуждений т.н. «социальной инженерии», обычно затрагивающих лишь контекст преступлений местечкового масштаба.

### ЭХО ХОЛОДНОЙ ВОЙНЫ

Тон конференции зададо выступление Андрея Крутских. Заявив, что выступает не как официальное лицо, а как учёный-политолог, он заострил внимание на четырёх узловых негативных моментах:

1. отсутствие международно-правовых механизмов для сдерживания

агрессии в киберпространстве и договорённостей о том, какие проявления такой агрессии позволяют применять положения договорённостей ООН о праве на самооборону;

2. официальная позиция США, заявивших о готовности использования всех видов оружия в ответ на ситуацию, которая в одностороннем порядке будет расценена этой страной как кибератака, угрожающая безопасности США;

3. торпедирование США и её партнёрами (в первых рядах которых — Англия, Канада, Австралия, Украина, Эстония) попыток объединения мирового сообщества вокруг решения ключевых проблем глобальной кибербезопасности навязыванием обсуждения явно второстепенных вопросов (в качестве примера можно привести «проблему» обеспечения гендерного равенства в сфере разработки норм информационного права);

4. активизация поддерживаемой российским правительством дискуссии о повышении роли т.н. «искусственного интеллекта» и необходимости повсеместного внедрения соответствующих ИТ-технологий. Эти действия совершенно не учитывают, что такого рода «интеллект» станет первоочередной и легко поражаемой целью нападения из киберпространства.

### ТРЕВОЖНАЯ ПЕРСПЕКТИВА

Резюмируя суть этого и последующих выступлений, можно утверждать, что ключевой проблемой системы международной К&ИБ является отсутствие самой этой системы и нежелание ряда «развитых» стран её создавать.

На сегодняшний день не решён широкий круг задач: от «расшифровки» базовых понятий до подписания обязывающих договорённостей. Вместо

договоров некоторые страны предпочитают творить политику в рамках ограничений в виде т.н. «мягкого» права, до сих пор не избавившись от синдрома однополярного гегемонизма и ощущения вседозволенности.

Такой вывод можно было сделать из выступления Александра Савенкова, директора Института государства и права РАН, который поделился своими оценками состояния международного права в целом и права в сфере информационных технологий в частности. По его мнению, в сфере международных отношений явно наблюдается стремление ухода от конкретики договорных обязательств в направлении провозглашения аморфных «общих принципов» и деклараций.

### ПОЗИЦИЯ ВОЕННЫХ

Представитель Военной академии Генштаба ВС РФ сообщил, что в сложившейся ситуации Вооружённые силы России исполняют свой долг по защите страны от угроз, исходящих из киберпространства, не только в условиях правовой неопределённости, но и в условиях, когда, например, Конвенция Совета Европы от 23 ноября 2001 года рассматривает в качестве допустимых действий проникновение в компьютерные системы сопредельных по киберпространству стран, легитимизируя, фактически, кибершпионаж.

Представитель ВС РФ отметил, что лишь сопутствующие кибератаке разрушения материальной инфраструктуры и гибель людей являются для российских военных критериями развязывания военных действий.

В этих условиях пока нет однозначного вывода о характере ответной реакции российской армии на деста-



билизацию, например, банковской системы страны, источником которой станут действия из киберпространства.

### ПОЗИЦИЯ БИЗНЕСА

В свете тревог учёных, политиков и военных обратила на себя внимание реалистичная позиция бизнеса. В ответ на утверждения об отсутствии одобренных «международным сообществом» официальных указаний по вопросам «демаркации границ» в киберпространстве, методик «атрибуции» агрессора и оценки ущерба из-за киберагрессии, выступивший на конференции представитель «Норильского никеля» отметил, что для специалистов его компании не являются нерешаемыми задачи идентификация источников кибератак и определения нанесённого ущерба.

Некоторые иностранные государства в условиях нынешней формальной правовой неопределённости также не испытывают дискомфорта.

В качестве примеров приводились удар израильских военных в ответ на предполагаемую кибератаку Хезболлы на объекты страны и история противостояния в связи с применением вируса Stuxnet. Тогда кибератака против иранского ядерного объекта довольно оперативно получила «ответку», нанёсшую многомиллиардные убытки киберагрессору, и на какое-то время привела его в чувство, что вызвало всплеск сотрудничества в сфере борьбы за снижение напряжённости в киберпространстве.

### ОШИБКИ ПРОШЛОГО ПОМОГАЮТ

На конференции отмечалось, что в сложившихся условиях Россия ведёт актив-

ную работу по заключению двухсторонних межгосударственных договоров об урегулировании сотрудничества в киберпространстве. Об этом рассказал Сергей Бойко, начальник департамента аппарата Совета безопасности РФ, упомянув о наличии двухсторонних межгосударственных договоров России с Бразилией, Беларусью, Китаем, Индией, ЮАР, Вьетнамом, Туркменистаном.

Тем не менее, нельзя переоценивать значимость этих шагов на фоне усиления глубинных экономических противоречий между региональными группировками государств. На конференции не раз обращались к историческому опыту, вспоминая и о ситуациях, предшествовавших Первой и Второй мировым войнам, когда эффективные мирные инициативы не позволили предотвратить военное противостояние.

Нынешняя же ситуация кризиса в экономике по сравнению с событиями прошлого усугубляется ещё и появлением весьма эффективных инструментов оглушения масс и управления их поведением, подавления воли потенциальных жертв агрессии к сопротивлению.

### УГРОЗА ВИДУ «ЧЕЛОВЕК РАЗУМНЫЙ»

Судьба людей, для которых киберпространство становится привычной средой обитания, стала ещё одной темой конференции. Ибо предпосылки для физической и умственной деградации «детей киберподземелий», «сужденья черпающих из интернет-газет» уже сегодня вызывают опасения исследователей.

Своеобразный итог этому пласту обсуждений подвёл Андрей Юров, науч-

ный руководитель Международного Центра Прав Человека при Санкт-Петербургском Институте Права им. Принца П.Г. Ольденбургского. В качестве основной причины возможной деградации вида «человек разумный» и трансформации его в несколько новых видов, разнесённых по социальной шкале, г-н Юров назвал непонимание серьёзности проблем дегуманизации общества даже экспертами, «упивающимися цифрами» и не понимающими, что они сами уже стали частью этих цифр и инструментами этих цифр. Ведь угрозы гуманитарной сфере, исходящие из киберпространства, в отличие от атомной бомбы, не видны.

Инструментами для борьбы с кибердегуманизацией общества г-н Юров назвал гражданский контроль, способный эффективнее «рамоч» выявить и остановить конкретного киберпреступника, и «новую солидарность людей», осознающих угрозы виду «человек разумный», исходящих из киберпространства.

Длинная реплика г-на Юрова вытащила на божий свет самую суть противоречий строительства новой Вавилонской башни в виде мифического единого киберпространства.

\* \* \*

К сожалению, может оказаться прав Армен Оганесян, сопредседатель конференции, главный редактор журнала «Международная жизнь» МИД РФ, выразивший опасения, что «новая солидарность людей» станет главной целью кибератак.

И весьма вероятно, что не только «кибер».

### BIS-ИНФО

#### В МИД ПОЯВИЛСЯ ДЕПАРТАМЕНТ ПО ИБ

В МИД России создан новый департамент — Департамент международной информационной безопасности (ДМИБ), который будет курировать работу в области международной ИБ, а также противодействовать использованию информационных технологий в военно-политических, террористических и иных преступных целях. Соответствующий указ подписал президент России В.В. Путин. Возглавил структуру А.В. Крутских.

Кроме того, департамент займется «подготовкой предложений по совершенствованию нормативной правовой базы сотрудничества с другими странами, международными организациями и компетентными неправительственными организациями в области информационной безопасности». Он также будет участвовать в «разработке и согласовании национальных мер по информационной безопасности в сфере международного сотрудничества и международных отношений».





Александр БОДРИК  
обозреватель BIS Journal

# SOC-ФОРУМ 2019

В ПРЕДЧУВСТВИИ ЖАЖДЫ ТАЛАНТОВ

**П**ятый юбилейный SOC-форум оставил яркое послевкусие — отрасль была представлена в полном объеме. Два главных вывода: с одной стороны, налицо полноценный рынок услуг по мониторингу и реагированию на инциденты ИБ, — а значит, возможности российского бизнеса по защите своих активов расширились. С другой, в завершение 2019 года мы услышали от представителей ФСТЭК и ФСБ, что надо учиться говорить с бизнесом на его языке, — а значит, такая базовая задача ещё не решена. Заметно и усиление кадрового голода, что в свою очередь окажет давление на качество внутренних процессов поставщиков и потребителей услуг SOC.

## НЕДОСТАТКИ ПАРАДИГМЫ ЗАЩИТЫ

SOC-Форум открылся пленарным заседанием, на котором заместитель директора ФСТЭК России Виталий Лютиков

выступил с сенсационным заявлением: «В моделях угроз (десятках и сотнях — *прим. авт.*), которые поступают в ФСТЭК на согласование и в итоге согласовываются, нет внутренних нарушителей, в том числе привилегированных — системных администраторов». Это значит, что рынок информационной безопасности по-прежнему фрагментирован — банки и телекомы живут своей жизнью, и для них внутренний нарушитель исторически представляет основную угрозу. Государственный сектор ориентируется на выполнение государственных требований и защиты от внешнего нарушителя, не смотря на то, что реализация электронных услуг и цифровизация сделали госорганы крупнейшими хранителями персональных данных в цифровом виде. Это также значит, что мы ещё увидим десятки и сотни инцидентов банального воровства данных, тем более, что по тону г-на Лютикова было понятно, что меры организационно-правового характера

в отношении системных администраторов применяются недостаточно (г-н Лютиков призывал применять их более активно).

По направлению защиты от внутренних нарушителей заместитель начальника центра ФСБ России Игорь Качалин предложил мыслить более системно: положить в основу ИБ организации модель нарушителя, трансформировать всю систему ИБ для учёта возможностей внутреннего нарушителя, считая недостаточным просто рисовать новые планы реагирования на инциденты ИБ.

Кроме концептуальных замечаний коллеги поделились и цифрами о проделанной в 2019 г. работе:

- ♦ Количество выявленных в 2019 г. в рамках ГосСОПКА инцидентов достигло 3000. 90% из них НКЦКИ выявил самостоятельно, направив владельцам КИИ уведомления — 2700 шт. (в 2018 г. заявлялось о 700 уведомлениях — рост в разы, но без расследования инцидентов)





тов на стороне владельцев КИИ нельзя сказать, что это действительно инциденты — максимум подозрения на них — *прим. авт.*).

- ◆ Заключено 42 соглашений о взаимодействии с НКЦКИ (в 2018 г. заявлялось о 18 соглашениях).

- ◆ Количество объектов КИИ за последний год увеличилось в 2+ раза — до 45 410 (с 21 500).

- ◆ Производство отечественных сертифицированных СЗИ увеличилось на 69%.

- ◆ База данных уязвимостей ФСТЭК выросла до 23 545 записей (с 20 256).

В рамках дальнейшей работы форума обсуждались Практические кейсы работы SOC и три классических направления развития SOC — Технологии, Компетенции и Процессы.

### ПРАКТИЧЕСКИЕ КЕЙСЫ

Год назад автор высказывал желание увидеть практические кейсы работы SOC-провайдера (и не только квазимонополиста Ростелеком-Солар). В этом году практические кейсы пока-

зали три компании: Ростелеком-Солар с электроэнергетической компанией с немецким капиталом Юнипро и международным агрохолдингом с российским капиталом Содружество, Ангара Ассистанс с платёжной системой Юнистрим (пострадавшей в конце 2018 года от серии инцидентов ИБ) и SOC Информзащиты с HeadHunter.ru.

Теперь на рынке присутствуют уже как минимум три компании с публичными SOC-кейсами, что формирует понятное пространство для выбора. Впрочем, для формирования шорт-листа, автор рекомендует не забывать Kaspersky и BI.Zone, экспертиза и масштаб деятельности которых обещают заметные результаты.

### ТЕХНОЛОГИИ SOC

На форуме продолжилось обсуждение традиционной темы автоматизации мониторинга и выявления инцидентов ИБ, но всё больший уклон наблюдался в сторону автоматизации расследования и реагирования на инциденты. Для автоматизации и оркестрации про-

цессов расследования и реагирования предлагались решения класса Endpoint Detection & Response, Incident Response Platform, комплексные наборы решений от крупных и средних производителей (преимущественно российских).

Новой темой стали киберучения и соответствующее программное обеспечение, флаг которых особенно активно поднимала компания Инфотекс, а также Ростелеком, в планах которого создать кибертренажер федерального уровня уже в 2020 г. Оба поставщика говорили о том, что квалифицированных кадров ждать неоткуда, надо учить самим.

Неожиданно снова была поднята тема сетевой аналитики в целях выявления кибератак, сразу три компании (Cisco, РТ, Гарда) говорили о необходимости контроля сетевых потоков и выявления в них аномалий. Интересно, что пионер в этой области — американская компания NetWitness была основана ещё в 2006 г., таким образом можно определить отставание нашего технологического стэка минимум в пять лет.





Виталий Лютиков, заместитель директора ФСТЭК России



Игорь Качалин, заместитель начальника центра ФСБ России

## КОМПЕТЕНЦИИ SOC

Нехватка кадров стала столь острой, что перестала быть забавной, и эта тема даже не подвергалась шуточным сомнениям, как другие гипотезы (нужен ли SIEM в SOC? Нужен ли SOC?). О нехватке говорили представители ФСТЭК, ФСБ, Сбербанка, органов местного самоуправления, а в кулуарах и каждый второй участник форума.

Свой рецепт предложил Виталий Лютиков: «Нужно работать с вузами», — и подчеркнул, что такой системной работы он пока не видит. Также эксперт рекомендовал производителям средств защиты предоставлять своё ПО для будущих безопасников в рамках учебного процесса в высших учебных заведениях. Но тут стоит заметить, что вузы сами далеко не всегда хотят работать с компаниями по направлению ИБ, иногда даже с самыми крупными. Расположенность вуза к сотрудничеству, помимо прочего, зависит от качества презента-

ции возможностей компании, которую проводят её представители, «запах денег» и умения «продавать» компанию руководству кафедры.

А вот Муслим Меджлумов, директор блока MSS BI.ZONE, поделился своей формулой с упором на развитие вчерашнего студента внутри компании: («высшее образование» + «системное мышление») × «институт наставничества в компании».

Компетенциям («людям») SOC была посвящена отдельная секция, на которой, в частности, HR-директор Ростелеком-Солар Мария Сигаева поделилась целым списком инструментов по работе с вузами: с чем приходить и куда приходить (Рисунок 1).

## ПРОЦЕССЫ SOC

Фундаментальным оказался доклад руководителя SOC BI.Zone Теймура Хеирхабарова, который рассказал, как в зрелых SOC (автору известны в России,

как минимум, четыре таковых) ведётся прикладной threat intelligence и организован процесс разработки правил корреляции (use case management).

Совсем с другой стороны показал SOC начальник отдела ДИТ Москвы Валерий Комаров. Из его презентации стало понятно: необязательно иметь десятки серверов и технологий и «городить космический корабль», чтобы постепенно, шаг за шагом растить практики регистрации, расследования и реагирования на инциденты ИБ и информационного обмена с регулятором. Среди крайне полезных результатов работы процессов (процессных артефактов) Валерий назвал журнал учёта компьютерных инцидентов, карточку и форму регистрации компьютерного инцидента. Для работы же самих процессов (предпосылки) нужны приказ о назначении ответственных, должностные инструкции ответственных, регламент выявления и реагирования на компьютерные инциденты, план реагирования на компьютерные инциденты и регламент взаимодействия с НКЦКИ. В этом же докладе Валерий подчеркнул, что специалистов для обеспечения безопасности КИИ на объектах КИИ в достаточном количестве никогда не будет. Палочкой-выручалочкой эксперт видит тут «Инструкцию» (выстроенные процессы ИБ — прим. авт.). Кстати, некоторый доступ к экспертизе Валерия может получить каждый читатель BIS Journal через открытые методические рекомендации по защите КИИ и ПДн, доступные на сайте ДИТ Москвы: <https://www.mos.ru/dit/documents/informatcionnaia-bezopasnost/>.

### КОМУ ИДТИ

Нанимающему менеджеру  
Сотруднику HR-службы  
Сотруднику отдела по работе с молодежью  
Сотруднику отдела по работе с соц. программами

### С ЧЕМ ИДТИ

Мастер-класс  
Лекции  
Практические занятия  
Участие в днях карьеры и ярмарках вакансий  
Партнерство – НИРы, НИОКРы, темы магистерских

### КУДА ИДТИ

Факультет или кафедра  
Студенческий профком  
Студенческий центр карьеры  
Индивидуально к преподавателю

### ЗАТРАТЫ

Ваше время  
Ваш бюджет

Рисунок 1. Инструменты по работе с вузами (из презентации HR-директора Ростелеком-Солар Марии Сигаевой)





## ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КИИ И АСУ ТП

С точки зрения Виталия Лютикова, для безопасности КИИ необходимо внедрение риск-ориентированного подхода, и Ф3-187 де-факто внедряет этот подход на объектах КИИ. В сущности, Ф3-187 де-факто требует оценки влияния рисков ИБ КИИ на риски государства. Однако специалисты ИБ оказались не готовы общаться с производителями — полноценно лидировать в процессе оценки рисков ИБ КИИ. Почему? Ответ прост: профессиональное сообщество ИБ не смогло довести представление о рисках ИБ на понятном руководителям промышленных предприятий языке и, соответственно, внедрение технических мер отстаёт от законодательной основы по защите КИИ.

Впрочем, крупные организации намеренно не спешат с внедрением технических мер, к примеру, представитель Россетей заявил, что в полной мере обеспечение безопасности КИИ будет реализовано на объектах КИИ Россетей к 2023 году.

С другой стороны, представитель Самарской области рассказал о радикальной нехватке всех видов ресурсов и при-



вёл в пример случай, когда специалист регионального SOC ушёл работать официантом на большую зарплату. И этот рассказ не удивляет (по крайней мере, автора), ведь при стагнирующей не первый год экономике брать заметные деньги на защиту КИИ и создание центров ГосСОПКА многим государственным организациям просто неоткуда.

С мнением г-на Лютикова о важности риск-ориентированного подхода перекликается и замечание экс-директора по ИБ глобальной сети дата-центров LeaseWeb (штаб-квартира в г. Амстер-

дам) Фреда Стрифлэнда: «В конце концов управление рисками организации является одной из обязанностей совета директоров компании».

Однако ФСТЭК России вводит и новые требования к операторам КИИ. В частности, с 1 января 2021 г. вводятся требования к квалификации руководителей и специалистов подразделений по безопасности объектов КИИ. Они заметно мягче аналогичных по сути требований для лицензиатов ФСБ, и за год все желающие организации смогут переподготовить своих специалистов.





Впрочем, скорее всего мы увидим аналогичную процессу категоризации картину всяческого затягивания/запоздывания и в процессе развития квалификации специалистов по безопасности КИИ. Заместитель начальника управления ФСТЭК Елена Торбенко отдельно отметила, что курсы переподготовки и/или повышения квалификации для руководителей и работников подразделений по обеспечению безопасности КИИ должны быть целостными. К примеру, не два курса по 36 часов, но один курс на 72 часа.

Еленой были даны ответы и на ряд других злободневных вопросов по категорированию КИИ:

- ♦ водоканалы не являются субъектами КИИ по виду деятельности «транспортировка воды», так как не относятся к сфере транспорта из 187-ФЗ.
- ♦ СКУД и камеры наблюдения — не объекты КИИ.
- ♦ органы муниципальной власти не могут быть субъектами КИИ, но субъектами КИИ точно будут подведомственные им организации.
- ♦ в форме категорирования нужно заполнять все поля.
- ♦ ФСТЭК России в любом случае предоставит ответы на сведения, представленные по результатам категорирования,

независимо от того, какие там объекты указаны. Но сейчас с направлением данных ответов наблюдаются проблемы.

### СООБЩАЮЩИЕСЯ КАДРОВЫЕ СОСУДЫ. ВМЕСТО ЗАКЛЮЧЕНИЯ

На самом деле кадрового голода в сфере ИБ в России нет. Ещё нет, но уже близится кадровая «чёрная дыра». В 2020 г. вступят в силу изменения в трудовом законодательстве Германии, направленные на привлечение экспертов из стран вне ЕС, будет реализован Brexit, вытесняющий европейские ИБ-кадры из Соединённого Королевства, а предприимчивые голландские рекрутеры с контрактными окладами по 7–9 тыс. евро в месяц уже добрались до Москвы, и «Победа» уже год как открыла рейсы в Эйндховен.

Однако на горизонте маячит гораздо более страшная угроза, чем будто спящая в летаргии Европа. Осенью 2019 года киевские ИТ-компании поставили новые рекорды по окладам специалистам: DevOps Lead — \$12 тыс. чистыми, DevOps Engineer — \$7 тыс. Американские компании заливают в киевский аутсорсинг десятки и сотни миллионов долларов, в Киеве по-прежнему большинство населения говорит

по-русски, цены на жизнь в два раза ниже московских, мягкий миграционный режим и десятки оборотистых ИТ-рекрутеров. А тематика DevOps, с одной стороны, будет расти и расти (поддерживая цифровую трансформацию), а с другой, добрая половина лучших экспертов SOC как раз и обладает DevOps-компетенциями.

\*\*\*

Возможно, отражением упомянутых угроз нужно заниматься совместно. Регуляторам — пролоббировать давно назревшее введение обязанности владельцев информационных систем ПДн информировать субъектов ПДн об утечках ПДн. В США и Великобритании подобная практика привела к росту значимости ИБ и повышению конкурентоспособности местных рынков труда. А организациям — создавать условия труда и корпоративную культуру такими, чтобы от них не хотелось уходить. Лишь в общих усилиях есть шанс удержать кадровый фронт против могучих (ИБ-бюджет JPMorgan, Bank of America и др. подобных организаций — около \$700 млн каждый), но всё же разрозненных конкурентов за ИБ-таланты.





**Рузанна АХОБЕКОВА**  
юрист российской практики  
ИС, ИТ и телекоммуникаций  
Dentons, аспирант РГАИС



**Виктор НАУМОВ**  
управляющий партнёр офиса в Санкт-Петербурге, руководитель российской практики ИС, ИТ и телекоммуникаций Dentons, кандидат юридических наук

# КАК НЕ УТРАТИТЬ ПРАВА НА ПО

## ПРАКТИЧЕСКИЕ ВОПРОСЫ ПРАВОВОЙ ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

**С**егодня сложно представить компанию, в которой бы активно не использовались программы для ЭВМ. Не являются исключением банки и финансовые организации, для которых программы для ЭВМ в составе информационных систем и ИТ-услуги на их основе — неотъемлемая часть и во многом залог успешного бизнеса.

В этой связи многие банки не только приобретают и используют лицензионное программное обеспечение и заказные разработки, но и развивают собственную разработку. Поэтому вопросы правовой защиты программного обеспечения во всём многообразии ситуаций их создания и использования становятся как никогда актуальными, в том числе для банков. Об этом свидетельствуют и рекомендации Банка России, который в качестве одной из угроз информационной безопасности называет утрату прав (лицензий) на использование отдельных видов программ<sup>1</sup>.

Какие вопросы необходимо учитывать банкам и другим компаниям в процессе разработки и использования программного обеспечения? В настоящей статье авторы дают ответ на этот во-

прос, обобщая многолетний опыт юридического сопровождения «софтверных» проектов.

Статья изложена в виде небольших разделов, каждый из которых освещает отдельный «проблемный» вопрос, на который необходимо обратить внимание, чтобы не потерять права на программу или не оказаться в ситуации нарушения прав третьих лиц.

Стоит отметить, что в статье освещаются основные вопросы, но, конечно же, далеко не все. Так, отдельный интерес представляют вопросы создания и использования баз данных, которые остались за рамками настоящего материала.

### 1. ПРАВОВОЙ РЕЖИМ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Как показывает практика, у правообладателей не всегда есть понимание правового режима программного обеспечения, то есть того, какие элементы программы охраняются, а какие — нет, какое использование программы является нарушением.

Между тем, потенциальный правообладатель должен понимать правовой режим программ.

С точки зрения права, программа для ЭВМ — это объект **авторского права**, который по своему правовому режиму приравнен к литературному произ-

ведению. В этой связи, по общему правилу, охраняемой частью программы является форма, то есть код (исходный и объектный), и аудиовизуальные отображения, порождаемые программой. Содержание/суть программы (к ним, например, может быть отнесен функционал программы) авторским правом не охраняются. Это означает, что, вероятно, в большинстве случаев нарушением прав на программу будет признаваться буквальное или почти буквальное копирование кода (аудиовизуальных отображений). Правовой статус технических элементов, например, алгоритмов и логики, которая заложена в коде (вернее, идей и принципов построения этих алгоритмов), до конца не определён. Учитывая специфику авторско-правовой защиты, есть основания полагать, что такие элементы не всегда будут охраняться.

Чтобы суть правовой охраны объектов авторского права была понятнее, можно привести следующий пример. Если в литературном произведении изложен рецепт приготовления блюда (пусть даже очень оригинального), использование такого рецепта для приготовления блюда не будет считаться нарушением. Нарушением будет являться копирование текста, при условии, что такой текст является оригинальным результатом творческого труда.

<sup>1</sup> См., например, Ф.Я. Держинский «Об опасности иностранного ПО и рекомендациях Банка России», BIS Journal № 4(15)/2014.



## Если правообладатель понимает, что в конкретной программе особую ценность представляют принципы построения алгоритма/логики или иное техническое решение, необходимо задуматься о патентовании

Авторское право не охраняет идеи, концепции, принципы, методы, процессы, системы, способы, решения технических, организационных или иных задач, открытия, факты, языки программирования (п. 5 ст. 1259 ГК РФ). Например, на этом основании российские суды отказали в иске испанской компании к Первому каналу за использование формата телепередачи «Один в один». Суд по интеллектуальным правам следующим образом мотивировал своё решение: «Производственная библия является литературным произведением. В нём описано содержание телепередачи «Ваше лицо кажется мне знакомым» (перечислены её основные элементы, технология производства, принципы кастинга, технического оснащения, расположение камер и иные технические вопросы, в т. ч. расписание репетиций, примеров грима). Данное произведение включает в себя как охраняемые элементы (фотографии, логотип, схема), так и не охраняемые (концепции, идеи, принципы, методы, способы).

Суду не представлено доказательств того, что в спорной программе использовалось указанное литературное произведение или его часть. Как и доказательств того, что при её создании были использованы какие-либо части программы «Один в один». Ответчиком не отрицается факт использования идеи, метода. Вместе с тем, использование идеи, концепции нарушением авторского права в смысле ГК РФ не является»<sup>2</sup>.

**Патентное право**, в отличие от авторского права, охраняет содержание решения, а не его форму.

Поэтому, если правообладатель понимает, что в конкретной программе особую ценность представляют принципы построения алгоритма/логики или

иное техническое решение, необходимо задуматься о патентовании.

Яркой иллюстрацией того, как суды могут толковать предмет правовой охраны программ, является следующий судебный спор<sup>3</sup>. Новозеландская компания *OTOY New Zealand Limited*, правообладатель программы для рендеринга, обратилась с иском о нарушении к компании *Пинксофт* — российскому разработчику аналогичной по функционалу программы. В итоговом решении суд по результатам экспертизы отказал в удовлетворении иска на том основании, что буквального совпадения в исходном коде программ не было обнаружено. То, что в обеих программах используется один алгоритм обработки данных не свидетельствует о нарушении: «...законодательство не запрещает реализацию двумя разными программами для ЭВМ полностью или частично одного и того же алгоритма обработки данных, либо использование такого алгоритма в одном из множества модулей программ, такие программы не могут признаваться воспроизведёнными (скопированными) либо переработанными (модифицированными), если они имеют существенно разные исходные тексты/коды программ, о чём свидетельствуют метрики эксперта»<sup>4</sup>. Если бы у новозеландской компании был патент на алгоритм, действующий на территории России и защищающий алгоритм, она смогла бы предотвратить использование этого алгоритма на основании патентного права.

Указанный судебный спор связан с самостоятельной ёмкой задачей, на которую стоит обращать внимание при разработке и использовании программ

для ЭВМ. Это оформление **служебных разработок**, то есть разработок, которые создаются работниками в пределах установленных для них трудовых обязанностей. Дело в том, что основателем российской компании-ответчика в указанном выше споре являлся бывший работник новозеландской компании, который, уйдя от работодателя, успешно занялся собственным делом, создав конкурирующую программу с похожим функционалом. Причём истец приводил аргументы о том, что бывший работник заимствовал разработки, созданные им в период трудоустройства у истца, но доказать ничего не смог.

## 2. ОФОРМЛЕНИЕ И УЧЁТ ПРАВ НА СЛУЖЕБНЫЕ РАЗРАБОТКИ

Существует распространённое заблуждение о том, что все разработки, которые создаются работниками компании, включая программы, автоматически принадлежат компании.

На самом деле, это не совсем так. Чтобы права принадлежали работодателю, необходимо правильно оформить трудовые отношения с работниками и документы по созданию программ. Трудовая функция работника должна недвусмысленно предусматривать обязанность по созданию программ (написанию кода, разработке интерфейса и т.д.). Если у работника неоднозначное название должности, в трудовом договоре, должностной инструкции и иных документах прямо не указано, что в обязанности работника входит создание программ, то работодатель попадет в зону риска: разработки, созданные этим работником, могут быть признаны неслужебными.

Здесь стоит привести примеры из судебной практики. В одном из дел суд посчитал, что права на программу, созданную работником, принадлежат не работодателю, а работнику, потому что последний был принят на должность «дизайнера-верстальщика», в обязанности которого не входит создание программ<sup>5</sup>. Интересно, что работник, по сути, в рабочее время занимался в основном созданием программы.

<sup>2</sup> Постановление Суда по интеллектуальным правам от 8 мая 2015 г. № C01-320/2015 по делу № А40-84902/2014.

<sup>3</sup> Апелляционное определение Московского городского суда от 16.05.2018 по делу №.33-15686/2018.

<sup>4</sup> Решение Московского городского суда от 5 декабря 2017 г. по делу №.33-15686/2018.

<sup>5</sup> Решение Псковского городского суда по делу № 2-2496/2011.



Из последних споров можно вспомнить спор между компанией ООО «Интервим» (дочерняя компания Veeam Software) и её бывшим работником<sup>6</sup>. Работнику удалось отсудить в первой инстанции у бывшего работодателя двадцать три миллиона рублей за незаконное использование его программы<sup>7</sup>. Поскольку судебное заседание по этому спору было закрытым, не все детали по нему доступны. Однако, как следует из открытых источников, в том числе публичных выступлений самого работника, у него не было явной должностной обязанности по созданию программ, частично программа создавалась до трудоустройства. Поэтому созданную работником программу работодатель мог использовать только на основании договора с работником.

Особую сложность представляют случаи **совместной разработки программ** работниками из разных, но аффилированных компаний.

Казалось бы, какие могут возникать проблемы в такой ситуации. Ведь компании группы вряд ли будут предъявлять друг другу иски. Однако сложности могут возникнуть, например, при продаже программы (или компании, для которой такая программа является основным активом). Неопределённая ситуация с правами на программу<sup>8</sup> может негативно сказаться на потенциальной сделке. Чтобы избежать каких-либо рисков при совместной разработке работниками группы компаний, необходимо заранее структурировать такие проекты и детально определять в договорах между компаниями права сторон на результаты работ.

Наконец, стоит отметить, что оформление прав на служебные разработки не устраняет все потенциальные риски, связанные с правами на собствен-

*При возникновении судебного спора (в том числе о правах на служебные программы) именно сторона, имеющая солидную доказательную базу, выигрывает спор*

ные разработки. Крайне важным элементом является **учёт собственных разработок**, без которого сложно доказывать их служебный характер. При возникновении судебного спора (в том числе о правах на служебные программы) именно сторона, имеющая солидную доказательную базу, выигрывает спор. Учёт служебных программ может быть организован как в традиционной документальной форме, так и в электронном виде. Здесь законодательство и судебная практика не предъявляют особых требований. Главное, чтобы можно было соотнести конкретную разработку с соответствующими работниками и их трудовыми обязанностями.

### 3. НЕЗАКОННОЕ ИСПОЛЬЗОВАНИЕ ПРОГРАММ И ИНЫХ ОБЪЕКТОВ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ ТРЕТЬИХ ЛИЦ

Следующая распространённая проблема, с которой сталкиваются компании — это незаконное использование программ третьих лиц, в том числе в собственных разработках.

Рассмотрим две ситуации нарушения прав третьих лиц: а) нарушение условий лицензионных договоров при использовании программ третьих лиц и б) использование чужих программ в собственных разработках.

Эти случаи незаконного использования программ третьих лиц имеют разные причины и последствия. В этой связи имеет смысл рассматривать их отдельно.

#### 3.1. Нарушение условий лицензионных договоров

Как правило, незаконное использование лицензируемых продуктов возникает вследствие недостаточного учёта прав на программы третьих лиц, которые используются в хозяйственной деятельности. Особенно это актуально для больших компаний, которые используют много разных программ. В такой

ситуации можно «упустить» истёкший срок лицензии или допустить большее количество пользователей, чем разрешено лицензией.

Условия лицензирования некоторых программных продуктов не всегда могут быть понятны, особенно для ИТ-специалистов. Нередко, помимо самого лицензионного договора, который подписывается сторонами, обязательными являются условия различных стандартных правил и положений, на которые по тексту договора есть ссылка. Как правило, такие стандартные документы публикуются на сайте компании-правообладателя программы.

В большей степени сложность вызывает интерпретация положений лицензии о способах использования программы (хотя, конечно, во многом сложности интерпретации зависят от специфики программы). Часто компании сталкиваются с проблемой невозможности внесения изменений в код программы, в том числе в целях адаптации и интеграции этой программы с разными устройствами и другими программами.

#### 3.2. Незаконное использование в собственной разработке

Чаще всего незаконное использование чужого кода в собственной разработке возникает в связи с тем, что **работники используют собственные разработки** или разработки, которые они создавали в период трудоустройства у **предыдущего работодателя**.

Здесь важно отметить, что какие-то элементы, например, идеи/принципы построения технических решений использовать можно (о чём было сказано выше), но при этом они не должны представлять объект, защищаемый в качестве конфиденциальной информации прошлого работодателя. Несомненно, нельзя копировать исходный код без законных оснований.

Но ошибиться может каждый и использовать чужой код могут не только работники, но и разработчики, кото-

<sup>6</sup> См. информацию по этому спору, например, <https://300.pravo.ru/>

<sup>7</sup> На момент написания настоящей статьи решение суда первой инстанции было отменено судом второй инстанции, однако окончательный исход дела еще не определен.

<sup>8</sup> Если в разработке участвуют работники разных компаний, ни одну из этих компаний невозможно назвать единственным правообладателем (за исключением случаев, когда отношения между этими компаниями имели надлежащее договорное оформление, что на практике является довольно редкой ситуацией).





рым компании поручают разработку программ по договору заказа.

Какие риски таит даже не очень значительное на первый взгляд заимствование? Риск заключается в том, что правообладатель переработанной программы не сможет использовать программу, которую создали его работники (исполнители по договору). Таким образом, он оказывается в ситуации наличия у него «парализованных» прав. В дополнение, правообладатели заимствованных элементов могут предъявлять иски о нарушении исключительных прав.

Вопросы использования переработанных программ для ЭВМ также актуальны в сфере использования программ для ЭВМ из *Единого реестра российских программ для электронных вычислительных машин и баз данных*<sup>9</sup>, когда некоторые из зарегистрированных программ представляют собой переработку аналогов, не находящихся в этом реестре. Здесь ключевым правовым вопросом становится квалификация пределов переработки исходных объектов

и то, действительно ли в ходе неё создавался самостоятельный объект интеллектуальных прав.

Судебная практика показывает, что незаконное использование в собственной разработке чаще всего возникает именно потому, что работники и контролирующие разработку менеджеры не очень внимательно относятся к заимствованиям. Если формулировать иначе, отсутствует достаточный контроль над тем, что именно используется в разработке.

Здесь можно привести два примера из судебной практики.

В первом случае истец обратился в суд, потому что его бывшие работники использовали части принадлежащих ему программного кода и пользовательской документации в разработках для нового работодателя<sup>10</sup>. Суд согласился с доводами истца и удовлетворил иск. В этом споре интересно то, что суды анализировали использование не только самой программы, но и руководства пользователя.

Во втором случае тоже фигурировали бывшие работники истца, но реше-

ние было вынесено в пользу ответчика, т.к. совпадения в кодах программ были вызваны объективными факторами, а не незаконным заимствованием<sup>11</sup>. Обе программы были созданы на основе платформы 1С: Предприятие 7.7.

#### 4. ИСПОЛЬЗОВАНИЕ ПРОГРАММ С ОТКРЫТЫМ ИСХОДНЫМ КОДОМ

Последний вопрос, который будет рассмотрен в настоящем обзоре ключевых вопросов в сфере защиты и использования программ, это использование Open Source Software — программ с открытым исходным кодом (далее для краткости — «с открытым кодом»). При использовании таких программ необходимо учитывать несколько моментов.

*Во-первых*, программа с открытым кодом — это программа, которая имеет правообладателей и распространяется по лицензионному соглашению. Такое лицензионное соглашение, открытая лицензия (в России она регулируется ст. 1286.1 ГК РФ), имеет юридические особенности. Между тем, требования

<sup>9</sup> Реестр создан в соответствии со статьёй 12.1 Федерального закона «Об информации, информационных технологиях и о защите информации».

<sup>10</sup> Постановление СИП от 31 мая 2017 г. по делу № А40-141340/2015.

<sup>11</sup> Постановление СИП от 17 марта 2017 г. по делу № А27-6440/2013.



такой лицензии необходимо соблюдать, как и требования любой другой лицензии. Нарушение условий открытой лицензии может повлечь юридическую ответственность и запрет на использование программы.

Зарубежная судебная практика о нарушении условий открытых лицензий является более развитой, чем российская. Так, интерес представляет дело, рассмотренное ещё 10 лет назад во Франции, где был спор между поставщиком компьютерного оборудования со встроенной программой для ЭВМ и покупателем такого оборудования. Покупатель заявлял о нарушении договорных условий, в том числе<sup>12</sup>, в связи с непредставлением поставщиком и разработчиком оборудования исходного кода программ и удалением текстов лицензии вопреки требованиям GNU GPL. Апелляционный суд Парижа поддержал доводы покупателя о нарушении условий GNU GPL<sup>13</sup>.

Во-вторых, программы с открытым кодом могут содержать условия, которые являются обременительными для конкретного проекта или компании. Например, использование в разработке кода, распространяемого по strong copyleft-лицензии, впоследствии будет означать необходимость предоставления исходного кода, а также прав на модификацию и последующее распространение всем пользователям этой разработки. Некоторые лицензии предусматривают иностранное применимое право и подсудность иностранным судам. Например, лицензия Red Hat предусматривает право Англии и подсудность английским судам, что означает необходимость юридического анализа, исходя из соответствующих национальных норм.

Наконец, стоит отметить, что существуют особенности, которые связаны с правовым режимом открытых лицензий. Например, в части гарантий лицензионной чистоты, распоряжения правами на продукт переработки, ко-

## Ответом на юридические риски в сфере оборота ПО является построение специального бизнес-процесса по защите и управлению правами на программы для ЭВМ, а также другие объекты ИС

торый содержит элементы открытого кода. Полноценное рассмотрение этих особенностей в рамках настоящей статьи не проводится, их рассмотрение может быть предметом отдельной статьи.

Главный вывод, который можно сделать из настоящего раздела, состоит в том, что в силу массового распространения и популярности программных решений на базе открытого кода, им необходимо уделять отдельное внимание.

### 5. ВЫВОДЫ: РАЗРАБОТКА И ИСПОЛЬЗОВАНИЕ ПРОГРАММ ДЛЯ ЭВМ КАК ПРЕДМЕТ ДЛЯ ЮРИДИЧЕСКОГО БИЗНЕС-ПРОЦЕССА

Очевидно, что в крупном технологически развитом бизнесе, к которому относится в т.ч. большинство банков, много авторов и разработчиков, которые, несомненно, без злого умысла (за исключением редких ситуаций):

- ♦ используют прошлые наработки с предыдущих мест работы;
- ♦ заимствуют решения, не определив их правовой статус (например, дизайн интерфейса, код Open Source Software);
- ♦ уносят наработанное при увольнении и, к сожалению, могут требовать за это денежную компенсацию или, даже, исключительные права на программные решения, запрещая организациям использовать последние.

Увы, немало «ответственных» менеджеров в организациях, при этом:

- ♦ небрежно относятся к конфиденциальной информации, к организации учёта создаваемых служебных объектов и контролю законности приобретения прав;
- ♦ параллельно участвуют в схожем бизнесе, используя знания и решения с текущего места работы;
- ♦ иногда даже при уходе переманивают с собой ключевых разработчиков.

Всё это может происходить в больших холдингах, где много организаций,

подрядчиков и информационных систем, где в потоках информации в них всех можно легко потеряться.

Это означает, что единственным методологически правильным ответом, на всё возрастающие юридические риски в сфере оборота программного обеспечения, является построение специального бизнес-процесса по защите и управлению правами на программы для ЭВМ, а также другие объекты интеллектуальной собственности (ИС), в рамках которого происходит:

- ♦ Идентификация создаваемых и приобретаемых различных по своей правовой природе объектов ИС;
- ♦ Обеспечение ИС правовой охраной;
- ♦ Приобретение прав на ИС у третьих лиц;
- ♦ Учёт прав на ИС (управленческий, налоговый, бухгалтерский);
- ♦ Коммерциализация ИС в продуктах и услугах;
- ♦ Лицензирование прав на ИС;
- ♦ Использование Open source;
- ♦ Контроль за выплатой вознаграждений в сфере ИС;
- ♦ Выявление, финансовая оценка и минимизация рисков в сфере ИС;
- ♦ Мониторинг нарушений исключительных прав на объекты ИС компании и их пресечение.

\* \* \*

Не имея целью раскрыть в рамках настоящей статьи особенности указанного бизнес-процесса, нужно отметить, что его «сердцем» должен быть реестр объектов ИС и прав на них. А сам процесс должен быть автоматизирован с обязательной интеграцией с существующими информационными системами — от сред разработки программ до систем бухгалтерского учёта.

<sup>12</sup> Названное дело было комплексным и вопросы правомерного использования программ с открытым кодом были не единственными, которые рассматривались в рамках дела

<sup>13</sup> Решение Апелляционного суда Парижа 04/24298 от 16.09.2009 (<http://fsffrance.org/news/arret-ca-paris-16.09.2009.pdf>).





Дмитрий РОМАНЧЕНКО  
директор департамента ИБ IBS

# «ПРОПУСК» В ЗАВТРА ИНФОРМАТИЗАЦИИ

РУБЕЖИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ  
В ПЕРИОД ИТ-ТРАНСФОРМАЦИИ

**ИТ**-трансформация — процесс, идущий в мире и в России долгие годы. Но в последний десяток лет данный процесс стал оказывать фундаментальное воздействие на все производственные процессы и социальную среду, создавая массу возможностей... и противоречий.

## ГОРИЗОНТЫ ПРОРЫВНЫХ РЕШЕНИЙ

В материальном производстве стало типовым использование цифровых моделей изделий и производственных процессов. При этом минимизируется дистанция между дизайном, проектированием, моделированием и собственно производством. Активное применение 3D-печати изделий всё больших размеров и сложности в классических отраслях практически стирает грань между проектированием и производством.

Обычной становится ситуация, когда изделие, состоящее из сотен тысяч компонентов, или производственный процесс, состоящий из множества фаз преобразований, существуют в виде единой цифровой модели уровня предприятия. В новой реальности процессы управления параметрами производства или планирования выпуска по существу представляют собой изменение параметров данной модели.

В управленческой деятельности (не важно, что это: управление пред-

приятием, управление отраслью, госуправление) прочное место заняли «большие данные». Это позволяет проводить эффективный ретроспективный анализ и анализ «что если», вовлекать в рассмотрение множество сопутствующих факторов. Массив данных становится средой, в которой напрямую принимаются управленческие решения.

В областях, связанных с работой с человеком и социальными группами, формирование цифрового профиля стало обычной практикой. Многофакторный анализ множества структурированных и неструктурированных данных позволяет формировать «цифрового двойника». Использование технологий искусственного интеллекта открывает возможность выстраивать поведенческие модели, моделировать или эмитировать поведение отдельного человека и социальных групп. В сочетании с высококачественными технологиями обработки звука и видеоряда это позволяет массово порождать deep-fake артефакты.

Таким образом, по мере ИТ-трансформации происходит существенная концентрация и связывание разнородной информации, что, в свою очередь, приводит к концентрации информационного риска. Современные заказчики вполне осознают риск компрометации или утраты своих данных, особенно если эти данные относятся к категории ключевых активов, включая цифровые модели

производства. Нелегитимная (случайная) корректировка или утрата цифровых моделей изделий или процессов может приводить к значимым негативным последствиям. Этот риск достаточно хорошо формализуется и количественно оценивается, что позволяет адекватно оценивать стоимость защитных мер.

Риски произвольного манипулирования данными о личности, персональными данными, оцениваются не в полной мере. На практике оценка этих рисков часто ограничивается первичными последствиями и соответствующим ущербом. Оценка вторичных последствий и последствий более высоких порядков часто не просчитываются. Что не позволяет адекватно оценивать необходимую стоимость защиты таких данных. Классическим примером такого неадекватного подхода является история с продолжавшимися в течение долгого времени манипуляциями с данными Московской лаборатории РУСАДА, о которой много писала пресса. В российской, а теперь и международной практике законодатель идет по пути императивного нормативного регулирования вопросов защиты персональных данных. В случае BigData это может порождать как недостаточный, так и завышенный уровень защиты.

Оценка рисков, связанных с кражей цифрового профиля гражданина, формированием фейковых личностей, ис-



пользования технологий искусственного интеллекта для создания цифровых поведенческих моделей (ботов), связанных с отдельными людьми или сообществами, в должной мере массово не оцениваются в гражданском применении. В профессиональном ИТ-сообществе очень стоек стереотип о том, что нарастающий вал инцидентов ИБ следует рассматривать как чисто криминальное явление, а не как акты гибридной информационной войны.

В условиях происходящих изменений классические технологии защиты информации, построенные на принципах выделения физического и информационного периметра информационных систем, становятся всё менее эффективными. Открытость для взаимодействия современных информационных систем является их неотъемлемым свойством, что явно противоречит классической логике выстраивания защиты информации.

### «ПОСТКЛАССИЧЕСКИЕ» ТЕХНОЛОГИИ ЗАЩИТЫ

Фокус развития систем защиты должен ускоренно смещаться с классических технологий защиты на уровне сети и базовой ИТ-инфраструктуры к технологиям защиты на уровне данных. Ценность различных информационных активов существенно отличается, в связи с чем тратить много средств на анализ и защиту огромных информационных потоков и огромных массивов данных не всегда целесообразно.

Эффективность будут демонстрировать интегрированные в платформы технологии и решения безопасности, которые объединяют в себе возможности:

- ◆ таргетирования (маркирования) данных, относящихся к различным информационным активам (имеющим различную ценность);
- ◆ эффективного управления доступом к этим данным в многомерных массивах BigData;
- ◆ мониторинга событий безопасности, связанных с этими данными;
- ◆ мониторинга легитимных транзакций, совершаемых с этими данными.

К сожалению, на текущий момент таких готовых решений не существует. Имеющиеся технологии защиты, рабо-



тающие на уровне прикладных данных, сейчас ориентированы на определение разницы между типовыми потоками операций и локальными девиациями, которые рассматриваются как аномалии, подлежащие детальной проверке или блокированию.

Анализ складывающейся ситуации позволяет сделать вывод, что успешное решение вопросов ИБ в рамках ИТ-трансформации будет являться пропуском на очередной уровень развития: насколько безопасной будет работа с массивами данных, настолько эти технологии могут быть массово применимы. Есть риск технологического отката назад. Текущие осторожные попытки факторизации интернета рядом государств пока воспринимаются как ущемление свободы, а инициативы по выработке глобальных правил безопасности информации блокируются.

Данная ситуация очень напоминает жаркие дебаты вокруг вопроса клонирования человека, когда в течение уже ряда лет нет фундаментальных техни-

ческих ограничений для выполнения данного эксперимента. Однако, невозможность и неготовность просчитать последствия такого шага блокируют научный поиск на уровне общественного и религиозного мнения. Возможно, что и в генетических исследованиях также будут выявлены естественные или разработаны искусственные средства защиты, которые не позволят процессу генетических исследований выйти из-под контроля.

\*\*\*

ИТ-технологии тоже подошли к рубежу, когда их дальнейшее развитие может быть признано общественным сознанием опасным и будет приняты жёсткие законодательные ограничения развития. Если такая ситуация сложится, адекватные технологии информационной безопасности станут тем ключом, который будет открывать дверь дальнейшему развитию ИТ.





**Валерий КУЛИКОВ**  
корреспондент BIS Journal

# АНТИСАНКЦИИ ИЛИ ИНДУСТРИАЛИЗАЦИЯ 2.0?

ОБЗОР МЕРОПРИЯТИЙ, ПОСВЯЩЁННЫХ  
ИМПОРТОЗАМЕЩЕНИЮ В СФЕРЕ ИКТ

**В** конце 2019 года в Москве прошли две конференции, затрагивающие проблемы импортозамещения в сфере ИКТ. Обзор нашего корреспондента, побывавшего на обеих, вполне вписывается в рамки дискуссии, развернувшейся на страницах BIS Journal<sup>1</sup>.

## «УСПЕХИ» И «ПРОВАЛЫ»

На старте ноябрьской конференции ТАСС «Антисанкции. В чём выгода импортозамещения в сфере ИТ» аналитики информагентства представили гостям свой список «успехов и провалов» в области ИТ-импортозамещения. По окончании первой части мероприятия были показаны и результаты дистанционного голосования (по системе да/нет) по этому списку (рис. 1, 2).

Список неудач практически никто не оспаривал. По поводу «успехов» аудитория дважды почти согласилась (70% голосов) с мнением аналитиков.

Уместно отметить, что в дискуссии об «импортозамещении в сфере ИТ» центральной стала тема ПО и оргмероприятий, связанных с внедрением тех или иных софтверных решений (подготовка кадров, взаимодействие вендоров и заказчиков в части доработок ПО, меры

стимулирования и т.п.). И это понятно. Но вот единодушные положительные оценок по поводу того, что процесс импортозамещения привёл к росту радиоэлектронной промышленности России, вызвало удивление.

Так есть ли у России своё «железо» и наблюдается ли в стране рост радиоэлектронной промышленности?

## «ЖИРАФ БОЛЬШОЙ, ЕМУ ВИДНЕЙ!»

На этот вопрос ответ держала декабрьская конференция «Электроника в России: будущее отрасли». Ситуацию освещал целый пул чиновников, включая зампреда Правительства РФ Юрия Борисова и заместителей министров Минпромторга и Минэнерго, а также директора департамента радиоэлектронной промышленности Минпромторга.

Комментарии чиновников напоминали выступления жонглёров, только вместо шариков и булав в речах мелькала эклектичная смесь из контроллеров и конденсаторов, микроэлектроники и информационных двойников, импортных комплектующих и продукции гражданского назначения вкупе с каскадом заявлений о намерениях и миллиардах рублей инвестиций и триллионном объёме рынка в ближайшей перспективе.

При этом в выступлении замов присутствовала дисгармония.

Самый старший по должности сначала оптимистично заметил, что в настоящее время отрасль электронной промышленности находится в стадии активного развития, чему способствует растущий спрос на внутреннем рынке. Но чуть позже признал: «Сегодня глупо говорить, что в России существует серийное микроэлектронное производство. Мы даже отсутствуем в мировой статистике».

Дальше — больше. Зампред Правительства РФ утверждает: «Пока что у нас нет необходимой инфраструктуры, необходимого количества дизайн-центров, которые могли бы работать по всему спектру востребованной номенклатуры... Наша задача — защита внутреннего рынка, создание условий для появления этой номенклатуры, причём, на внебюджетные средства». А замминистра из Минпромторга уже рапортует: «Российский бизнес нашёл инвестиции, привлёк необходимых специалистов, запустил новые технологии и оборудование и смог снова выйти на рынок».

Зампред Правительства РФ заявляет: «В отрасли не хватает 25–30 тысяч специалистов, нам нужно сделать эту сферу и образование более привлекательными, чтобы молодые люди сами шли. Я взял за правило встречаться со студентами, они приносят мне удовольствие. Студенты очень мало знают, что такое оборонно-промышленный

<sup>1</sup> Дискуссия посвящена ИТ-импортозамещению в России (см. BIS Journal №№ 2–4/2019). В ней приняли участие Карл Сумманен, Александр Баранов, Алексей Смирнов, Наталья Касперская и др.



## Достижения импортозамещения

1. Повышение конкурентоспособности российских IT-продуктов.
2. Активная технологическая кооперация российских вендоров для закрытия потребностей заказчиков по функционалу.
3. Начало разработок ГИС без иностранных компонентов.
4. Первые реализованные проекты федеральных служб и ведомств по переходу на отечественное ПО.
5. Рост отечественной радиоэлектронной промышленности и разработки в сфере базовых ИТ технологий.
6. Появление рынка труда и обучающей инфраструктуры по отечественным программным продуктам.

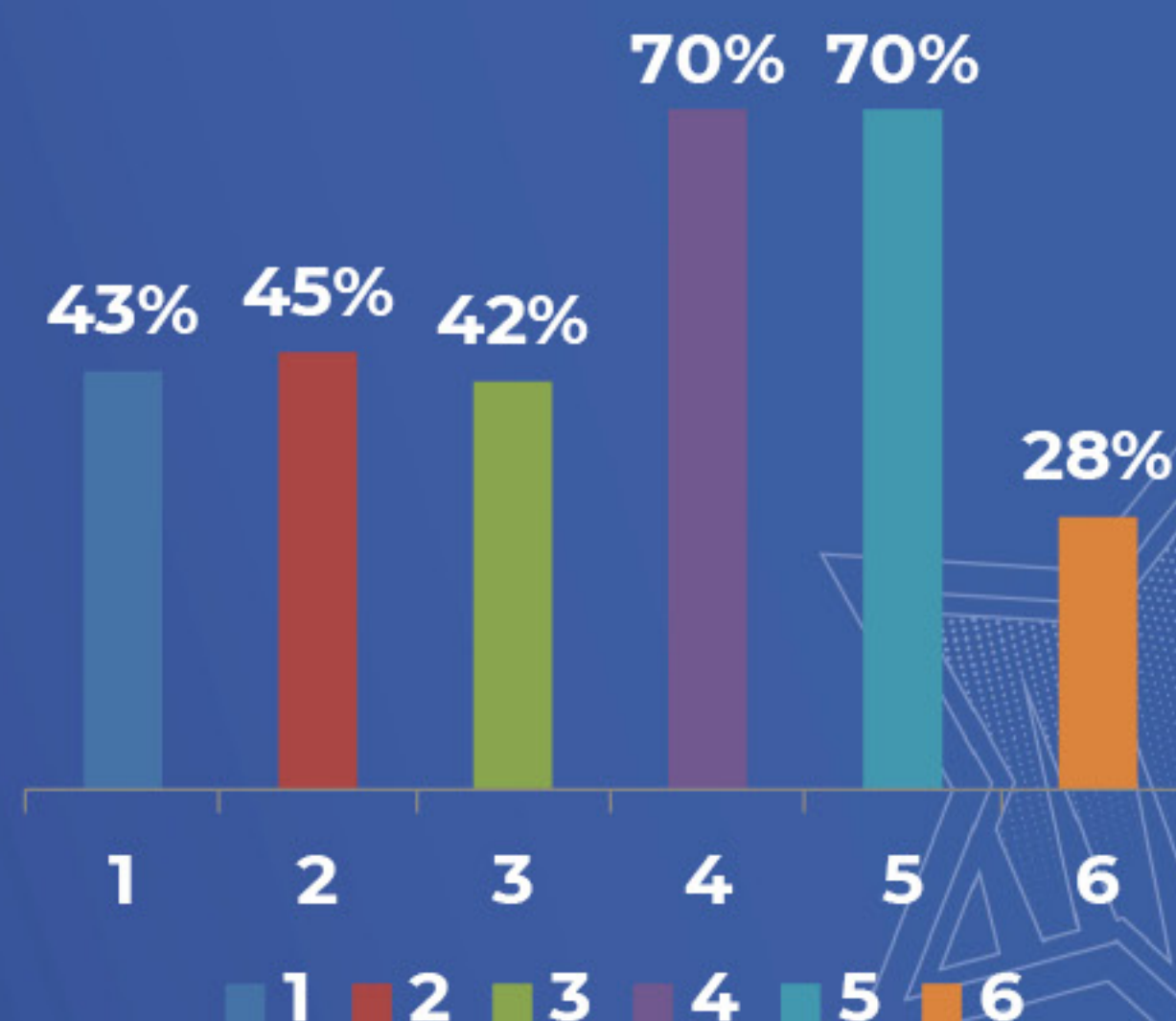


Рисунок 1. Список «Достижения IT-импортозамещения» и результаты дистанционного голосования по системе да/нет

## Провалы импортозамещения

1. Отсутствие четкого определения «отечественное ПО».
2. Неэффективное расходование бюджетных средств.
3. Фактический срыв срока перехода на отечественное офисное ПО.
4. Отсутствие опыта разработки архитектурных решений на базе отечественного ПО.
5. Отсутствие типовых/коробочных масштабируемых отраслевых решений (полностью отечественный технологический стек аппаратного оборудования, системного и прикладного ПО).
6. Недостаточность квалифицированных специалистов в области отечественного ПО.
7. Путаница и несогласованность документов в нормативной базе программы импортозамещения.

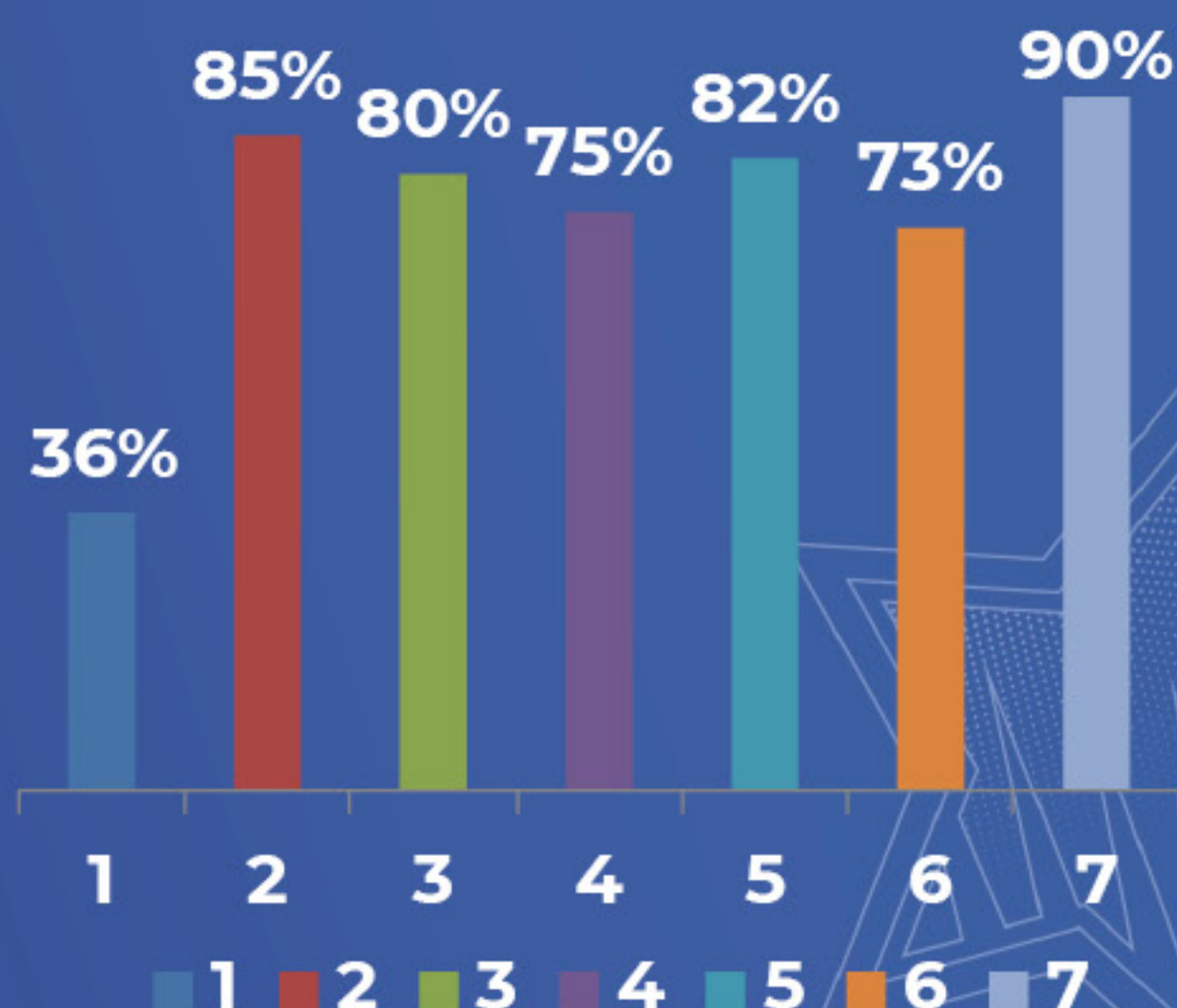


Рисунок 2. Список «Провалы IT-импортозамещения» и результаты дистанционного голосования по системе да/нет



## Уместно ли измерять отрасль в «пластинах в месяц», если «пластины» могут быть весьма разными и по размерам, и по материалам, и по сложности технологий обработки, и по цене?

комплекс, что такое оборонная радиоэлектроника. Нам надо чаще читать лекции об этом, а то кадры будут уходить на Запад». А в ответ находящийся ближе всего к «земле» директор департамента радиоэлектронной промышленности Минпромторга бьёт, что называется, «по площадям», сообщая, что на внутреннем рынке микроэлектроники 82% приходится на импорт, на военную продукцию — 15% и лишь 3% — на гражданскую продукцию, а место России в распределении производственных мощностей (тысяч пластин/месяц) находится «ниже статистической погрешности» — всего 0,04%.

В общем, после выступлений чиновников на ситуацию с импортозамещением вместо прозрачной ясности опускается туман. Где для капитанов электронной промышленности проходит водораздел между «микроэлектроникой» и «гражданской продукцией»? Уместно ли измерять отрасль в «пластинах в месяц», если «пластины» могут быть весьма разными и по размерам, и по материалам, и по сложности технологий обработки, и по цене? Непонятно.

А как надо читать лекции: чаще или систематически? А может, доверять обучение студентов достойно оплачиваемым доцентам и преподавателям?

Короче, из всего сказанного участникам конференции стало понятно одно — зампред правительства в первую очередь должен безальтернативно добыть 10 миллиардов, а не разочаровывать аудиторию туманной фразой: «Надеюсь, смогу убедить правительство выделить эти деньги».

### «ВЕРШИНА, КОТОРУЮ НЕ ПОКОРИЛ»

Но всего этого ещё не знали гости ноябрьской конференции ТАСС, что и позволило им почти дружно одобрить в списке «успехов» пункт: «Рост

отечественной радиоэлектронной промышленности и разработки в сфере базовых IT-технологий».

По поводу формулировки «...и разработки в сфере базовых IT-технологий» тоже было интересно. К базовым принято относить, в частности, и операционные системы, а в этом, по замечанию члена Совета по развитию цифровой экономики при Совфеде РФ Андрея Безрукова, Россия — мировой лидер. В том смысле, что разработками разных ОС в стране занято несколько десятков компаний. И хотя в этих словах формально нельзя было услышать негатива, но «ориентируясь на тон командора»...

А вот в «разработках» и, что зачастую важнее, производстве того, что на птичьём языке профессионалов именуется ЭКБ, в России особых успехов точно нет. Так, по крайней мере, считают участники конференции, знающие отрасль микроэлектроники не понаслышке.

Наиболее наглядно ситуацию с отечественным «железом» описал представитель МЦСТ «Эльбрус», признавший, что «значительный рост» есть, если считать таковым превышение единицы отношения двух бесконечно малых величин. Практически то же самое, но более округлыми фразами сказала и Ольга Пестерева, представлявшая ПАО «Микрон».

### «Я НЕ ЛЮБЛЮ, КОГДА НАПОЛОВИНУ»

На конференции ТАСС государственное управление процессом импортозамещения было представлено лишь одним лицом — директором Центра компетенций по импортозамещению в сфере ИКТ. Ранее Илья Массух на разных своих ответственных должностях неоднократно заявлял, что «мы» уже не успели «вскочить на поезд» в том, что касается «железа». Теперь у него другое мнение: «цифровую независимость»

страны в части «железа» он оценивает даже выше, чем в части ПО.

К сожалению, он быстро покинул конференцию, избежав тем самым необходимости прокомментировать выступления представителей «Эльбруса» и «Микрона». Тем не менее, в качестве улыбки чеширского кота, он оставил залу идеи и цифры перспективного «импортозамещения в сфере ИКТ». Вот суть:

♦ «частичная локализация» зарубежного ПО для «некоторых ниш российского рынка» с сохранением 50% прав на программный продукт на территории России;

♦ технологическая самостоятельность за счёт доли в 60% отечественного ПО в госкомпаниях.

Что такое 50% прав на программный продукт и как измерять доли отечественного ПО — это уже частности, стратегия же заявлена!

### ИМПОРТОЗАМЕЩЕНИЕ AS IS

Выступление г-на Массуха представило софтверную индустрию России не в самом лучшем свете. Наверное поэтому лицо президента партнёрства «Руссофт» Валентина Макарова в ходе этого выступления несколько вытянулось. Ведь именно г-н Макаров, опираясь на солидный аналитический потенциал возглавляемого им партнёрства, на протяжении десятилетия доказывал, что экспортный потенциал отечественных программистов сопоставим с доходами от продажи вооружений, подкрепляя это утверждение цифрами и числами.

А ведь такой потенциал, умело замкнутый на внутреннюю «нагрузку» потребностей российской экономики, не может не дать результата.

Однако предвкушение интеллигентной дискуссии президента «Руссофт» и директора Центра компетенций рассеялось как дым после быстрого ухода г-на Массуха, и Валентин Макаров и, аккуратно следом за ним, Армен Кочаров («Новые облачные технологии») провели спарринг с директором Центра компетенций заочно.

Президент «Руссофт» аргументированно покусился на авторитет Реестра отечественного ПО как одного из локомотивов «импортозамещения в сфере





Конференция «Антисанкции. В чём выгода импортозамещения в сфере ИТ». Фото: conference.tass.ru



Конференция «Электроника в России: будущее отрасли» Фото: events.vedomosti.ru

ИКТ». Оказывается, респонденты партнёрства оценили эффективность этого инструмента импортозамещения в величину 0,09 (в диапазоне оценок от -3 до +3), тогда как двумя годами ранее этот показатель достигал аж 0,25. Сегодня 55% респондентов «Руссофт» считают, что Реестр отечественного ПО не оказывает в нашей стране никакого влияния на процесс импортозамещения в сфере ИКТ.

Президент «Руссофт» поведал также об успехах своих коллег в создании платформенного ПО для использования в банковском секторе и ПО для информационного моделирования в сфере эксплуатации месторождений нефти и газа. Проекты «Консорциум Бета» и «Консорциум Союз» продемонстрировали свои возможности в части функционала и техподдержки, и выполнены они были за счёт собственного финансирования участников проектов, но ответных стимулирующих мер со стороны внутреннего рынка так и не последовало.

Значительную часть выступления г-н Макаров посвятил тому, как государство может именно рыночными методами стимулировать не только ускорение импортозамещения, но и довести его валовые показатели до осязаемых величин.

Жаль только, что эти предложения в тот день не были услышаны официальным представителем государства.

### ЧЕГО В ЭТОМ СУПЕ НЕ ХВАТАЕТ?

На конференции «Антисанкции. В чём выгода импортозамещения в сфере ИТ»

был представлен ряд успешных опытов по переводу на отечественные платформы ИТ-обеспечения организаций госуправления и органов управления регионами. Масштаб впечатляет: ФНС России, Министерство образования, науки и молодёжи Республики Крым, Челябинская область, Фонд социального страхования РФ, Правительство Свердловской области РФ и др. IT-решения для таких опытов объективно — на основе представленных результатов нагрузочных испытаний — конкурентоспособны на мировом рынке.

Компании «Новые облачные технологии» и ТИОНИКС продемонстрировали готовность предложить отечественные разработки для инновационного развёртывания вычислительных «облаков» (а это мощно и отказоустойчиво), в том числе и на основе «железа» отечественных процессоров от МЦСТ «Эльбрус» и «Байкал Электроникс».

А выступление Армена Кочарова из «Новых облачных технологий» включало в себя вполне обоснованный панегирик советскому опыту обретения технологической и производственной независимости и предложение нынешним руководителям импортозамещения перенять опыт долгосрочного планирования развития промышленности.

Чего же не хватает сегодня для того, чтобы повторить рывок 30–60-х годов прошлого века? Похоже, именно того, что и отсутствовало на конференции — продуктивного диалога между государством и отраслью ИКТ,

управление которой растащено по частным компаниям и госкорпорациям.

Одна из причин отсутствия такого диалога — разница уровней видения и понимания ситуации. То, что должно было стать индустриализацией 2.0, то есть локомотивом экономики огромной страны, съёжилось до локального процесса, называемого на языке государства «импортозамещение в сфере ИКТ».

К великому сожалению, на официальном уровне то, что называется «импортозамещением», часто связывают с понятием «антисанкции». Хотя по своей грандиозной сути «импортозамещение» является не тактическим выпадом на нервическую порывистость партнёров, датированную 2014 годом, а стратегическим инструментом восстановления экономического могущества России. Её выхода из состояния, которое ряд экспертов называет колониальной зависимостью.

\*\*\*

Вполне логично, что одним из результатов «импортозамещения» должна стать информационная безопасность. Которая тем более важна, что в эпоху «цифровой трансформации» покуситься на государственный экономический суверенитет может не только враждебное государство, но и просто транснациональная корпорация. Особенно когда кукловодами политического руководства и совета директоров являются одни и те же лица.





**Антон ЧУХНОВ**  
генеральный директор  
АВ Софт

# ПРОАКТИВНАЯ КИБЕРБЕЗОПАСНОСТЬ

ИМПОРТОЗАМЕЩЕНИЕ НЕ ТРЕБУЕТСЯ

**В**ысокие темпы обновления инструментария для кибератак — одна из особенностей нынешней ситуации в сфере ИБ. В связи с этим ставшие традиционными средства реактивной защиты — антивирусы, системы IDS/IPS, межсетевые экраны, реагирующие на уже известные угрозы, необходимо дополнять системами проактивной киберзащиты.

Наиболее перспективной для проактивной киберзащиты ИТ-инфраструктур, в том числе и включающих оборудование IoT/IIoT, является технология Desception, или технология обмана на основе т.н. «ловушек» (Honeypots). Они имитируют оборудование инфраструктуры, дезинформируя злоумышленников, и позволяют обнаруживать, замедлять и предотвращать атаки, не допуская нанесения значимого ущерба.

В основе проактивной обороны в киберпространстве лежит евангельский завет «По плодам их узнаете их». Исследование поведения подозрительного объекта в специальной изолированной среде «песочнице» (Sandbox), позволяет идентифицировать вредоносное ПО и предотвратить его проникновение в ИТ-инфраструктуру организации.

Системы киберзащиты, использующие «песочницы» и «ловушки», не слишком широко представлены на мировом рынке в виде «коробочных» продуктов, и ещё меньше таких систем предлагается отечественными вендорами. Возможно, не будет преувеличением ска-

зать, что для их перечисления хватит пальцев на одной руке, да и то не всех.

Система выявления и анализа вредоносного программного обеспечения ATHENA (АФИНА) на основе технологии «песочниц» и «ловушек» — это разработка отечественной компании АВ Софт. Компания начала работы над средствами киберзащиты ИТ-инфраструктуры на основе технологий динамического анализа в 2010 году, выполняя кастомизированные разработки для внешних заказчиков. К 2016 году накопленный опыт позволил предложить рынку «коробочное» решение, которое вошло в Реестр отечественного программного обеспечения РФ.

Более подробно рассказать об этом BIS Journal попросил генерального директора АВ Софт Антона Чухнова.

— Антон Павлович, возможно ли, что в некоторой перспективе в сфере ИБ технологии динамического анализа вытеснят технологии статического анализа для распознавания вредоносного ПО?

— Лучше не ставить вопрос выбора между статическим и динамическим методами анализа, а использовать их синергию. Комбинация этих подходов не только позволяет экономить ресурсы за счёт блокировки уже известных вирусов на этапе статического анализа, а на этапе динамической проверки выявлять неизвестные, но и повышает точность вердикта, что самое важное!

— То есть при построении системы киберзащиты на основе «коробочного» решения, использующего технологии динамического анализа, придётся приобретать ещё антивирус, например, и проводить самостоятельно или с помощью сторонней организации интеграционный проект?

— Если говорить о решении ATHENA, то оно уже сочетает в себе два вида анализа. «Классические» статические технологии ИБ — антиспам, IDS/IPS, антивирусы, парсинг файлов — это элементы первой линии обороны на её основе.

В рамках статического анализа осуществляется проверка 20 антивирусами (платными и бесплатными), детальный статический анализ структуры файлов (парсинг), проверка средствами ML. При желании пользователя система позволяет проверять подозрительные файлы внешними «облачными» аналитическими сервисами ИБ.

К решению об отнесении подозрительного объекта к группе риска подключается и аналитический блок, использующий технологию машинного обучения (нейросети).

И лишь после детального статического анализа объект передаётся в модуль для проведения многофакторного поведенческого анализа, в «песочницу».

— «Песочница» — это некая виртуальная среда?

— В том числе. Исследование поведения может проводиться как на виртуальной машине, так и на физическом



оборудовании. Оба варианта реализации поддерживают в операционной системе «песочницы» имитацию работы пользователя, реальные информационные ресурсы и состав ПО организации.

В части систем на базе технологии «песочницы» мы пошли дальше и решили реализовать не просто имитацию отдельной ОС персонального компьютера пользователя, а воссоздать инфраструктуру целой организации, которая включает в себя и базы данных, и сервера, и IoT в виде «ловушек».

— **А для чего нужны «ловушки»?**

— «Ловушки» — это имитация оборудования в ИТ-инфраструктуре, в структуре АСУ/АСУ ТП.

Самой организацией это «оборудование», естественно, не используется, но со стороны киберпространства оно «выглядит» как настоящее и может стать объектом реальной кибератаки. И не только извне. «Ловушки» могут стать объектом атаки, исходящей внутри защищаемого периметра организации. Развёртывание «ловушек» может проявить, например, активность вредоносного ПО, уже внедрённого в ИТ-пространство организации, перехватить атаку на любом этапе её развития.

— **Вы контролируете Интернет-трафик, электронную почту, ...?**

— Вы угадали, выдержав паузу. Источников информации для «размышлений» АФИНЫ множество. Помимо названных Вами, это ещё мессенджеры, мобильные устройства, рабочие места пользователей и IoT-устройства. Подозрительные файлы можно загрузить в систему вручную. Ну и, в конце концов, API системы и ICAR-сервис позволяют «кастомизировать» набор источников поступления объектов проверки.

— **При контроле почтового трафика письма, содержащие вредоносное ПО, идут в корзину?**

— Система ATHENA поддерживает технологию удаления подозрительного ПО из писем и их мгновенную конвертацию в безопасный формат, чтобы не замедлять бизнес-процессы организации и как можно скорее предоставить пользователю возможность ознакомиться с поступившей информацией. Все файлы, прошедшие проверку, находятся в карантине и могут быть проверены повторно в рамках ретроспективного анализа.

— **Даже просто из Вашего рассказа ясно, что ATHENA — это мощный инструмент, мощный не только по своим возможностям, но и ресурсоёмкий. Он может существенно затормозить работу организации?**

— Если речь идёт о бизнес-процессах, то ATHENA может быть интегрирована в ИТ-инфраструктуру как в режиме «в разрыв», так и в режиме «зеркало», она может работать с реальным информационным трафиком или с его копией, в автоматическом режиме или в режиме исследовательской и/или экспертной системы в качестве криминалистической лаборатории.

Использование той или иной комбинации этих режимов — это вопрос реализации принятой в организации политики ИБ, оценки рисков и того набора задач, что вы хотите решать.

Например, с помощью системы ATHENA решаются сугубо утилитарные задачи: можно в автоматическом режиме проверять, блокировать, обезвреживать файлы и уведомлять заинтересованные службы об угрозах и проблемах по разным каналам коммуникаций (e-mail, мессенджер, SIEM). А возникнет потребность, и с помощью системы ATHENA можно сформировать и наращивать базу знаний по киберугрозам, решать задачи в сфере повышения квалификации и расширения компетенции персонала службы ИБ.

— **Каковы минимальные требования к компетенции департамента ИБ в организации, решивший внедрить систему ATHENA?**

— Наш программный комплекс может быть «поставлен» в виде «облачной» услуги по обеспечению защиты электронной почты, Интернет-трафика и иных источников информации. Как Вы понимаете, в этом случае требования минимальны.

Иные варианты — это поставка системы в виде законченного программно-аппаратного комплекса или развёртывание ПО на инфраструктуре заказчика.

Компания АВ Софт обучает персонал заказчика. Мы также активно развиваем партнёрскую сеть, обучаем специалистов партнёров. Можно работать, включая и получение услуг по поддержке, через наших партнёров.

— **Обеспечивает ли использование системы ATHENA «чистоту» в контексте современных тенденций, в частности вопроса импортозамещения?**

— Хорошо, что напомнили о современных тенденциях! Замечу, что в ходе динамического анализа система ATHENA позволяет выявлять ПО, расходующее ресурсы для майнинга.

Что же касается импортозамещения, то разработка полностью отечественная. Сторонний код — лишь тот, что используется в рамках Open Source. Он используется, например, при создании модуля сети «ловушек» для имитации оборудования IoT/IIoT.

Среди поддерживаемых антивирусов — отечественные и те, что предоставляются бесплатно.

В портфолио компании есть интеграции системы ATHENA с отечественными межсетевыми экранами и другими системами первой линии защиты.

— **Какие операционные системы поддерживает система ATHENA в «песочнице»?**

— В динамическом анализе поддерживаются MS Windows, Windows Server, разнообразные варианты Linux: Astra Linux, Debian, openSUSE, CentOS, Ubuntu и другие, macOS, вся линейка версии Android.

— **Резюмируя Ваши ответы, для системы ATHENA видится широкий круг задач, которые могут решить пользователи.**

— Совершенно верно. От автоматического выявления вредоносного ПО и его обезвреживания без участия пользователей системы и до исследований поведения программного обеспечения в различных ИТ-средах. В последнем случае пользователь имеет широкие возможности для настроек эмулируемых сред по интересующим его направлениям исследований. А API-интерфейс системы ATHENA позволяет масштабировать возможности для решения практических задач построения линий киберзащиты, исследований в сфере ИБ, быть основой для построения комплексных систем безопасности, подготовки кадров или повышения квалификации персонала.

— **Спасибо.**

*Беседовал Валерий Куликов*



**Александр ШМЕЛЕВ**

заместитель  
начальника  
Управления  
информационной  
безопасности  
ПАО «Московский  
Индустриальный  
банк»

**Олег ТАРАСОВ**

начальник отдела  
защиты пластиковых  
карт Управления  
информационной  
безопасности  
ПАО «Московский  
Индустриальный  
банк»

# САМАЯ БОЛЬШАЯ ПРОБЛЕМА

## СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ ПРЕВРАЩАЕТСЯ В ПОРОХ И ДИНАМИТ

**С**оциальная инженерия — одна из тех технологий, которые со временем перешли на «тёмную сторону». Порох, изобретённый китайскими учёными с целью создания эликсира бессмертия, стал использоваться для метания ядер и пуль. Динамит изначально помогал горнякам в разработке месторождений и прокладывании транспортных туннелей, однако сегодня чаще применяется в военных действиях. То же произошло и с социальной инженерией — долгое время она находилась в арсенале спецслужб, но в настоящее время этот термин ассоциируется в первую очередь со «взломом человека» хакерами.

### ОСНОВНАЯ ОЗАБОЧЕННОСТЬ БАНКОВ

Понятие «социальная инженерия» используется для обозначения широкого спектра злонамеренных действий, совершённых посредством взаимодействия преступника и жертвы. В основе этого метода — психологические манипуляции, заставляющие пользователей пренебрегать правилами безопасности и разглашать конфиденциальную информацию. По различным оценкам, от 30 до 70% всех действий мошенников связаны с социальной инженерией.

Социальная инженерия особенно опасна потому, что основана на человеческих ошибках, а не на уязвимостях в ПО и ОС. Это подтверждают и слова первого заместителя директора департамента информационной безопасности Банка России Артема Сычева: «Наша основная озабоченность сегодня — не технические атаки и вредоносное ПО. Нам понятно, как с этим бо-

роться. Есть технические методы и методы через изменение законодательства. Самая большая проблема — социальная инженерия».

### ТИПЫ АТАК

Технология охватывает широкий спектр вредоносных действий, основными из которых являются следующие типы атак<sup>1</sup>.

**Приманка (Baiting).** Преступники используют ложное обещание, чтобы разжечь жадность или любопытство жертвы. Они заманивают пользователей в ловушку и крадут их личную информацию или наносят вред их системам. Например, злоумышленники оставляют приманку (заражённую вредоносными программами флешку) в заметных местах, где их обязательно увидят потенциальные жертвы (например, лифты, автостоянки компании, комнаты ожидания). Люди берут флешку из любопытства, вставляют её в рабочий или домашний компьютер, что приводит к автоматической установке вредоносных программ в системе. Онлайн-формы приманки часто имеют форму рекламы, которая ведёт на вредоносные сайты или побуждает пользователей загружать заражённое вредоносным ПО приложение.

**Scareware.** Этот тип атак включает в себя «бомбардировки» жертв ложными тревогами и фиктивными угрозами. Пользователей вводят в заблуждение, сообщая, что их система заражена вредоносным ПО. Это побуждает клиентов устанавливать программное обеспечение, которое не приносит реальной пользы (кроме как для злоумышленника) или представляет собой само вредоносное ПО. Распространённым примером такой программы являются легально выглядящие всплывающие баннеры, которые появляются в браузере во время просмотра веб-страниц с текстом о за-

<sup>1</sup> На сегодняшний день ни одна типология, связанная с социальной инженерией, не является исчерпывающей и окончательной. В предыдущих номерах BIS Journal опубликовал несколько классификаций, не повторяющих друг друга. В этом номере продолжает расширять «коллекцию» (Редакция).

Социальная инженерия особенно опасна потому, что основана на человеческих ошибках, а не на уязвимостях в программном обеспечении и операционных системах



ражении компьютера. Пользователю предлагается установить инструменты ПО, которое заражено вредоносной программой, или направляет на вредоносный сайт. Scareware также распространяется через спам, который выдаёт ложные предупреждения или предлагает пользователям купить бесполезные или вредные услуги.

**Услуга за услугу (Quid pro quo).** Злоумышленник часто притворяется сотрудником службы поддержки организации, в которой работает жертва или продукты которой использует. Стандартный сценарий предполагает, что преступник звонит в компанию по корпоративному номеру и сообщает о технических проблемах в работе системы. В процессе устранения неполадок злоумышленник вынуждает сотрудника совершать действия, позволяющие хакеру запускать команды или устанавливать нужно ему программное обеспечение на компьютере жертвы.

**Предлог (Pretexting).** Этот метод похож на quid pro quo. Единственное исключение состоит в том, что преступник обычно устанавливает доверия со своей жертвой, выдавая себя за известного жертве человека — коллега, авторитетная фигура в организации, сотрудник полиции, банка, налоговых органов или других лиц, которые могут знать конфиденциальную информацию. Преступник задаёт вопросы, которые якобы необходимы для подтверждения личности жертвы, посредством чего собирает важные личные данные.

**Фишинг (Phishing).** Один из самых популярных типов атак социальной инженерии. Главное отличие — использование скомпрометированной учётной записи электронной почты. 91 % всех успешных атак начинаются как фишинговые письма<sup>2</sup>.

Согласно отчёту Proofpoint<sup>3</sup>, в 2018 году 83 % специалистов по ИБ подвергались фишинговым атакам, что на 76 % больше, чем в 2017 году. Центр жалоб на интернет-преступления ФБР сообщает, что компрометация деловой электронной почты (Business Email Compromise, BEC) привела к убыткам в размере более 1,2 миллиарда долларов только в 2018 году<sup>4</sup>.

На почту отправляется текстовое сообщение, вызывающее у жертв чувство срочности, любопытства или страха. Данное письмо подталкивает их к раскрытию конфиденциальной инфор-

*Центр жалоб на интернет-преступления ФБР сообщает, что компрометация деловой электронной почты привела к убыткам в размере более \$1,2 млрд только в 2018 году*

мации, переходу по ссылкам на вредоносные веб-сайты или открытию вложений, содержащих вредоносные программы.

Примером может служить электронное письмо с предупреждением о нарушении политики безопасности и требованием немедленных действий со стороны сотрудника, например, изменение пароля. Письмо содержит ссылку на незаконный веб-сайт — по внешнему виду почти идентичный «правильной» версии сайта. Ничего не подозревающий пользователь вводит свои текущие учётные данные и новый пароль. После заполнения формы информация отправляется злоумышленнику.

**Целевой фишинг (Spear phishing).** Это более целенаправленная версия фишинг-атаки, при которой злоумышленник выбирает конкретных людей или предприятия. Если целью является высокопоставленный руководитель, эту атаку часто называют «китобойным промыслом».

Хакеры обычно разбиваются на отдельных пользователей, например, администраторов. Затем они настраивают свои сообщения на основе характеристик, рабочих мест и контактов, принадлежащих их жертвам, чтобы сделать атаку менее заметной.

Используя высоко персонализированные электронные письма или сообщения в социальных сетях, хакеры получают их идентификаторы и пароли, которые обычно имеют высокий уровень доступа к конфиденциальной информации. Поддельный фишинг требует гораздо больших усилий со стороны злоумышленника и может занять несколько недель или месяцев. Их гораздо сложнее обнаружить, поэтому они имеют более высокие показатели успеха.

Так, например, жертвой такой атаки стали администрация округа Кабаррус (Северная Каролина, США), которой пришло оповещение о том, что реквизиты строительного подрядчика якобы изменились. Как итог — платёж на сумму 2,5 млн долл. администрация перевела киберпреступникам. Аналогичная атака была организована на компанию Toyota Boshoku Corporation, которая потеряла 37,5 млн долл. США. По данным Центра жалоб

<sup>2</sup> <https://smallbiztrends.com/2019/11/social-engineering-attacks.html>

<sup>3</sup> <https://www.secureworldexpo.com/industry-news/state-of-the-phish-2019-report>

<sup>4</sup> [https://pdf.ic3.gov/2018\\_IC3Report.pdf](https://pdf.ic3.gov/2018_IC3Report.pdf)



## Преступники используют сложные поведенческие сценарии, направленные установление доверительных отношений с жертвой

на киберпреступления<sup>5</sup> ФБР (Internet Crime Complaint Center, IC 3), в мире убытки от ВЕС-мошенничества за последние 3 года составили более 26 млрд долл.

**Вишинг (Vishing).** Этот метод аналогичен фишингу, за исключением того, что способ атаки осуществляется через поддельную копию IVR-системы (Interactive Voice Response) компании. Обычно речь идёт о мошенниках, звонящих клиентам по телефону под предлогом, что что-то плохое уже произошло. Преступники используют сложные поведенческие сценарии, направленные установление доверительных отношений с жертвой. В такой ситуации клиенты охотно раскрывают конфиденциальную информацию (PIN-коды, пароли). При вишинге мошенники часто апеллируют к человеческим страхам.

**Задняя дверь (Tailgating),** метод также известен как «контрейлерная передача». Злоумышленник получает несанкционированный физический доступ к защищённой области в организации, следуя за человеком, который получает доступ посредством надлежащей проверки. Здесь могут использоваться различные приёмы: от клонирования бейджей до бесплатных подарков со встроенными беспроводными приёмниками, которые могут прослушивать беспроводной трафик Bluetooth.

### ЧТО МОЖЕТ ПОМОЧЬ?

Вследствие применяемой персонализации и интеллекта несанкционированный доступ с помощью инструментов социальной инженерии трудно предотвратить привычными методами ИБ. Вот некоторые меры, которые могут помочь:

- ♦ основные средства защиты, такие как спам-ловушки, которые идентифицируют спамеров для упреждающей блокировки электронных писем от них, «песочницы» электронной почты для проверки достоверности каждой нажатой ссылки и мониторинга сети на наличие необычных всплесков трафика;

- ♦ многофакторная аутентификация (MFA) является одним из наиболее эффективных способов заблокировать такие атаки, поскольку она

не ограничивает аутентификацию приложения только паролем, а объединяет её с токеном и/или другими формами идентификации. Поскольку схемы социальной инженерии в первую очередь нацелены на учётные данные пользователя, MFA блокирует их. Многофакторная аутентификация не способна обеспечить 100-процентную защиту. Однако преступники чаще предпочитают не иметь дело с MFA и выбирают более доступные цели;

- ♦ обучение сотрудников также может оказаться мощным способом предотвращения атак. Необходимо регулярно проводить тренинги по кибербезопасности и симуляции фишинга, отправлять по электронной почте оповещения и информационные бюллетени, чтобы сотрудники знали о последних схемах социальной инженерии и типах вредоносных программ.

### ОДНАКО...

Однако опрос<sup>6</sup>, проведённый Spanning в США, показал, что 64 % опрошенных сотрудников не определили подозрительные ссылки. Почти 55 % признались, что нажимали на ссылки, которые они не распознавали, а 49 % загрузили веб-расширение на своё рабочее устройство. Если добавить к этому настойчивость хакеров и изобретательность социальных инженеров, лучшая защита организации — быть готовым к худшему.

Иногда внутренние бизнес-процессы организации оказывают «медвежью услугу» в борьбе с атаками. Например, эффективность работы сотрудников справочных служб часто оценивают по скорости решения проблем. Это приводит к тому, что специалисты вынуждены слишком быстро реагировать на запросы, не проверяя их на безопасность.

### ДО И ПОСЛЕ АТАКИ

Также каждая компания должна иметь план восстановления работоспособности после успешной атаки. Методы, которые могут оказаться полезными, — планирование непрерывности бизнеса и аварийного восстановления. Последний метод предусматривает наличие превентивных мер в организации (резервное копирование данных в облаке, детективные меры).

Планирование непрерывности бизнеса относится к более комплексному процессу, который включает аварийное восстановление, оценку всех рабочих процессов бизнеса, установку приемлемых Целей времени восстановления (RTO) и Точек восстановления (RPO) для различных функций.

<sup>5</sup> <https://www.bleepingcomputer.com/news/security/business-email-compromise-is-a-26-billion-scam-says-the-fbi/>

<sup>6</sup> <https://spanning.com/resources/reports/trends-us-worker-cyber-risk-aversion-threat-preparedness/>



# МНОГОЛИКИЙ ФИШИНГ

КОГДА ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ НЕ ПОМОГАЮТ

**Ф**инансовые учреждения — очевидная и самая популярная мишень для киберпреступности. В 2018 году на пять крупнейших целевых сервисов — финансовые, почтовые, облачные, платёжные и SaaS — приходилось 83,9% от общего объёма фишинга, причём в лидеры вышло хищение учётных данных от финансовых сервисов. По данным отчёта «2019 Phishing trends and intelligence report» доля таких атак увеличилась с 21,1% в 2017 году до 28,9% в 2018.

В этой статье мы рассмотрим виды угроз, к которым должны быть готовы финансовые учреждения, планируя меры безопасности для защиты своих активов, клиентских данных и репутации компании, а также проанализируем тенденции развития фишинговых атак на организации финансовой сферы РФ в 2016–2019 годах и выделим психологические уязвимости, которые эксплуатируют мошенники.

## ГЛАВНЫЕ УГРОЗЫ

Выделяют пять видов наиболее опасных угроз для компаний кредитно-финансовой сферы:

- ♦ кража личности;
- ♦ эксплуатация чужого аккаунта;
- ♦ поддельная личность;
- ♦ вымогатели;
- ♦ социальная инженерия.

### 1. Кража личности

Злоумышленники крадут личную информацию, данные банковских карт, биометрические характеристики, а затем совершают покупки от

имени жертвы или просто переводят её деньги на свои счета.

**Схема преступления:** Похищение → Профит.

**Средства реализации:** технический инструментарий в виде эксплуатации уязвимости сайта, фишинга, вируса; социальная инженерия.

**Жертвы:** клиенты компаний кредитно-финансовой сферы, реже — сотрудники банков.

**Потери:** как правило, жертва узнаёт о краже личных данных уже после столкновения с последствиями киберпреступления. Потери могут варьироваться от незначительных сумм до миллионов долларов.

**Способ борьбы:** подтверждение личности с помощью ЭЦП и/или биометрической идентификации с распознаванием живого человека (liveness detection), обнаружение аномалий, обучение персонала.

### 2. Эксплуатация чужого аккаунта

Атака, производная от предыдущей, с добавлением изюминки под названием «многоходовочка». При этом скомпрометированные данные используются не для непосредственной кражи денег, а для дальнейших незаконных действий.

**Схема преступления:** Похищение чужого аккаунта → Эксплуатация → Профит.

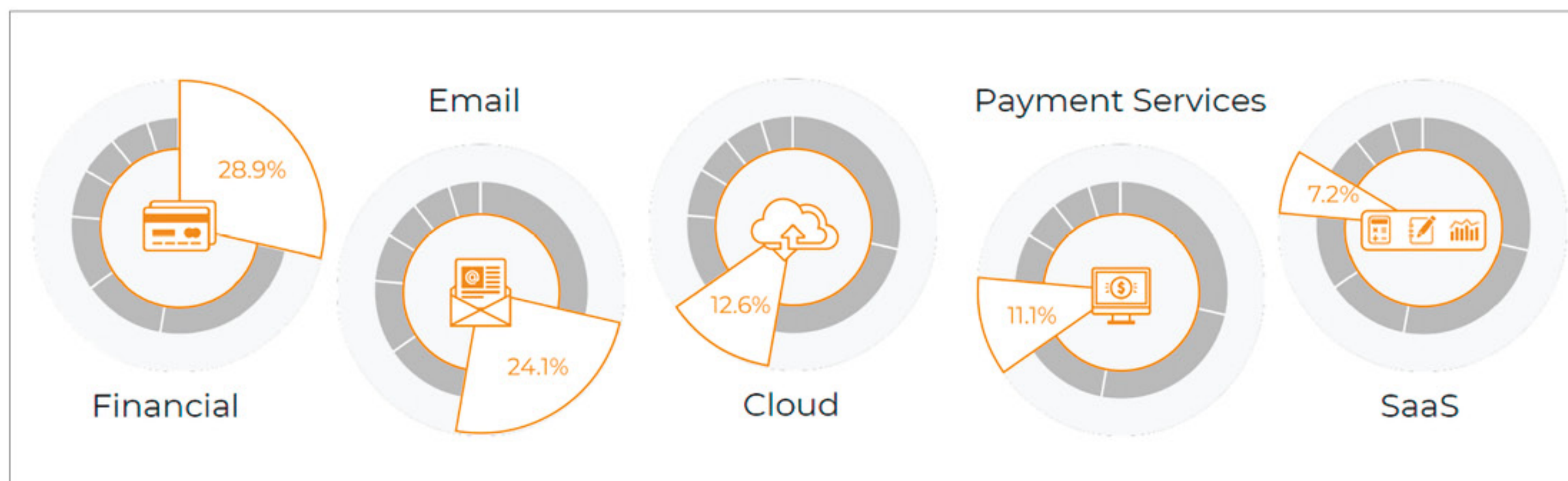
**Средства реализации:** как технический, так и психологический инструментарий, причём значимость психологического становится выше, поскольку используется эффект «доверенного источника». Например, атаки с компрометацией деловой переписки (Business Email Compromise, BEC) вообще не требуют применения технических средств.



**Ольга ЛИМОНОВА**  
психолог  
ООО «Антифишинг»



**Андрей ЖАРКЕВИЧ**  
редактор  
ООО «Антифишинг»



**Рисунок 1.** Объём фишинга на пять крупнейших целевых сервисов за 2018 г.



**Жертвы:** клиенты и сотрудники компаний кредитно-финансовой сферы.

**Потери:** защитные системы не реагируют на такие атаки, поскольку они выполняются с помощью обычных писем от легитимных отправителей и не содержат вредоносных ссылок или вложений. Жертвы доверяют своему адресату, а потому обнаруживают, что пострадали от атаки, лишь столкнувшись с потерями или узнав о компрометации учётной записи от его истинного обладателя.

**Способы борьбы:** идентификация отправителя с помощью ЭЦП или биометрических технологий, обнаружение аномалий, обучение персонала.

### 3. Фальшивые личности (синтетическое мошенничество)

Это киберпреступление реализуется посредством кражи и создания фиктивной личности из фрагментов реальной и сфабрикованной информации (например, паспортных данных, номера социального страхования, телефона и т.п.). Чаще встречается в западных странах.

**Схема преступления:** Кража персональных данных → Создание фальшивой личности → Обман финансового учреждения → Профит.

**Средства реализации:**

- ♦ технические — эксплуатация уязвимостей, связанных с идентификацией личности;

- ♦ психологические — подделка «живых» социальных страниц, фотовидеомонтаж и другие.

**Жертва:** банк или кредитор, настоящий владелец использованных данных. Это может быть взрослый или даже ребёнок, который в будущем обнаружит, что за ним числятся непогашенные долги, а кредитная история безнадежно испорчена.

**Потери:** такие атаки и их последствия можно обнаружить спустя годы, причём денежный ущерб будет лишь частью проблемы. Финансовым учреждениям придётся потратить время и ресурсы, чтобы отследить действия, совершённые с использованием поддельных личностей.

**Способ борьбы:** идентификация с помощью ЭЦП и/или биометрии с проверкой на живого человека, обнаружение аномалий, симулированные атаки, обучение персонала.

### 4. Вымогатели

Эта атака выполняется с помощью вредоносного программного обеспечения, которое блокирует доступ к компьютерной системе до тех пор, пока не будет выплачен выкуп. Компании, предоставляющие финансовые услуги, по-прежнему являются второй по популярности отраслью, подвергающейся вымогательству.

**Схема преступления:** Доставка → Заражение → Профит.

**Средство реализации:** единственная атака из представленного списка, использующая исключительно технический инструментарий. Однако моменту начала заражения всегда предшествует доставка вредоноса на компьютер, которая, как правило, производится через нажатие ссылки в фишинговом письме. Чтобы убедить пользователя сделать это, используется психологический инструментарий — социальная инженерия.

**Жертва:** учреждения финансовой сферы, в меньшей степени их клиенты.

**Потери:** обнаружение атаки моментальное. Чем дольше компании пытаются бороться с вымогательством, тем больше риск перепродажи и раскрытия конфиденциальной информации клиентов компании. Это ведёт как к финансовым потерям, так и репутационным.

**Способ борьбы:** симулированные атаки, резервное копирование, обучение персонала.

### 5. Социальная инженерия.

Может использоваться в составе других атак либо как самостоятельный метод обмана людей для получения какой-либо выгоды: доступа к системам, хищения информации, перевода денег. По данным KnowBe всего 3 % кибератак используют исключительно технические уязвимости, остальные 97 % реализуются с помощью социальной инженерии.

**Схема преступления:** Любая форма атаки → Профит.

**Средство реализации:** любая форма взаимодействия с другим человеком, предпочтительно дистанционная — телефон, электронная почта, социальные сети и т.п.

**Жертва:** любой человек.

**Потери:** все указанные в предыдущих типах угроз.

**Способ борьбы:** подтверждение личности, биометрия и проверка жизнеспособности, симулированные атаки, обучение персонала.

### ЧТО ОБЪЕДИНЯЕТ ГЛАВНЫЕ УГРОЗЫ?

Скрепляющей нитью рассмотренных киберугроз служит использование социальной инженерии. Технические средства защиты не помогут, если человек обманут и добровольно отдаёт мошенникам деньги или конфиденциальную информацию.

Именно поэтому главный инструмент современных киберпреступников — разнообразные варианты фишинговых атак. По данным отчёта «2019 Phishing trends and intelligence report» в



2018 году объём фишинга вырос на 40,9%. При этом 98% использованных в атаках писем не содержали вредоносных программ. Для хищения учётных данных и других преступных целей использовались фишинговые ссылки (88%) и сайты. В 2018 году было выявлено 1263 фальшивых сайтов финансовых брендов.

Далее мы рассмотрим фишинг и его разновидности более детально и объясним, как преступники используют социальную инженерию для реализации рассмотренных атак.

## ФИШИНГ

Фишинг — кибератака, в которой злоумышленники, выдавая себя за известного человека, делового партнёра или поставщика услуг, входят в доверие к пользователям и заставляют их выполнять какие-либо небезопасные действия.

Наиболее распространены следующие типы фишинга:

### 1. Вишинг

Вишинг — это атаки, совершаемые с помощью телефонных звонков.

Примеры вишинга:

- ◆ звонки от «служб безопасности банков» с сообщением о блокировке аккаунта или подозрительного перевода денежных средств,
- ◆ звонки от «коллег» и «поставщиков» с просьбой срочно открыть какое-либо письмо в почте или совершить оплату по новым реквизитам,
- ◆ звонки от «высшего руководителя» с приказом срочно перевести деньги.

### 2. Смишинг

Смишинг — это СМС-рассылки с предложением перейти по ссылке и ввести свои данные в фишинговую форму или совершить ответный звонок по указанному номеру, скорее всего, платному. Обычно используется по отношению к клиентам банков.

### 3. Фишинговые сайты

Это атака, использующая поддельные сайты узнаваемых компаний, которым жертвы доверяют и без сомнений передают свою конфиденциальную информацию. Чаще всего пострадавшими становятся клиенты банков, пытающиеся зайти в фальшивый личный кабинет.

### 4. Целевой фишинг

Целевые атаки создаются специально для конкретного пользователя с учётом его слабостей и уязвимостей. Одна из разновидностей целевого фишинга — атаки с компрометацией деловой переписки — Business Email Compromise, BEC.

### 5. Китобойный промысел

Это фишинговая атака, аналогичная целевой, но жертвой выбирается один из топ-менеджеров организации — «кит».

## СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ В ФИШИНГЕ

Основными элементами социальной инженерии, которые используют мошенники в фишинге и других атаках, являются:

◆ **Атрибуция** — отправитель сообщения. Чем более авторитетен и узнаваем для получателя отправитель письма, тем быстрее он проникнется доверием к его содержанию.

◆ **Персонафикация** — обращение к получателю письма. Если в нём фигурирует ФИО и персональные данные жертвы, получатель приобретает уверенность, что имеет дело с подлинным отправителем.

◆ **Эмоция** — объект манипуляций для социальных инженеров. Их цель — заставить человека совершить необдуманное небезопасное действие. Сильный испуг или интерес заставляют забыть о правилах осторожности.

◆ **Усилители** — элементы атаки, которые повышают интенсивность вызываемых эмоций. Самые распространённые среди них — срочность и авторитет. Усилители заставляют жертву действовать быстрее вместо того, чтобы осмысливать технические индикаторы фишингового письма.

◆ **Потребности и личностные черты**, как правило, учитываются социальными инженерами при целевых атаках, хотя и требуют дополнительного изучения профиля жертвы. Это позволит персонализировать атаку с учётом личностных слабостей и потребностей и тем самым повысить её результативность. Если на странице пользователя в соцсети есть множество сообщений о сборе помощи животным, наборе волонтеров в приюты и другие альтруистичные порывы, мошенники могут ударить именно в эту точку: «получите перевод в фонд помощи животным», «поучаствуйте в акции от WWF» и т.д.

## ОСОБЕННОСТИ ФИШИНГА В РОССИИ

Анализируя сообщения ФинЦерта с января 2016 по сентябрь 2019 гг. о киберугрозах (640 штук) и примеры фишинговых рассылок (469 штук), нам удалось выявить основные особенности фишинга в финансовой сфере и тенденции его развития.

Основные темы фишинговых писем:

### 1. Уведомления:

◆ Технические (смена настроек платёжных шлюзов, блокировка ресурса, СБИС, уведомления от факса/принтера);



*В части эмоционального манипулирования наблюдается тенденция к сокращению атак, нацеленных на запугивание и жадность, в то время как количество попыток использовать любопытство и желание помочь растёт*

- ◆ От государственных органов (суд, налоговая, госуслуги);
- ◆ О новых законах, приказах, условиях работы (новый закон к ознакомлению, постановление ЦБ РФ);
- ◆ Для банков (компрометация банковских систем, уведомление о выдаче паёв);
- ◆ Для клиентов банков (блокировка карт, выписка из банка);
- ◆ От курьерской службы (Почта России, DHL).

## **2. Рабочий документооборот:**

- ◆ Документы без пояснений (на подпись, доверенность, запрос, документы по запросу);
- ◆ Первичная документация (счета, акты, закрывающие документы);
- ◆ Договоры (на подпись, изменения, вопросы к договору);
- ◆ Счета (подтвердите оплату, выставлен счёт, не оплачен счёт);
- ◆ Отчёты (отчёт не прошел проверку в ФНС, отчёт по обработанному заказу, итоговый отчёт);
- ◆ Сверка (сверка расчётов, сверка остатков, сверка платежей);
- ◆ Реквизиты (новые, изменения, проверка реквизитов);
- ◆ Возврат товара (акт на возврат товара, заявка на возврат товара).

**3. Денежные переводы** (ошибочный перевод, отменён перевод денег, возврат средств, несанкционированный перевод).

**4. Заказ услуг/товаров** (заявка на открытие счёта, заявка на участие в тендере, забери-те оплаченный заказ);

**5. Долг** (погасите, проблемы с оплатой штрафа, числится недоплата по предыдущей поставке, просим обратить внимание на просроченные платежи);

**6. Проверка информации по клиентам и транзакциям** (чёрный список клиентов, запрос о мошеннических транзакциях на счета в вашем банке);

**7. Другое** (подарочный купон, предложение по выводу денег с карты, вакансия/резюме).

На рисунке 2 показано изменение частоты использования разных тем атак в 2016–2019 годы. Большую часть составляют атаки с рабочей до-

кументацией: в 2016 года их доля составляла 59,1 %, а в 2019 году выросла до 70,7 %. Остальные темы используются с разной частотой. Самые популярные — уведомления, долги, заказ услуг/товаров и денежные переводы.

Наиболее популярные виды документов, на которые ссылаются организаторы фишинговых атак — счета и первичная документация. Они стабильно встречаются в каждой второй кампании. Следующие по популярности темы — «сверка» и «договора» (рисунок 3).

В части эмоционального манипулирования наблюдается тенденция к сокращению атак, нацеленных на запугивание и жадность, в то время как количество попыток использовать любопытство и желание помочь растёт (рисунок 4).

В области усилителей наблюдается выраженная динамика к сокращению использования авторитетов и брендов, зато срочность стабильно сохраняет свои позиции (рисунок 5).

В целом изменение других характеристик атак за 2016–2019 гг. не столь значительно. Среди всех атак стабильно используются универсальные темы, где только 9,8 % — письма, предназначенные исключительно для финансовых организаций. Более 90 % писем — содержат в себе вложения, заметно меньше атак со ссылками.

При этом важно понимать, что это характеристики зафиксированных массовых рассылок, из-за чего наблюдается определённая «стандартность» данных фишинговых писем и их характеристик. Например, во всех письмах используются анонимные обращения.

## **ЗАКЛЮЧЕНИЕ**

Финансовые учреждения — лакомые цели для кибермошенников. Размер компании-жертвы и уровень технической защищённости не имеют значения, поскольку всегда можно «взломать» её сотрудников с помощью социальной инженерии. Главное средство реализации такого взлома — фишинг во всех его проявлениях.

\* \* \*

С учётом сохраняющейся в течение последних четырёх лет тенденции к росту количества фишинговых атак на российские компании кредитно-финансовой сферы, при планировании защиты организаций от кибератак крайне важно учесть риски, связанные с человеческим фактором, и предусмотреть в бюджете расходы не только на программно-аппаратные комплексы, но и на обучение сотрудников правильным навыкам.



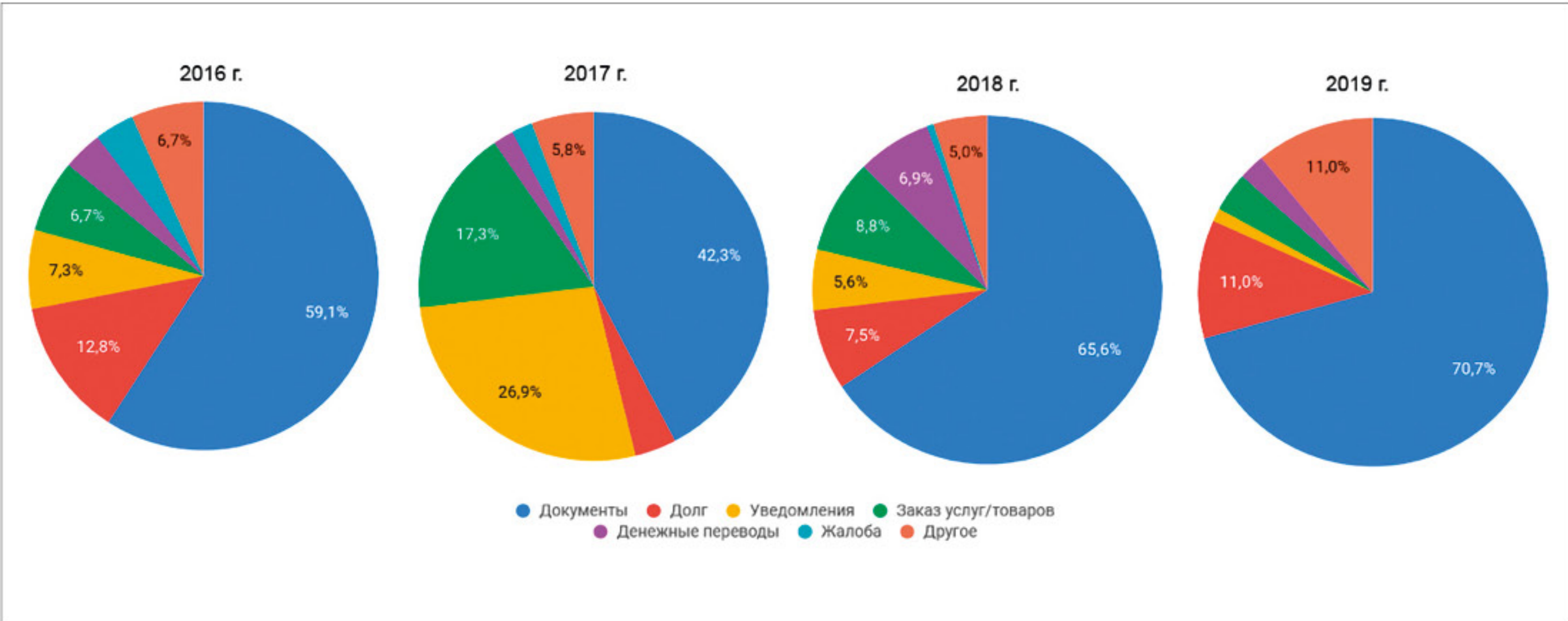


Рисунок 2. Темы фишинговых атак 2016–2019 гг.

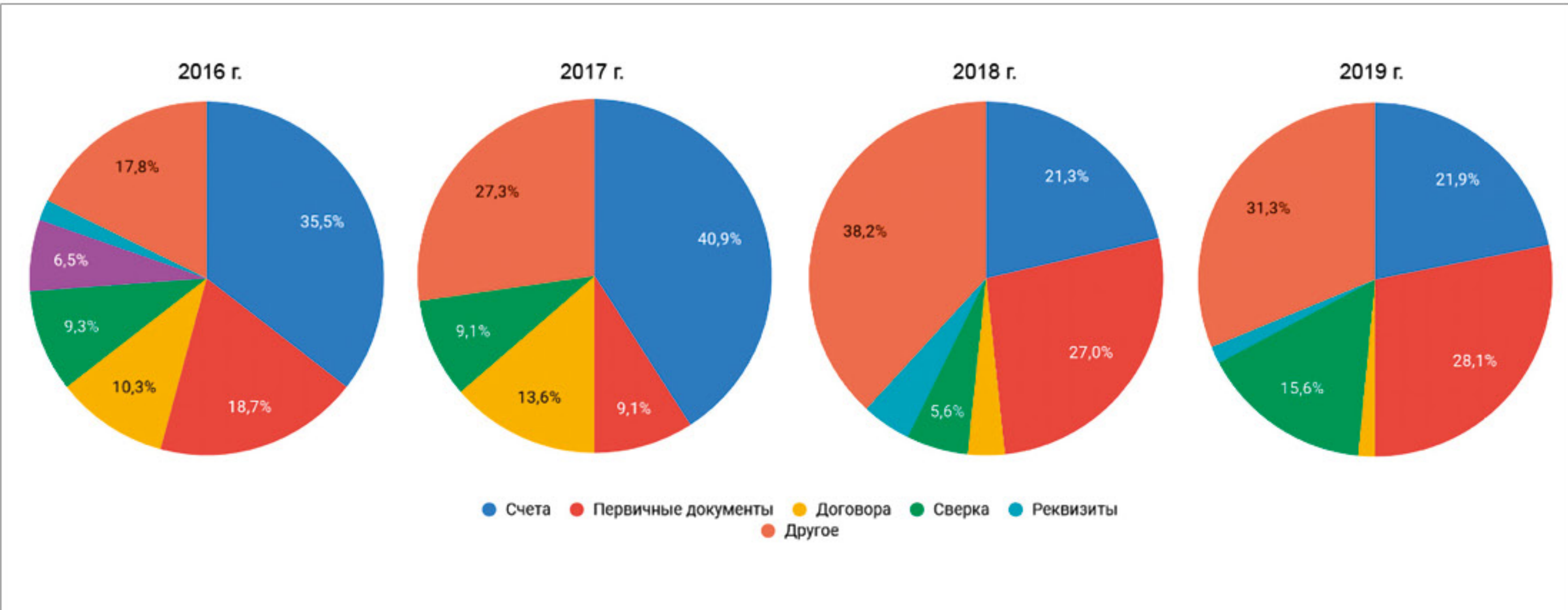


Рисунок 3. Виды документов в фишинговых атаках 2016–2019 гг.



Рисунок 4. Эмоциональное манипулирование в фишинговых атаках 2016–2019 гг.



Рисунок 5. Использование усилителей в фишинговых атаках 2016–2019 гг.



# ИНСАЙДЕРЫ В БАНКАХ — МИФЫ И РЕАЛЬНОСТЬ

ИНСАЙД, КАК ТЕХНОЛОГИЯ, ТРЕБУЕТ ИЗУЧЕНИЯ



**Оксана ДЯЧЕНКО**  
корреспондент  
BIS Journal

**В** рамках X Международного форума AntiFraud Russia состоялся семинар «Инсайдеры в банках — мифы и реальность». Презентация независимого исследователя даркнета Антона Ставера показала, как происходят утечки данных, и раскрыла подробности технологии инсайда.

В прошлом году широкой общественности стало известно о масштабных утечках данных из крупных банков — Сбербанк, ВТБ, Альфа-Банк. Эти «сливы» объединяет одно — они стали возможны исключительно из-за действий инсайдеров, техническая составляющая тут не сыграла никакой роли.

Так откуда берутся инсайдеры? Ответ прост: их вербуют.

## КТО ВЕРБУЕТ СОТРУДНИКОВ БАНКОВ?

Сотрудников банков вербуют три сферы. Первая — это «обнальщики», работающие по своим специфичным схемам. Вторая — «пробивщики», третья — «вербовщики», которые являются главным индикатором того, куда идёт рынок. Если в стране появилась сфера, где люди зарабатывают вербовкой сотрудников для инсайда, значит, дела совсем плохи.

Возвращаясь к «пробивщикам», Антон продемонстрировал, как выглядит скриншот теневого форума, где каждый запрос — это показатель спроса, который эксперт анализирует, чтобы понять, насколько востребован «пробив» в зависимости от сезона. «Кроме запросов есть множество предложений на «пробив», они поступают в сервис напрямую», — подчеркнул Антон.

Он проанализировал рынок «пробива» и пришёл к следующим выводам. Общее число пробив-сервисов — 100+ (т.е. 100 и ещё несколько сервисов, которые появляются после обновления страницы), что говорит о популярности данной сферы. Среди них 30 сервисов с прямым выходом на сотрудников банков и 45 так называемых арбитражных сервисов. Тут речь о сделках, когда «арбитражники» при поступлении к ним заказа обращаются к партнёрам, у которых и покупают инсайдеров для своих заказчиков. Оставшиеся 25 сервисов, то есть, четверть, по словам Ставера, — кидалы.

## СХЕМА РАБОТЫ И РАСЦЕНКИ

Каноническая схема работы пробив-сервиса выглядит так. Сервис даёт рекламу, общается с заказчиками и вербует для них сотрудников-инсайдеров. При поступлении оплаты от заказчика сервис берёт деньги себе, отсчитывая инсайдеру заранее оговорённую, как правило, фиксированную сумму. Сотрудники за счёт «сливов» получают в месяц примерно 30–40 тыс. руб. Бывали случаи, когда платят и по 200 тыс. — за разовый «слив».

Антон привёл действующие расценки:

- ♦ банковская выписка на физическое лицо за один месяц — 2–8 тыс. руб.;
- ♦ банковская выписка на юридическое лицо за один месяц — 2–12 тыс. руб.;
- ♦ детализация звонков — 3–25 тыс. руб.

## МИФ № 1

Первый миф, который укоренился в общественном сознании: данные сливают только нелояльные и низкоранговые сотрудники. Это не так. Антон специализируется на инсайдерах с 2014 года. Вместе с коллегами ему удалось выловить несколько сотен по всему миру. Проанализировав их должности, он приводит такую статистику:

- ♦ Сотрудник службы поддержки — 75
- ♦ Менеджер по продажам — 97
- ♦ Директор филиала/начальник отдела — 44
- ♦ Контрагенты — 21
- ♦ Прочие — 27

Как видим, большинство инсайдеров — это менеджеры по продажам. Они, как правило, «сливают» информацию из госорганов. Например, это очень хорошо знают индивидуальные предприниматели: стоит только зарегистрироваться в качестве ИП, как тут же начинаются звонки из разных банков с предложением открыть расчётный счёт.

Сотрудники службы поддержки чаще всего подбирают по определённым критериям базы для атакующих.

Директора филиалов или начальники отделов встречаются в основном в других странах (в основном в Германии и Австрии). В России инсайдом чаще занимаются начальники отделов продаж и директора региональных филиалов, работающие на долгосрочной основе. Если



в среднем цикл деятельности одного инсайдера — 2–3 месяца, то данная категория может работать и год.

21 пойманный контрагент — это исключительно зарубежные примеры. Речь идёт о внедрении в банк подкупленных партнеров-интеграторов и сторонних специалистов.

К категории «Прочие» эксперт отнёс специалистов по безопасности и обслуживающий персонал (в том числе и уборщиц).

## ТИПЫ ИНСАЙДЕРОВ ПО ЛОЯЛЬНОСТИ

Антон рассказал о типах инсайдеров по лояльности. Во-первых, есть действительно нелояльные сотрудники, которые обижены, обозлены, по каким-то причинам не сумели влиться в коллектив. Особенно много таких появляется, когда по рынку идёт волна сокращений.

Во-вторых, это лояльные сотрудники, которые сливают данные не по своей воле или их попросту разводят. Антон рассказал о мошеннице, которая звонила в банк и излагала душещипательную историю о том, что у неё на руках трое детей, а муж-подлец скрывается от семьи. И просила сделать выписку по его счёту. Удивительно, но схема работала.

Что касается сотрудников, сливающих данные не по своей воле, то среди них самыми опасными являются так называемые слейв — люди, попавшиеся на удочку шантажа. Данный вид инсайдеров распространён в арабских странах — там процветает порядка 20 группировок, занимающихся поиском информации для последующего шантажа. Для сравнения, в России таких группировок всего 2–3.

Наконец, есть такая категория, как «подсадка»: сотрудник работает на конкурентов и слив данных — его цель. Этот тип инсайда сформировался на фоне ужесточения контроля за данными и является серьёзным оружием в конкурентной борьбе. В России «подсадка» пока не развита, хотя примеры есть.

## МИФ № 2

«У нас в банке нет сотрудников, сливающих данные» — это второй миф, не имеющий ничего общего с реальностью.

Антон взял ТОП-100 банков с сайта Banki.ru и проанализировал объявления по «пробиву». Оказалось, что 52 банка из этого списка можно пробить, а это значит, в них уже есть инсайдеры.

Вот список наиболее часто встречающихся у «пробивщиков» банков: Сбербанк, Альфа-Банк, ВТБ, Промсвязьбанк, Райффайзенбанк, Тинькофф Банк, Газпромбанк, Россельхозбанк, МКБ, Совкомбанк и др.

## ВЕРБОВКА

По словам эксперта, даже если нет сервисов, пробивающих банк, есть сервисы, занимающиеся вербовкой.

Всего в России работает 73 сервиса по вербовке персонала. Средняя стоимость найма сотрудника через сервис составляет 15 тыс. руб. (минимум, 7 тыс., максимум — 100 тыс. руб.). Есть банки, в которых стоимость найма выше 100 тыс. руб. — там сотрудники не идут на сделки. Одно время так было в Газпромбанке. Но в большинстве банков сотрудников можно найти в тот же день — везде есть «подкормленные люди». Средний срок найма — одна неделя (минимум, три дня, максимум — один месяц).

В качестве примера эксперт привёл такое объявление: «Помогу в вербовке сотрудников в любом банке РФ. Быстро! Качественно! Недорого! Уже сейчас имеются подкормленные люди в зелёном, красном и большом синем!».

Антон уверен, что даже если в банке сейчас нет инсайдеров, это не значит, что они не появятся: вербовщики работают по чётким схемам уговоров и, как правило, работают хорошо.

## МИФ № 3

«Слив данных через сотрудников искоренить невозможно» — это третий миф.

В общественном сознании прочно укоренилось: если выгнать одного инсайдера, появится другой и т.д. Это не так, уверен Антон Ставер, просто нужно изучить свою организацию и системно заниматься проблемой. Для этого необходим человек, ориентированный на кадровую безопасность.

Специалист по кадровой безопасности должен взаимодействовать с СЭБ, ИБ, HR, контрагентами, предоставляющими данные. Также он должен проводить кадровую диагностику, подбирать контрагентов для мониторинга даркнета либо самостоятельно организовывать мероприятия по поиску сливщиков данных в даркнете. Планировать и организовывать мероприятия по поимке и обезвреживанию сливщиков данных, готовить материалы для контрольной закупки и проводить её, согласовывать мероприятия между отделами, при этом важно, чтобы они проводились без огласки. Также должен быть усилен контроль за наймом и за системами оценки благонадёжности соискателей и сотрудников.

Кроме того, чтобы находить сливщиков, в банке должна быть DLP или иная система мониторинга даркнета. Неплохо иметь в штате или на аутсорсинге полиграфолога. Но главным первым шагом по борьбе с инсайдерами Антон Ставер всё же считает внедрение специалиста по кадровой безопасности. Иначе организацию ждёт хаос.





**Марина БРОДСКАЯ**  
обозреватель BIS Journal

# БРИТАНИЯ В ТРЕВОГЕ

АНАЛИТИКИ ВЕЛИКОБРИТАНИИ ПЫТАЮТСЯ  
ОЦЕНИТЬ ПОСЛЕДСТВИЯ BREXIT И ИЩУТ СПОСОБЫ  
ЗАВЛЕЧЬ В ИБ СВЕЖИЕ КАДРЫ

**Б**ританские эксперты полагают, что к 2021 г. во всём мире будет 3,5 млн вакансий специалистов по кибербезопасности. Доля таких вакансий в Великобритании должна быть, по их мнению, срочно уменьшена, а вклад страны в глобальную индустрию ИБ необходимо сделать более динамичным, разнообразным и устойчивым.

## ЭКСПЕРТЫ СТАВЯТ ПРОБЛЕМУ

Влиятельное интернет-издание Tech-Radar пишет о проблемах информационной безопасности довольно часто. Его позиция полна тревоги, и причин этому предостаточно. Несмотря на то, что сектор информационной безопасности Великобритании оценивается в \$5 млрд и рассматривается как крупнейший в Европе, он страдает от непрерывно растущего дефицита кадров. Больше половины всех предприятий и некоммерческих организаций сталкиваются с нехваткой специалистов в области кибербезопасности. В государственном секторе такой дефицит кадров составляет 18%.

При этом эксперты не устают говорить о том, что молодёжь не расстаётся с гаджетами и осваивает новые технологии и приложения быстрее, чем старшее поколение. Однако, на фоне регулярных сообщений о финансовых потерях в результате взлома компьютерных систем и утечек информации в частных и государственных компаниях, возникает вопрос: почему современное цифровое поколение не стремится делать карьеру в области информационной безопасности? Многих пугает рост стоимости базового университетского образования и растущее значение учёных степеней и постдипломного образования. Но в то же время средняя годовая зарплата в сфере ИБ составляет до £72,5 тыс., что значительно больше средней зарплаты для выпускников других направлений (£23 тыс.). И погасить долги за учёбу, работая в сфере ИБ, можно намного быстрее, чем в других сферах.

Стоит отметить, что в исследовании издания IT Pro указываются другие зарплаты: пятёрка лидеров отрасли ИБ платит своим сотрудникам в среднем £45 851 в год против средней по стране зарплаты в £27,6 тыс.

Что понимает большинство обывателей под кибербезопасностью? Конечно, в первую очередь в голову приходит антивирусное программное обеспечение на рабочем компьютере. Дальше вспоминаются хакеры и киберпреступления. Большинство школьников, планирующих поступать в университеты, слабо представляют, кто такой начальник службы ИБ или начальник отдела защиты информации (CISO), криптограф, пентестер или аналитик вредоносных программ, — пишет Джеймс Лайн, технический директор SANS Institute. — Даже подавляющему большинству студентов, серьёзно задумывающихся о выстраивании карьеры, названия этих должностей ничего не скажут.

## УРОВЕНЬ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Отсутствие специальных навыков по защите информации в IT-секторе негативно сказывается на национальной безопасности в целом. Вопрос защиты от всё более изощрённых угроз уже поднимался на правительственном уровне, бывший министр цифровых и креативных индустрий Марго Джеймс выделяла кибербезопасность как «главный приоритет для правительства», отмечая, что ИБ играет ключевую роль в национальной безопасности и важна для Великобритании, чтобы стать лучшей в мире цифровой экономикой.

*Средняя годовая зарплата в сфере ИБ составляет до £72,5 тыс., что значительно больше средней зарплаты для выпускников других направлений (£23 тыс.)*



Признавая пробел, правительство запустило стратегию «Начальные навыки кибербезопасности», обещая финансирование в размере £2,5 млн для создания в Великобритании Совета по кибербезопасности для подготовки квалифицированной рабочей силы в будущем. Это позитивный шаг, но задача правительства — решить проблему дефицита кадров уже сегодня.

В августе 2019 г. правительство назначило Инженерно-технологический институт (IET) ведущей организацией для разработки и предоставления нового Совета по кибербезопасности Великобритании. Но для комплексного решения проблемы кадрового голода и продвижения ИБ как престижной профессии к этому процессу должны подключиться частные инвесторы, компании из индустрии ИБ, некоммерческие организации, руководители IT-подразделений различных компаний.

### КАК ПОСЛЕДСТВИЕ BREXIT

Участники этого процесса не должны ждать, когда возникнет ситуация полного дефицита кадров или полагаться на программное обеспечение для защиты информации, полагают эксперты. Дефицит кадров может обостриться и при выходе Великобритании из ЕС — как следствие Brexit. В этот момент утечка мозгов из Великобритании в Европу станет более чем реальной. Поэтому компании должны тщательно просчитать все последствия действий политиков и понять необходимость инвестирования в талантливые кадры в области ИБ.

### ЛЮБОПЫТНАЯ СТАТИСТИКА

Согласно опросу Департамента по цифровым технологиям, культуре, СМИ и спорту (DCMS), опубликованному в 2019 г., средний отдел кибербезопасности в компаниях Королевства состоит всего из двух сотрудников. Более половины организаций, согласно тому же отчёту, не знают, что делать при атаке хакеров на сервера компании.

Национальный центр кибербезопасности Великобритании (National Cyber Security Centre) помогает организациям решать проблемы ИБ, предоставляя бесплатные ресурсы для организа-

*Средний отдел кибербезопасности в компаниях Королевства состоит всего из двух сотрудников. Более половины организаций, согласно тому же отчёту, не знают, что делать при атаке хакеров на сервера компании*

ций, стремящихся повысить уровень своей киберзащиты. Но опять же для создания качественных служб ИБ в бизнесе необходима главная составляющая — кадры. А их надо искать и создавать, главным образом, в школах и колледжах.

### ПОЧЕМУ СТАТУС ИБ НЕ ВЫСОК?

Возникает вопрос: почему молодёжь не выбирает карьеру в области ИБ, если там хорошо платят? Многие дети растут, узнавая о традиционных рабочих профессиях (врач, продавец, медсестра) от родителей, и о новых направлениях (например, блогер) — из соцсетей. Но о профессии специалиста по ИБ там не говорят.

Эксперты утверждают, что для изменения такой ситуации вопросы ИБ должны изучаться в раннем возрасте, включаться в учебную программу наравне с математикой, родным и иностранным языками, литературой. Изучение ИБ должно продолжаться и дальше.

### УДАЧНАЯ ПРОГРАММА

Как пример удачного подхода к изучению ИБ часто вспоминают бесплатную учебную программу по кибербезопасности Cyber Discovery, поддерживаемую правительством Великобритании. За два года с момента её запуска в ней приняли участие около 50 тыс. студентов в возрасте от 13 до 18 лет.

Cyber Discovery проходит в британских школах и колледжах и использует геймификацию для обучения и демонстрации, что делает освоение порой сложных основ кибербезопасности (включая криминалистику, кодирование и криптографию) безопасным и увлекательным. Подростки могут на практике проверить свои навыки в ИБ в реальных сценариях, не нарушая закон.

### ОЖИДАНИЯ И РЕАЛЬНОСТЬ

Британское издание IT Pro приводит следующую статистику. По данным аналитической компании Frost&Sullivan, за 2018 г. число вакансий специалистов по кибербезопасности увеличилось на 15%, при этом отмечается и рост предложений по заработной плате специалистов. Государственная статистика скромнее, но тоже впечатляет. В прошлом году количество рабочих мест в секторе ИБ Великобритании выросло на 3,2% по сравнению со средним показателем по стране в 1,9%. Уровень безработицы в британском секторе ИБ составляет всего 1%, спрос на специалистов стабильно опережает предложение.

Так с чем же связан кадровый дефицит? — задаёт со своей стороны вопрос IT Pro, но отвечает на него по-другому. Оказывается, проблема во многом создана самими компаниями.

«Организации выдвигают нереалистичные требования к опыту и технической компетентности потенциального кандидата и ориентированы исключительно на тех, кто занимается компьютерными науками», — это мнение старшего аналитика Forrester Пола Маккея. «Кадровики хотят видеть в должности специалиста по ИБ дипломированного и сертифицированного сотрудника, — уточняет Джаррад Карлтон, руководитель глобальной программы по кибербезопасности Frost&Sullivan. — Но с таким подходом дефицит персонала неизбежен. Должна быть большая гибкость в подборе кадров, стоит привлекать к работе разных специалистов, в том числе и прошедших курсы самоподготовки по ИБ, оценивать их потенциал».

### ЛУЧШИЕ РАБОТОДАТЕЛИ

Недавно опубликован список из 20 крупнейших работодателей Великобритании в сфере кибербезопасности. В ли-



дерах «большая четвёрка» компаний консалтинга и аудита — KPMG, PwC, EY и Accenture. В первой десятке также преобладают финансовые организации. Но эксперты сходятся во мнении, что спрос на специалистов по ИБ будет расти во всех секторах экономики, поскольку организации захотят иметь собственных сотрудников, а не обращаться к консультантам.

«Сегодня специалисты консалтинговых компаний работают как эксперты-аналитики. Они приходят в организацию, на месте оценивают ситуацию и предлагают решение по кибербезопасности. Как только проблема решается, с ними расплачиваются и сотрудничество заканчивается. Предприятия должны быть в состоянии сами обеспечить свою безопасность», — полагает Джард Карлтон.

### КОГО ИЩУТ?

Согласно результатам исследования, вакансий специалиста по информационной безопасности компьютерных систем в Великобритании в три раза больше, чем вакансий инженеров по безопасности (они на втором месте по спросу). В пятёрку лидеров также вошли консультант по безопасности, аналитик по ИБ и аудитор. Отмечается, что аудиторы востребованы, поскольку существующие компьютерные системы подвергаются различным типам угроз. Векторы атак расширяются и меняются ежедневно, а это требует особого контроля.

Информационная безопасность охватывает много разных областей, и аналитические компании и рекрутеры соглашаются, что спрос растёт на навыки во всех областях ИБ. Например, переход компаний на облачные технологии требует всё больше людей с практическим опытом облачной безопасности.

В настоящее время исследовательской компании Forrester требуются специа-



Штаб-квартира Центра правительственной связи (GCHQ) в Четлхеме

листы в центр оперативного реагирования (SOC): операторы, аналитики SOC и аналитики технической безопасности, а также специалисты по анализу угроз и поиску уязвимостей. В Hays Digital Technology аналитик по ИБ возглавляет список востребованных в этом году специалистов — аналитиков по безопасности, архитекторов безопасности, аналитиков по киберугрозам и аналитиков по инцидентам. Руководители компании отмечают также нехватку специалистов по безопасности приложений и растущий спрос на кандидатов из числа программистов-разработчиков, знакомых с жизненным циклом разработки программного обеспечения (SDLC).

### РАБОТЫ МНОГО

Большие хабы, специализирующиеся на кибербезопасности, работают в Англии. В Лондоне и Кембридже, где представлено много стартапов, в Четлхеме работает штаб-квартира Центра правительственной связи (GCHQ), хабы есть в Манчестере и Бирмингеме. В Шот-

ландии, где базируются штаб-квартиры многих международных компаний, крупные центры по защите информации открыты в Глазго и Эдинбурге. В Белфасте (Северная Ирландия) открыт один из самых сильных центров кибербезопасности Великобритании. Центр в Белфасте стал штаб-квартирой для большого кластера международных компаний, поставляющих глобальные продукты и услуги в области безопасности. В создании и налаживании работы центра в Белфасте принимали участие такие компании как Allstate, CME, Citi, PwC, Deloitte, Ernst&Young и BDO. Они же разработали ряд решений по кибербезопасности и используют их при работе с клиентами.

\*\*\*

Британские эксперты полагают, что в сложившейся ситуации с кадрами, единственный правильный путь — это ужесточение законодательства в области ИБ. С одной стороны, такой подход вынудит компании соблюдать требования регуляторов, что безусловно облегчит им выполнение Директивы ЕС по сетевым информационным системам (NISD) и Общего регламента по защите персональных данных (GDPR). А с другой, заставит активно нанимать профессионалов по ИБ и вообще озаботиться проблемой подготовки кадров в этой сфере.

*Согласно результатам исследования, вакансий специалиста по информационной безопасности компьютерных систем в Великобритании в три раза больше, чем вакансий инженеров по безопасности*



**Сергей ПАЗИЗИН**

член редколлегии BIS Journal,  
заместитель начальника Управления  
по обеспечению информационной  
безопасности ДБ Банка ВТБ (ПАО)

# ДЕЙСТВОВАТЬ ПО ВСЕМ НАПРАВЛЕНИЯМ

## ПРИЧИНЫ ВОЗНИКНОВЕНИЯ ДЕФИЦИТА КАДРОВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПУТИ РЕШЕНИЯ ПРОБЛЕМЫ

**О**дной из самых обсуждаемых тем в сфере информационной безопасности в течение последних двух лет является острая нехватка квалифицированных специалистов. Данная проблема актуальна как для государственных структур, так и для коммерческих организаций.

### О ДЕФИЦИТЕ СПЕЦИАЛИСТОВ

В связи с расширением области применения цифровых технологий возрастает интенсивность разработки и внедрения новых приложений и услуг, а также расширяется поддерживающая инфраструктура. Соответственно растет численность подразделений информационных технологий (ИТ) и параллельно потребность в специалистах в сфере информационной безопасности (ИБ).

Кроме того, последние несколько лет происходит активное освоение преступностью открывшихся возможностей, связанных с использованием цифровых технологий. Растет уровень организованности и квалификации киберпреступников, совершенствуются применяемые ими инструменты. С точки зрения киберугроз, среда, в которой функционируют автоматизированные системы, становится гораздо агрессив-

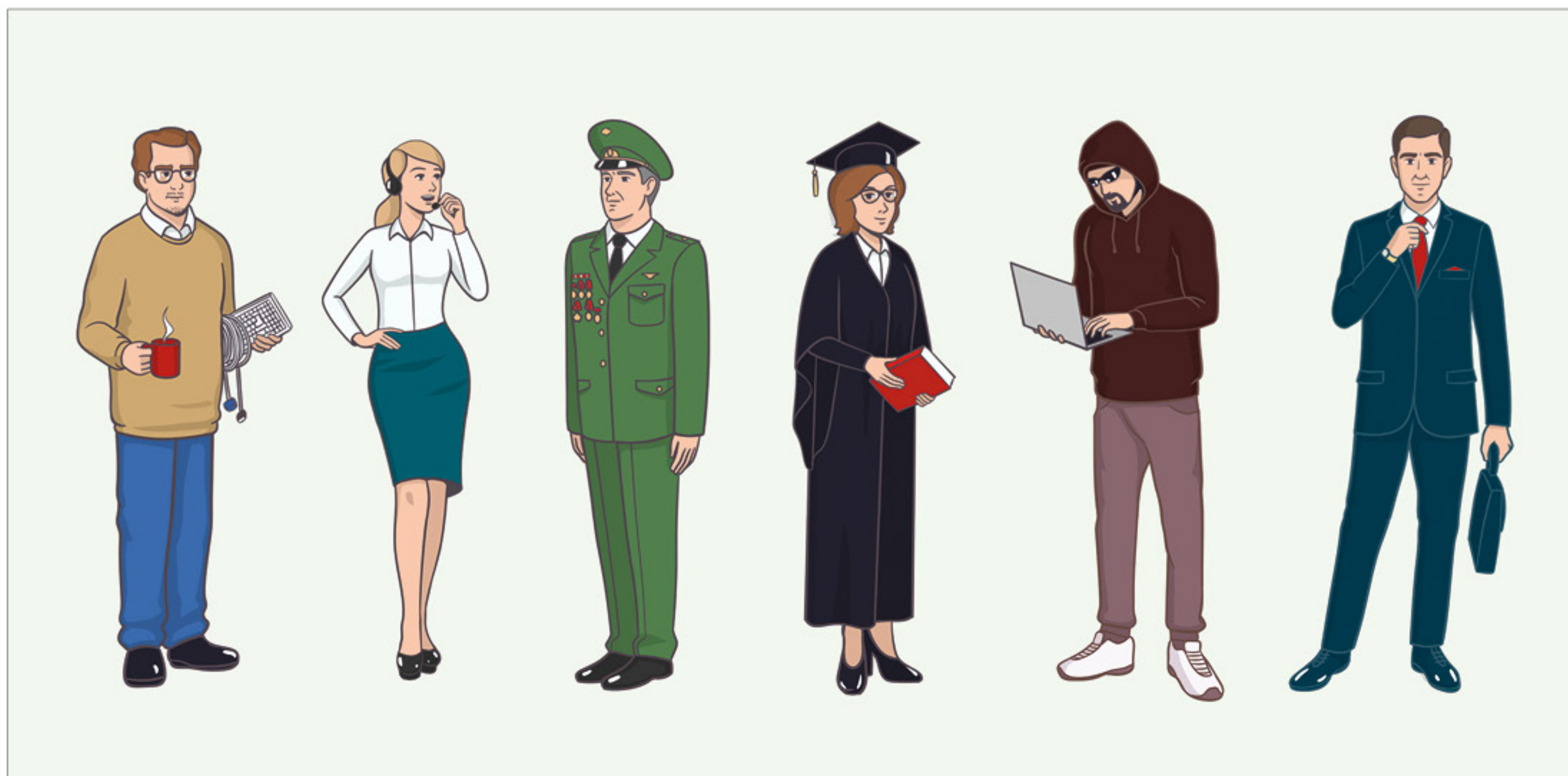
нее. Одновременно растет объем защищаемой информации. Дистанционные банковские сервисы, заказ гостиниц и билетов через интернет, агрегаторы такси, сбор и коммерческое использование информации о посещаемых сайтах и поисковых запросах, возможность распознавания лиц на основе записей камер наблюдения, электронный документооборот и т.д. — все это порождает огромные объемы персональных данных и другой чувствительной информации, нуждающейся в защите. Риски, связанные с кибератаками, вошли в пятерку глобальных рисков рейтинга Всемирного экономического форума в 2019 году. Многие эксперты считают киберугрозы даже более опасными, чем терроризм и глобальные экологические проблемы. Данные процессы естественным образом приводят к ужесточению требований регуляторов и росту объема отчетности. Как следствие, растут затраты времени на обеспечение не только реальной, но связанной с ней «бумажной» безопасности.

Одновременно с количественным расширением отрасли, в настоящее время, происходит качественный переход, связанный с изменением места и роли ИБ в современном (в т.ч. банковском) бизнесе. Применяемые меры обеспечения ИБ уже не могут быть ограничены

выполнением контрольных функций и администрированием средств защиты. Рост электронной коммерции, переход к дистанционному предоставлению финансовых и государственных услуг, высочайшая степень автоматизации приводят к 100 % зависимости бизнес-процессов от достоверности информации, содержащейся в автоматизированных системах, и возможности ее обработки. Характер угроз ИБ, в современных условиях, напрямую зависит от решений бизнес-подразделений по внедрению тех или иных бизнес-процессов. В частности, в кредитно-финансовой организации практически любое изменение бизнес-процессов связано с изменением работы автоматизированных систем, и, следовательно, требует анализа со стороны ИБ. Специалисты ИБ должны участвовать в создании/изменении каждого сервиса/услуги от бизнес-идеи до ее реализации, контролировать безопасность каждого обновления.

При этом на конкурентоспособность компании влияет не только недооценка угроз, но и избыточные ограничения. В этих условиях простое следование стандартам безопасности уже не позволяет обеспечить адекватность решений — необходимо уметь оценивать и принимать риски.





Обеспечить безопасность организации может только команда профессионалов. Для подготовки таких специалистов нужны разные стандарты и разные формы образования

Данные процессы отражаются также в нормативном регулировании сферы ИБ. Выполнение требований новых законодательных инициатив в области защиты персональных данных, безопасности критической информационной инфраструктуры, учету рисков ИБ при определении достаточности капитала Банков подразумевает, что обеспечение ИБ — это задача всей организации, а не только подразделения ИБ.

Реализация такого подхода к обеспечению ИБ порождает потребность в новых категориях специалистов, которые пока не предусмотрены профессиональными стандартами. Имеющиеся профессиональные стандарты в области ИБ не покрывают всех потребностей практики. В отличие от сферы ИТ, где имеется широкий спектр образовательных стандартов для самых разнообразных видов работ, в сфере ИБ их явно недостаточно.

### **ПОСТРОЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА**

Чтобы эффективно решать проблему дефицита специалистов в области защиты информации, необходимо представлять, какие виды работ выполняют

сотрудники подразделения ИБ. Перечислим основные из них:

- ◆ внедрение средств защиты, их настройка и поддержка;
- ◆ выполнение функций операторов программно-аппаратных комплексов, взаимодействие с персоналом, информирование и обучение;
- ◆ контроль соблюдения требований ИБ, выявление внутренних нарушений;
- ◆ обеспечение соответствия требованиям регуляторов, подготовка нормативно-методических документов;
- ◆ согласование в части ИБ внутренних нормативных документов, подготовленных другими подразделениями; организация и совершенствование системы управления ИБ;
- ◆ поиск уязвимостей, тестирование на проникновение, анализ кода разрабатываемых приложений на безопасность;
- ◆ обработка инцидентов, противодействие кибератакам;
- ◆ оценка состояния ИБ, выявление угроз и анализ рисков, взаимодействие с бизнес-подразделениями.

Для каждого из перечисленных видов работ требуется наличие специфических знаний и опыта, а также разных личных качеств. Поэтому обеспечить

безопасность организации может только команда профессионалов. Для подготовки таких специалистов нужны разные стандарты и разные формы образования, предполагающие подготовку специалистов как в области компьютерных наук, телекоммуникаций, технической защиты, нормативного регулирования, так и тех, кто способен проводить аналитическое исследование бизнес-процессов и связанных с ними информационных потоков с точки зрения ИБ.

При этом требовать от 17-летнего выпускника школы, чтобы он раз и навсегда решил, чем будет заниматься, было бы наивно. Поэтому необходимо не только иметь комплекс профессиональных стандартов, перекрывающий все возможные потребности в специалистах, но и обеспечить для специальностей, входящих в укрупненную группу направлений и специальностей в области ИБ в рамках их образовательных стандартов, специализацию по отдельным видам выполняемых работ и общих трудовых функций, входящих в профессиональные стандарты, с учетом общего направления базовой подготовки учащихся. Студент старших курсов должен иметь возможность выбрать ту специализацию, которая ему интересна,



и в которой он сможет максимально реализоваться. То есть, должна быть возможность выбора дисциплин или блоков дисциплин в рамках специальности. Тем более, что на практике, в основном, нужны не «универсальные безопасники», а специалисты максимально компетентные в своей узкой области.

Подход, основанный на универсальной базовой подготовке и возможности выбора дополнительных дисциплин, позволит также не пытаться определить на много лет вперед точное число специалистов по каждому узкому направлению. На последней стадии подготовки появится возможность подстройки под имеющийся спрос. Кроме того, должна быть возможность получить еще одну специализацию уже после окончания обучения, пройдя обучение по соответствующему набору дисциплин.

Следует также учитывать, что подготовка и утверждение стандарта образования, базирующегося на определенных профессиональных стандартах, — это длительный процесс, а срок обучения специалиста (магистра) — это еще 5 (6) лет. Поэтому, даже если сделать фантастическое предположение о том, что кто-то напишет идеальный профессиональный стандарт, с учетом которого будут созданы новые или уточнены имеющиеся образовательные стандарты, в такой быстро меняющейся области, как обеспечение ИБ, к моменту выпуска специалистов по этому стандарту он уже устареет. Следовательно, нет другого выхода, как доверять вузам и преподавателям определять содержание профильных учебных курсов непосредственно перед их включением в расписание или даже в процессе чтения. При этом важно научить специалиста думать, привить исследовательские навыки, а не просто записать в программу набор знаний, которые вскоре устареют.

Здесь будет уместным привести мнение судьи Конституционного суда Константина Арановского о том, что одна из главных проблем российского высшего образования — подконтрольность вузов административному началу, когда «академическая свобода» университетов уступается в угоду обслуживанию «системы, которая выдает разрешения на профессию». Ключевым условием

*Важно научить специалиста думать, привить исследовательские навыки, а не просто записать в программу набор знаний, которые вскоре устареют*

работы вуза является автономность учреждения, отметил Арановский, и без нее нельзя рассчитывать на высокий уровень образования и качество дипломов. Сейчас же в учебной работе «ценят не преподавание и не учебу, а учебно-методические комплексы», которые в первую очередь нужны не для образовательного процесса, а для служб, «чтобы те хорошо себя чувствовали и оставались при важном деле на выгодных позициях». Подробнее на РБК: <https://www.rbc.ru/rbcfreenews/5da3fa6c9a7947230f0f57f8>

При построении системы образования в сфере ИБ нужно также учитывать, что квалифицированные специалисты такого профиля необходимы не только для обеспечения конкурентоспособности и безопасности компаний. Информационная безопасность — важнейшая составляющая обеспечения безопасности государства.

В то же время сложившаяся ситуация высокого спроса на специалистов ИБ со стороны коммерческих компаний приводит к оттоку специалистов из учебных заведений и, как следствие, к еще большему дефициту квалифицированных специалистов. Поэтому необходимы программы поддержки базовых вузов, осуществляющих подготовку по данному направлению, создание условий для работы профессорско-преподавательского состава. Нормативная учебная нагрузка на преподавателей должна позволять им развиваться, не отставая от технологий и передовых идей, вести активную научную работу.

### ЭФФЕКТИВНОЕ ИСПОЛЬЗОВАНИЕ КАДРОВЫХ РЕСУРСОВ

Совершенствование подготовки специалистов по ИБ — важная и очевидная задача. Но решать проблему дефицита кадров можно не только механически реагируя на происходящее: выросла потребность — расширяем подготовку. Необходимо также создавать условия

для максимально эффективного использования имеющихся кадровых ресурсов.

Очевидно, что мы не можем повлиять на возрастание роли цифровых технологий и значения ИБ, но вполне можем работать по следующим направлениям:

- ◆ Совершенствование и унификация нормативного регулирования (нормативное регулирование не должно представлять из себя лабиринт, зачастую невыполнимых требований; стандарты и требования должны быть инструментом, который упрощает работу специалистов ИБ).

- ◆ Международное сотрудничество в области противодействия киберпреступности и эффективное расследование киберпреступлений (создание безопасной среды для всех — экономически более эффективно, чем «рытье окопов и колючая проволока вокруг каждого здания»).

- ◆ Развитие защищенных облачных платформ и снятие нормативных ограничений на их использование (для защиты облачной платформы нужно гораздо меньше ресурсов, чем в сумме для построения защищенных систем в каждой отдельной организации).

- ◆ Разработка и внедрение эффективных средств защиты (в том числе, для надежной идентификации и аутентификации, средств автоматизации и других инструментов, повышающих производительность труда специалиста по ИБ).

\* \* \*

Таким образом, решение проблемы дефицита кадров не заканчивается разработкой новых образовательных стандартов — необходима работа по всем направлениям: совершенствование образовательного процесса, привлечение квалифицированных кадров к преподавательской работе, создание условий для переподготовки кадров, выстраивание эффективной системы безопасности.





**Борис СТОЛПАКОВ**  
историк криптографии,  
кандидат физико-  
математических наук

# ЭФИР ЛЬДА И ПЛАМЕНИ

## ВКЛАД КРИПТОГРАФОВ В ЗАЩИТУ СОЮЗНЫХ АРКТИЧЕСКИХ КОНВОЕВ

**В**о время Великой Отечественной войны в советской Арктике противоборство с врагом шло не только в ледяных морских водах и на скалистых заполярных рубежах, но и в радиоэфире. Радиосвязь на огромных пространствах Севера часто была единственно возможным и необходимым источником информации для наших воинов и тружеников Заполярья. Впрочем, как и для огромной вражеской группировки. В такой обстановке роль засекречивания радиосвязи и радиоразведки трудно переоценить. В сложных метеоусловиях, в условиях полярной ночи, зимы, силы и средства радиоразведки зачастую были единственными, способными информировать командование о противнике.

### НАЧАЛО

В советской Арктике гитлеровцам противостоял, прежде всего, наш Северный флот (СФ). Это самый молодой из флотов России. До 1917 года флот и его главная база Александровск на берегу Екатерининской гавани в Кольском заливе ещё не успели сформироваться в полной мере. Развитие Кольского севера России и военного флота в годы Первой мировой войны, связанные с поставкой союзниками военных грузов и прокладкой железной дороги Петрозаводск-Мурманск, было остановлено Гражданской войной. Положение изменилось лишь в 30-е годы, когда правительство СССР приняло решение о создании Северного флота. Его

первые боевые корабли были переброшены в Заполярье из Кронштадта по Беломорско-Балтийской водной системе. В 1939 году бывшему Александровску вернули статус города с новым названием — Полярный. Во время Великой Отечественной войны именно там находилась главная база СФ. В 1940 г. новый флот возглавил 34-летний контр-адмирал Арсений Григорьевич Головкин, он руководил СФ все военные годы. На флоте радиоразведка осуществлялась береговым радиоотрядом. Материалы радиоперехвата сообщений противника поступали в Полярный, в разведотдел штаба флота специалистам дешифровально-разведывательной службы (ДРС). В июне 1940 г. её начальником стал Евгений Иванович Портнов, молодой выпускник Высшего военно-морского училища имени Фрунзе в Ленинграде. Он возглавлял дешифровальную службу СФ всю войну. Это маленькое подразделение отличалось стабильностью: всего 15 офицеров побывали в его составе за все военные годы.

### ПЕРВЫЙ БОЕВОЙ ОПЫТ

Уже опыт первых месяцев войны показал важность перехвата сообщений в УКВ диапазоне. Именно он использовался в радиопереговорах авиации противника, имевшей в северных условиях бездорожья особое значение. Перехват радиосвязи немецкой авиации, которая велась в основном открытым текстом, несложная система условных обозначений и маскировки, быстро раскрывая, давали ценные сведения. Но ско-

ротечность действий боевой авиации не оставляла возможности своевременно использовать эту информацию, добытую в пунктах радиоперехвата. На что и рассчитывал противник, почти не маскируя радиосвязь. Чтобы результаты перехвата не теряли свою ценность, они сразу должны были поступать в органы управления действующих соединений, особенно авиации. Так, в 1942 г., по инициативе радиоразведчиков, при командном пункте ВВС флота была открыта специальная вахта перехвата в радиосетях «самолет — самолет» и «самолет — наземная станция».

### ПОДДЕРЖКА СОЮЗНЫХ КОНВОЕВ

Вскоре после начала боевых действий добавились и вышли на первый план задачи радиоразведки СФ по поддержке союзных арктических конвоев. Конвои доставляли в Советский Союз вооружение и прочие грузы из США и Великобритании, а из СССР для этих стран — стратегическое сырьё. Пунктами назначения являлись Архангельск, строившийся порт Молотовск (ныне Северодвинск) и Мурманск.

Ценность арктического маршрута заключалась в том, что так было ближе и проще доставлять грузы в европейскую часть СССР и непосредственно на фронт. Поэтому через северные моря везли особенно много оружия. Вместе тем, пути арктических конвоев проходили в сложных для плавания районах: постоянные штормы, туманы; а зимой ещё и льды, и обледенение судов, грозя-





Союзный конвой в пути



Зимний и летний маршруты арктических конвоев

щее гибелью. Полярная ночь скрывала караваны от противника, но во время полярного дня, около 115 суток, спрятаться было невозможно. Обеспечение безопасности перехода союзных конвоев от порта формирования до порта назначения возлагалось на английские корабли. Суда из портов восточного побережья США или Канады под конвоем шли в Великобританию или в Исландию, с декабря 1942 года арктические конвои стали формировать в Ливерпуле. Число судов в караванах доходило до 40–50. Караваны транспортов сопровождались эскортом из боевых кораблей для защиты от вражеских подводных лодок и авиации. На случай появления крупных надводных сил противника на отдалении от конвоя шли отряды ближнего и дальнего прикрытия из тяжёлых кораблей: линкоров, авианосцев, крейсеров. При пересечении меридиана мыса Нордкап конвои вступали в операционную зону советского Северного флота. Эскорт усиливался за счёт советских кораблей, обычно 2–3 эсминцев, и авиации.

За 10–14 суток конвои подходили к советским водам и далее шли либо в Мурманск, либо направлялись в сторону Архангельска. Главное преимущество Мурманска состояло в том, что его порт зимой не замерзал. Но весьма серьёзную опасность представляла близость линии фронта, проходившей всего в нескольких десятках километрах от города. Вражеским самолётам требовались всего лишь минуты, чтобы, взлетев со своих аэродромов, начать бомбардировку. Архангельск, удалённый от линии фронта, меньше подвергался

авиаатакам и был лучше подготовлен к приёму большого потока грузов. Но достичь его было тяжелее: Белое море на 6–7 месяцев замерзало, и тогда движение было возможно только с помощью ледоколов.

### ПЕРВЫЕ КОНВОИ И ПОТЕРИ

Первый английский конвой направился от Исландии к советским берегам 21 августа 1941 г. Уже 31 августа союзные суда благополучно достигли Архангельска. До конца года в СССР прибыли ещё шесть союзных конвоев и четыре отправились обратно. Все конвои добрались до цели без потерь: немецкое командование, рассчитывавшее на «молниеносную войну», в 1941 г. не предпринимало против них активных действий. Ситуация изменилась в начале 1942 года, к тому времени немцы сосредоточили на базах в Норвегии сильный флот во главе со своим самым мощным линкором «Тирпицем» и сотнями самолётов. Вот тогда началась настоящая охота за союзными караванами. 7 января 1942 года случилась первая потеря — был потоплен британский транспорт «Вазиристан», а вскоре жертвой подводной лодки стал эсминец «Матабеле». Английский автор так описал судьбу его экипажа: «Эсминец «Матабеле» был торпедирован и в течение двух минут затонул. Экипаж спасательного судна, прибывшего на место происшествия через несколько минут, увидел, что море усыпано телами людей в спасательных жилетах, но они не двигались, а безвольно и ритмично, как надувные куклы, качались на волнах, словно исполняя страшный танец смерти, напо-

миная живущим, что выживание в арктических водах — вопрос нескольких минут. Из 200 человек, входивших в команду, в живых остались только двое».

### БОЕВАЯ ЗАДАЧА — ВЗЛОМ АВИАКОДОВ

Получив сведения о выходе союзного конвоя из порта, противник обычно развёртывал в Норвежском море и в районе Новой Земли до 10–15 подводных лодок. На переходе конвой бомбила авиация. Четверть кораблей, отправленных за три месяца март-май по этому пути, были потоплены немцами. Всё же радиоразведка СФ и тогда помогала избежать более крупных потерь. Так, 30 мая 1942 г. она предупредила об атаке бомбардировщиков противника, и советские истребители сорвали её своей успешной атакой. Возглавлявший атаку Герой Советского Союза Борис Сафонов увеличил счёт своих побед. К сожалению, отважный лётчик тогда и сам погиб в море. Немецкое командование сочло чрезмерными свои потери: ещё во время боя радиоразведчики перехватили радиogramму с приказом прекратить атаки на конвой и всем самолётам вернуться на базы. Криптографы ДРС активно участвовали в защите конвоев. Согласно документам, А. Данилов взламывал немецкие авиакоды, «несмотря на ежедневную смену и применение оперативных позывных». С его помощью были получены сведения: «а) о вылетах бомбардировочной авиации на наши объекты (в 1941 г. 71 раз, за 4 месяца 1942 г. 29 раз); б) о вылетах разведывательной авиации, её последующей деятельности и местонахождении





Корабли прикрытия конвоя PQ-17

(в 1942 г. 91 раз); в) об обнаружении ею кораблей СФ и конвоев союзников (в 1942 г. 15 раз)».

### **«СОВЕТСКИЙ СОЮЗ НЕСЁТ НЕСРАВНЕННО БОЛЕЕ СЕРЬЁЗНЫЕ ПОТЕРИ»**

Британское адмиралтейство увеличило силы эскорта, но избежать потерь даже крупных боевых кораблей не удалось. Известна печальная история конвоя PQ-17. Этот конвой, вышедший 27 июня 1942 года, помимо эскорта сопровождали отряды ближнего и дальнего прикрытия из 6 крейсеров, 2 линкоров и авианосца. На перехват конвоя 5 июля вышел «Тирпиц» с кораблями сопровождения. Но вскоре немцы перехватили и дешифровали три радиogramмы, извещавшие о его выходе из фьорда: от советской разведывательной группы, скрывавшейся в прибрежных скалах; от подлодки K-21 под командованием Н. А. Лунина, дежурившей у выхода из фьорда; от британского самолёта авиаразведки. Командир «Тирпица» не стал рисковать и на следующий день вернул его на стоянку. Не зная этого и опасаясь встречи, британские отряды прикрытия, как известно, покинули конвой, а немецкие подлодки и самолёты принялись охотиться за союзными транспортами. В итоге из 36 судов конвоя PQ-17

дошли до Мурманска и Архангельска лишь 11. При этом из 202 фашистских самолётов, участвовавших в атаках на конвой, было сбито всего пять. Ввиду больших потерь правительство Великобритании усомнилось в продолжении арктических конвоев. На что И. В. Сталин в своём ответном письме особо подчеркнул: «Я, конечно, не считаю, что регулярный подвоз в северные советские порты возможен без риска и потерь. Но в обстановке войны ни одно большое дело не может быть осуществлено без риска и потерь. Вам, конечно, известно, что Советский Союз несёт несравненно более серьёзные потери».

PQ-18 отправился в путь в сентябре. «Он состоял из 40 судов, его сопровождал значительно более сильный эскорт, в составе которого впервые находился конвойный авианосец. Но всё же 13 транспортов были потоплены. В 1942 году немцы потопили 69 союзных транспортов из 85, уничтоженных ими в этом районе за всю войну».

### **ВЗАИМОПОМОЩЬ РАДИОРАЗВЕДЧИКОВ**

В 1942 г. в связи с активизацией противника возросла ценность сведений флотской радиоразведки. Также весьма полезным стало открытие в конце 1942 г. в Полярном станции радиопе-

ленгования английской морской радиоэлектронной разведки. Вскоре «начался взаимный обмен частотами радиосвязи объектов разведки, а также информацией о перехвате сеансов связи». Благодаря этой совместной деятельности, командования СФ и эскротов конвоев располагали необходимой информацией, что позволяло изменять маршруты конвоев в обход сил противника или подготовиться к отражению атаки, лишив противника преимуществ внезапности. За 1942 год ДРС «316 раз своевременно оповестила о налётах бомбардировщиков».

### **ЛЕТО 1943. ПЕРЕРЫВ КОНВОЕВ**

С марта по ноябрь 1943 года конвои снова не ходили, хотя союзники успешно вели битву за Атлантику. И вновь И. В. Сталин ответил категорично на присланное уведомление: «Я понимаю этот неожиданный акт как катастрофическое сокращение поставок военного сырья и вооружения Советскому Союзу со стороны США и Великобритании, так как путь через Великий океан ограничен тоннажем и мало надёжен, а южный путь имеет небольшую пропускную способность, ввиду чего оба эти пути не могут компенсировать прекращения подвоза по северному пути. Понятно, что это обстоятельство не может не отразиться на положении советских войск».

### **НОВЫЕ ВОЗМОЖНОСТИ**

Летний перерыв в движении союзных конвоев радиоразведчики СФ использовали для укрепления своих позиций в Арктике. В 1943 г. были созданы пункты радиоперехвата в Иоканье на Кольском побережье; в Губе Белушья и на мысе Желания на островах Новой Земли; в Коле; на острове Диксон в Енисейском заливе. Появились новые возможности для контроля сообщений противника. В результате удалось установить районы действия немецких подлодок. Туда направлялись дополнительные противолодочные силы и усиливалась охрана транспортных судов. Эти меры позволили существенно снизить потери конвоев, а в некоторых случаях и уничтожить врага. Так, в августе 1943 г., в предполагаемом районе дей-



ствия немецких субмарин у Новой Земли патрулировала советская подводная лодка С-101. Наши подводники обнаружили идущую в надводном положении немецкую лодку У-639 и потопили её залпом трёх торпед. На месте гибели лодки моряки нашли сигнальную книгу и передали её в ДРС. Попали в руки дешифровальщиков и кодовые переговорные таблицы с подбитого зенитчиками Ю-88, севшего у Териберки. Хотя экипаж успел выбросить в море бортовые документы, водолазы подняли их и передали в разведотдел.

### ОБМЕН ОПЫТОМ С СОЮЗНИКАМИ

Приобретённый опыт и расширение возможностей перехвата сообщений противника позволяли радиоразведчикам и криптографам «заблаговременно обеспечивать союзников информацией о позициях сил противника на маршруте перехода конвоев, о радиочастотах и позывных противника, о радиопеленгах на немецкие корабли и береговые радиостанции. Подобная информация была важна для британских штурманских служб, составлявших и корректировавших по данным разведки маршруты перехода конвоев». Но и результаты разведывательной деятельности англичан на Севере представляли интерес для флотских разведчиков. «Во-первых, это было связано с объективно высокими показателями работы англичан. Например, 25–26 декабря 1943 г., при поиске немецкого линкора «Шарнхорст» советской радиоразведкой было перехвачено две радиограммы, а англичанами — семь. Во-вторых, по причине отсутствия собственных корабельных радиопеленгаторов командование радиоразведки СФ просило союзников предоставлять информацию с их кораблей». Нередко данными британской радиоразведки пользовались негласно. Документы свидетельствуют: А. Марков «повседневно выполнял сложную техническую работу криптографического анализа шифрпереписки английских военно-морских сил и авиации», находившихся в операционной зоне СФ; Портнов «самостоятельно читал переписку английской авиации, действовавшей в Северном и Норвежском морях, что дало возможность знать о движе-

*Всего за годы войны было вскрыто 9 кодов и 575 их вариантов, прочитано свыше 55 тысяч криптограмм, исходящих от самолётов и авиабаз, что позволило контролировать закрытую переписку германской авиации в северных широтах*

нии там немецких конвоев и о действиях немецких подводных лодок на морских коммуникациях».

### ВСКРЫТИЕ СЕКРЕТОВ НЕМЦЕВ В НОРВЕГИИ

Возобновившись в конце 1943 года, движение конвоев продолжалось до апреля 1944 года, затем последовал перерыв на полярный день и с августа конвои шли уже до самой Победы. Как известно, в октябре 1944 года Петсамо-Киркенесская операция Красной Армии лишила гитлеровцев важных баз и аэродромов на Севере, а к 1 ноября 1944 г. советское Заполярье было освобождено. В период подготовки к этому наступлению, «состоялся обмен данными об организации радиосвязи береговой обороны южной Норвегии — со стороны англичан, и данными об организации радиосвязи береговой обороны в северной Норвегии, имевшимися в советской разведке». Специалистам ДРС было чем заинтересовать союзников. Так, майор В. Баташев «проделал большую и кропотливую работу по определению боевого состава и дислокации противника», включая детальное описание пяти его основных аэродромов, что весьма пригодилось при планировании Петсамо-Киркенесской операции. Лейтенантом В. Семёновым «разработана таблица условных сокращений, применявшихся в сетях ВМС береговой обороны немцев в Норвегии. Одновременно он же проделал большую аналитическую работу по определению систем шифров, использовавшихся немцами в ВМФ и частях береговой обороны». А. Данилов «разработал 8 сложных и часто меняющихся кодов, применявшихся в радиосетях береговой обороны». Это только в 1944 г. позволило выявить движение и состав 24 конвоев противника, установить базировавшиеся в Норвегии

соединения ВМС. «Под руководством капитана 3-го ранга Портнова был разработан код постов СНиС (службы наблюдения и связи — Б.С.) района Варангер-фьорда, что дало возможность в течение всего 1944 г. (вплоть до освобождения Северной Норвегии) читать донесения постов противника о движении немецких караванов, судов и военных кораблей». Как отмечено в документе, эти сведения сыграли особую роль в Петсамо-Киркенесской операции.

### ЗАВЕРШЕНИЕ КОНВОЕВ

Хотя в конце декабря 1944 г. британская станция в Полярном была закрыта, взаимодействие радиоразведчиков сохранилось, продолжались и союзные конвои. Потеряв базы на советском Севере, немецкие подводники сменили тактику. Теперь их субмарины ждали суда союзников у входа в Кольский залив, иногда им везло. Последний союзный конвой отправился из Шотландии уже после Победы, 12 мая 1945 года, и прибыл в Кольский залив 20 мая.

\* \* \*

*Всего за годы войны было вскрыто 9 кодов и 575 их вариантов, прочитано свыше 55 тысяч криптограмм, исходящих от самолётов и авиабаз, что позволило контролировать закрытую переписку германской авиации в северных широтах. С помощью аналитических методов были раскрыты 26 шифров, 13 кодов, использовавшихся силами береговой обороны, маячной, аварийно-спасательной и радионавигационной службами противника.*

Послевоенная жизнь бывшего руководителя флотских криптографов, капитана 1-го ранга Е. И. Портнова, прошла на Кольском Севере. С 1955 г. по 1974 г. он возглавлял Мурманское высшее инженерное морское училище.



# thycotic



**ХАКЕРЫ НАС  
НЕ НАВИДЯТ**

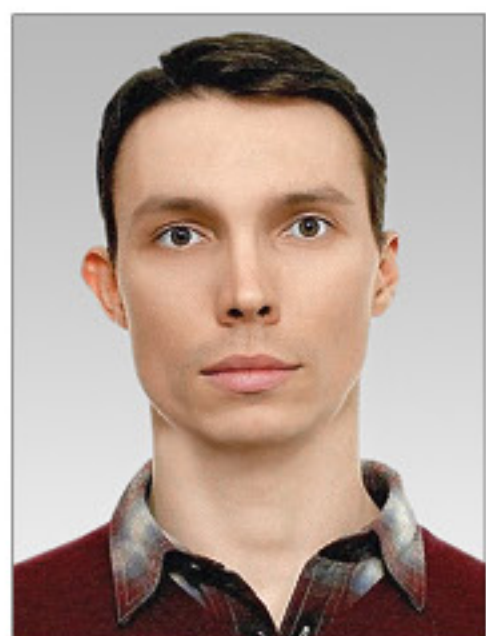


**ИТ-ПРОФИ  
НАС ЛЮБЯТ**



**Управление паролями и контроль доступа**  
**[www.thycotic.ru](http://www.thycotic.ru)**





**Илья ГОРЮНОВ**  
директор по развитию бизнеса  
ООО «АФИ Дистрибьюшн»

# КОГО ВЗЛОМАЮТ В 2020 ГОДУ?

**М**ы опросили 1340 средних и крупных российских компаний финансового и промышленного секторов: по итогам 2019 года «детские болезни» кибербезопасности были побеждены. Более 92% компаний обладают полным набором базовой защиты от спама и вирусов, исправно устанавливают обновления операционных систем и актуальные версии прошивок сетевых устройств — это на 22% больше, чем двумя годами ранее.

Почти на четверть увеличилось количество крупных организаций, которые установили в своих сетях SIEM-систему последнего поколения, включили мониторинг доступности и настроили автоматическое создание заявок в случае срабатывания систем защиты.

Взломать такие сети и заразить сервера шифровальщиками заметно сложнее, а атаки тысяч автоматических роботов, которые круглосуточно ищут уязвимости в сетях компаний всего мира, не пройдут незамеченными — прекрасный результат, но, скорее, для 2015 года.

В 2020-м планка заметно выше: помимо базовых средств безопасности, реагирующих, когда враг уже на пороге и ломится в сеть, жизненно необходимы решения, которые защитят от последствий кражи паролей или уничтожения данных.

После многочисленных кибератак и сливов похищенных данных более

4 000 000 000 паролей от учетных записей находятся в свободном доступе — любой желающий может загрузить такую базу данных из Интернета и использовать её для ускорения взлома.

**81% взломов корпоративных сетей происходит через украденные и подобранные пароли<sup>1</sup>**

Используете известный пароль — вас взломают.

Используете один и тот же пароль от почты и от сервера — вас взломают.

Используете похожие пароли от «Одноклассников» и от Active Directory — вас взломают.

Забыли поменять стандартный пароль от нового устройства — вас взломают.

Не меняли пароль более года — вас взломают.

Один и тот же пароль на нескольких устройствах — вас взломают ещё быстрее.

У кого-то из ваших специалистов есть описанные выше проблемы? **Правильно, вас взломают.**

Здесь стоит ещё раз отметить реалии 2020 года: настоящая армия роботов из сотен тысяч взломанных серверов по всему миру круглосуточно проверяет каждый (!) IP-адрес и старается взломать то устройство, которое за ним спрятано.

Тысячи камер видеонаблюдения — взломаны.

Сотни тысяч серверов — взломаны, добывают криптовалюту и взламывают соседей.

Миллионы компьютеров — взломаны и заражены программами-вымогателями.

Ради эксперимента мы арендовали сервер и оставили его в сети с несложным паролем — через 15 минут на нём было зарегистрировано более 20 успешных входов из нескольких стран, а ещё через полчаса на нём появился криптомайнер.

Лишь 44,3% опрошенных компаний серьёзно подошли к вопросу архивации электронной почты и документов, и только 23,9% действительно управляют паролями и защищают учётные записи системных администраторов.

Другими словами, с вероятностью более 50% вы в числе компаний, чьи методы защиты обойдут, а письма и документы безвозвратно уничтожат.

## УПРАВЛЯЙТЕ ПАРОЛЯМИ ПРАВИЛЬНО!

Если у вас «угнали» учётную запись администратора, вы заметите это очень нескоро: взломщик «закрепится» в вашей сети, создаст для себя дополнительные входы, учётные записи, поправит политики, найдёт и усыпит бдительность систем защиты, а затем будет тащить ваши документы, удалять важные письма, раскрывать



*Даже если взломщик подберёт пароль, он всё равно не получит всех прав, его действия будут записаны, а через некоторое время пароль будет изменён*

пароли остальных сотрудников, и об этом вы узнаете только через полгода-год.

**Хакеры продолжают иметь доступ к взломанным устройствам более 206 дней, прежде чем их заметят<sup>2</sup>**

«Что же делать?» — не спросите вы, а зря!

За последние пять лет на рынке появились простые в использовании программы, которые умеют управлять учетными записями администраторов и паролями от устройств так, что даже если взломщик подберёт пароль, он всё равно не получит всех прав, его действия будут записаны, а через некоторое время пароль будет изменён.

Речь идёт о программах **Thycotic: Secret Server** и **Privilege Manager**. Эти решения позволяют хранить пароли в зашифрованном хранилище, распределять доступы в соответствии с должностями сотрудников, вести аудит подключений к серверам и устройствам с видеозаписью, а также менять пароли по расписанию с учётом сложных взаимосвязей между серверными приложениями — когда у вас несколько администраторов, зоопарк из десятков различных систем и сотни локальных и доменных учетных записей, такая система просто необходима!

Администратор подключается к серверам и сетевым устройствам из списка разрешённых через удобный интерфейс, при этом Thycotic Secret Server скрывает от него пароль, который используется для подключения, предоставляя лишь одноразовую защищённую сессию, записывает факт подключения и разрешает запускать только те приложения, которые необходимы для работы.

Таким образом, внешний или внутренний нарушитель не получит не-

ограниченного доступа, не узнает паролей в чистом виде, а все его действия будут записаны и отправлены в SIEM-систему или **Thycotic Privileged Behavior Analytics** для автоматической аналитики.

Чтобы снизить риски, в продукт добавлена двухфакторная аутентификация: для входа в систему администратору потребуется ввести одноразовый код, который генерируется на его мобильном телефоне или ином устройстве, — взломщику придётся украсть и его.

Для внешних подрядчиков и службы технической поддержки можно выдавать одноразовые пароли с ограниченным сроком действия по заявкам, причём доступ будет ограничен не только списком серверов, но и перечнем приложений и команд, которые разрешено выполнять.

При увольнении или найме сотрудника Thycotic Secret Server позволяет отозвать или выдать доступы до систем в соответствии с любым процессом, который заведён в вашей компании: например, можно сделать так, что доступ будет выдаваться только с разрешения всех руководителей.

**Все подключения и действия записываются — выявить нарушителя и провести расследование становится значительно проще<sup>3</sup>**

Описанные функции доступны не только людям, но и программам: получать актуальные пароли, участвовать в процессе их смены и попадать в отчёты могут сканеры уязвимостей, клиенты баз данных, системы CRM и ERP и даже приложения, которые разработали вы сами, — для этого Thycotic предоставляет мощный программный интерфейс (API).

Соответствуйте стандартам SOX, PCI DSS, HIPAA, Basel II и MASS 201/

CMR/17 с Thycotic без лишних усилий. Это полезно не только крупным компаниям, банкам и медицинским учреждениям, но и любой организации, заботящейся о грамотном обеспечении безопасности сети.

Продукт устанавливается и настраивается со всеми подготовками для полноценного использования всего за несколько часов. Загрузить можно уже сейчас на веб-сайте: [www.Thycotic.ru](http://www.Thycotic.ru)

Перед установкой вы можете проконсультироваться со специалистами: [info@thycotic.ru](mailto:info@thycotic.ru), +7 495 223 35 33 (Москва), 8 800 550 52 23 (бесплатно по РФ).

## **АРХИВАЦИЯ ПОЧТЫ. ПОИСК И РАССЛЕДОВАНИЯ**

**Один из основных каналов утечки информации — электронная почта<sup>4</sup>**

Электронная почта — это и основной метод обмена информации, и историческое хранилище большинства передаваемых документов, требований и отчетов аудиторов, и популярный канал утечки информации, и важнейший инструмент расследования инцидентов.

Не архивируете электронную почту — **потеряете письма.**

Архивируете средствами почтового сервера — **погубите сервер и потеряете письма.**

Архивируете резервным копированием сервера — **потеряете письма с даты последней копии.**

Проблема архивации электронных писем становится еще актуальнее, если у вас больше одного почтового сервера, будь то резервные, дополнительные, почтовые сервера в филиалах или поглощенных компаниях.

**Актуальные стандарты безопасности: «электронная почта должна архивироваться»<sup>5</sup>**

«Должны быть определены, выполняться, регистрироваться и контролироваться правила и процедуры досту-



на к информации архива и ее изменения, предусматривающие возможность доступа работников службы ИБ к информации архива», — разумно дополняет СТО БР ИББС.

Читатель, знакомый с функциями популярных почтовых серверов, догадается, что стандартными средствами эту задачу не решить даже «для галочки», не говоря уже о разумном подходе для снижения рисков, уменьшения стоимости последствий и обеспечении себя инструментами для выявления утечек и нарушителей.

Но не стоит отчаиваться, даже если у вас 20 почтовых серверов, 30 ТБ электронной почты, требуется централизованная архивация, дублирование в два дата-центра и сохранение возможности поиска по всему архиву любых цепочек писем, включая поиск по тексту прикрепленных документов и изображений — на рынке уже 15 лет существует решение MailArchiva EE, которое умеет все перечисленное.

Вся разработка MailArchiva ведется в России, но сам продукт изначально был ориентирован на зарубежный рынок, где насчитывается более 7 000 установок. Крупнейшая установка MailArchiva EE включает более 500 000 почтовых ящиков с хранилищем в 2 петабайта (2 000 000 ГБ) писем. На январь 2020 года идет реорганизации компании для добавления продукта в реестр отечественного ПО.

На территории России MailArchiva EE используют такие компании, как ФК «Открытие», Ярославский шинный завод, входящий в холдинг «Кордиант», ВТБ24, Кит Финанс, Связной и другие организации схожего объема. Всем клиентам MailArchiva EE успешно помогает соответствовать Sarbanes Oxley Act, Gramm-Leach Bliley Act, Basel II, СТО БР ИББС в части защиты электронной почты и проведения расследований на базе электронной почты.

*Найти любую цепочку писем можно по десятку различных параметров, включая ключевые слова из приложенных файлов (поддерживается 100 различных форматов), причем тексты для поиска распознаются даже в изображениях и PDF-документах*

Пользоваться MailArchiva EE действительно удобно: найти любую цепочку писем можно по десятку различных параметров, включая ключевые слова из приложенных файлов (поддерживается 100 различных форматов), причем тексты для поиска распознаются даже в изображениях и PDF-документах, а «собирать» поисковый запрос можно удобным конструктором. На выходе вы получите граф связей между отправителями и получателями среди найденных писем, а также сможете подписаться на периодические отчеты о новых результатах.

Часть клиентов используют MailArchiva EE, как незаменимого помощника для решений DLP, которые не справляются с большим потоком писем: система DLP подключается к архиву через специальный программный интерфейс и просматривает письма в удобном для себя режиме, не мешая почтовому потоку.

Приятным эффектом станет ускорение ваших почтовых серверов за счет удаления старых писем и тяжелых встроенных архивов — оставьте почтовому серверу только его основные функции, ради которых он у вас работает.

В отличие от похожих решений, для MailArchiva EE не требуется покупать дорогостоящую лицензию на СУБД, а для хранения можно использовать существующие локальные сетевые и облачные хранилища, причем архив будет храниться в зашифрованном виде.

Теперь, если у кого-нибудь все-таки получится вас взломать, украсть одноразовый пароль администратора, незаметно обойти все эшелоны защиты, воспользоваться Oday для повышения привилегий на атакуемой системе, а затем уничтожить всю вашу почту — вы вернете все утраченные письма за любой период до самого последнего письма.

**Начните использовать MailArchiva EE уже сегодня!** Удобный инструмент поможет импортировать в архив всю накопленную переписку и получить выгоду от архивации писем с первых же дней работы. Все письма хранятся в зашифрованном виде.

Узнать больше, заказать демонстрацию и получить копию можно на веб-сайте: [www.MailArchiva.ru](http://www.MailArchiva.ru)

Перед установкой вы можете проконсультироваться со специалистами: info@afi-d.ru, +7 495 223 35 33 (Москва), 8 800 550 52 23 (бесплатно по РФ).

## ССЫЛКИ

1. По данным отчета «Data Breach Investigations» от Verizon.
2. По данным отчета «Cost of a Data Breach Report» от IBM.
3. Из описания функций Thycotic Secret Server на сайте производителя.
4. По данным исследований Device-Lock и отчета SecurIT.
5. Из требований и рекомендаций Basel II, СТО БР ИББС-1.0–2014, Sarbanes Oxley Act, Gramm-Leach Bliley Act, Guidelines on Electronic Mail Security (NIST).

## ООО «АФИ ДИСТРИБЬЮШН»

Российская компания-дистрибьютор решений Aventri, Altaro, GFI, MailArchiva и Thycotic. Компания оказывает консультации, техническую поддержку, предлагает бесплатную демонстрацию решений на русском языке, помогает в подборе решений, а также проводит обучение компаний-интеграторов и специалистов-заказчиков.



# ПЕРСПЕКТИВА ДЛЯ ПРИЗВАНИЯ

ИНСТИТУТУ КРИПТОГРАФИИ, СВЯЗИ И ИНФОРМАТИКИ  
(ИКСИ) ИСПОЛНИЛОСЬ 70 ЛЕТ



**Дмитрий ЛАРИН**  
историк криптографии,  
кандидат технических наук





**С**вою историю институт криптографии, связи и информатики (ИКСИ) ведёт от Высшей школы криптографов, созданной 19 октября 1949 года решением Политбюро ЦК ВКП(б) и образованного в том же году закрытого отделения механико-математического факультета Московского государственного университета им. М.В. Ломоносова. В дальнейшем эти учебные заведения были реорганизованы в технический факультет Высшей школы КГБ СССР им. Ф.Э. Дзержинского. В 1992 году технический факультет был преобразован в ИКСИ.

### ИКСИ СЕГОДНЯ

Сегодня Институт криптографии, связи и информатики Академии ФСБ России — это многопрофильное образовательное учреждение, имеющее высокий авторитет среди силовых структур, гражданских вузов и научной общест-венности.

Он является главным учебным заведением России по образованию в области информационной безопасности. На базе ИКСИ создано Федеральное учебно-методическое объединение в сфере высшего образования по УГСН «Информационная безопасность» (УМО ИБ), включающее более двухсот ведущих средних и высших учебных заведений по всей России.

На четырёх факультетах, включающих 11 кафедр, института ведётся подготовка специалистов по 6 специальностям высшего образования.

Все учебные программы рассчитаны на пять лет обучения. По всем специальностям выпускникам присваивается квалификация «Специалист по защите информации».

Слушатели ИКСИ, кроме специальных технических дисциплин, получают хорошую гуманитарную и военную подготовку. В стенах института существуют прекрасные возможности для углублённого изучения иностранных языков. В специально оборудованных классах под руководством опытных преподавателей они осваивают тонкости современной военной науки, огневой подготовки и боевого мастерства.

### ПРОФЕССОРСКО-ПРЕПОДАВАТЕЛЬСКИЙ СОСТАВ

В ИКСИ трудится более 200 человек профессорско-преподавательского состава (ППС). Среди них более 150 докторов и кандидатов наук, академиков и членов-корреспондентов различных академий. Все они — квалифицированные педагоги и известные учёные. В институте преподают лауреаты государственных премий, кавалеры высоких правительственных наград. Для проведения занятий активно привлекаются лучшие специалисты научно-исследовательских институтов и оперативно-технических подразделений ФСБ России, иных министерств и ведомств, а также ведущих российских вузов: МГУ, МИФИ, МФТИ, МГТУ, МИРЭА и др.

ППС ИКСИ проводит большую учебно-методическую и научно-исследовательскую работу. Учебники, монографии, учебные пособия, курсы лекций, разработанные по каждой из реализуемых специальностей, удовлетворяют самым современным требованиям Федеральных государственных образовательных стандартов.

Институт сохраняет и развивает лучшие традиции Высшей школы криптографов и специального отделения механико-математического факультета МГУ им. М.В. Ломоносова, достойным преемником которых он является. Эта преемственность заключается в глубокой специальной подготовке, ориентированной на решение сложнейших задач, стоящих перед практическими подразделениями, в интересах которых ведётся подготовка специалистов.

В основе образования, получаемого слушателями ИКСИ, лежат высочайшие достижения фундаментальных областей науки. Среди них математика, физика, программирование, кибернетика, радио- и микроэлектроника, теория связи и информации, нанотехнологии. Качество, полученного в ИКСИ образования, соответствует уровню наиболее авторитетных университетов страны.

### МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ ОСНАЩЁННОСТЬ

В связи с глобальным развитием информационных технологий институт уделяет большое внимание формированию умений и навыков работы с различными видами современной вычислительной техники. Разнообразный парк компьютеров института включает большое число персональных ЭВМ, рабочих станций и серверов известных производителей. Современная материально-техническая база компьютерных классов, новейшее программное обеспечение позволяют изучать самые сложные аспекты использования вычислительных средств, проблемы построения и защиты вычислительных сетей и компьютерной безопасности, защиты от компьютерных вирусов.

Выработке практических навыков по естественно-научным и специальным дисциплинам способствует развитая ла-

| Факультет                   | Специальность                                                                      |
|-----------------------------|------------------------------------------------------------------------------------|
| прикладной математики       | Криптография<br>Информационно-аналитические системы безопасности                   |
| специальной техники         | Информационная безопасность телекоммуникационных систем                            |
| информационной безопасности | Компьютерная безопасность<br>Информационная безопасность автоматизированных систем |
| оперативно-технический      | Противодействие техническим разведкам                                              |





Награждение победителей и призёров Межрегиональной олимпиады школьников им. И. Я. Верченко по математике и криптографии

бораторная база института. Занятия по физике, радиотехническим и специальным дисциплинам проводятся в аудиториях, оборудованных современными уникальными приборами и специальной техникой.

### НАУЧНО-ИССЛЕДОВАТЕЛЬСКАЯ ДЕЯТЕЛЬНОСТЬ

ППС привлекает слушателей способностью к самостоятельным научным исследованиям. Это является приоритетным направлением и неотъемлемой частью работы института.

Слушатели приобретают навыки научного мышления в ходе подготовки курсовых и дипломных работ, ведут внеплановые научные разработки. Наиболее интересные результаты публикуются в авторитетных общероссийских и ведомственных научных изданиях. Слушатели, проявившие способности к научно-исследовательской работе, получают возможность продолжить образование в адъюнктуре Академии. Большинство выпускников института в дальнейшем продолжает научные исследования, начатые в вузе. Ежегодно представители ИКСИ входят в число лауреатов и дипломан-

тов Всероссийского конкурса студентов на лучшую научно-исследовательскую работу.

Кроме того, в институте создан и поддержан грантами Президента РФ ряд научных школ (по математическому и радиотехническому направлениям). Научные исследования ряда молодых учёных института поддерживаются президентскими персональными грантами.

Работа выпускников ИКСИ имеет исключительно важное значение для обеспечения безопасности государства. По окончании института выпускникам гарантировано распределение на работу в технические и научные подразделения ФСБ России, иные министерства и ведомства, обеспечивающие безопасность страны. Высокий уровень и актуальность знаний, умений и навыков, получаемых в ходе обучения, позволяют им включаться в рабочий процесс, минуя период первоначальной адаптации. Именно выпускники ИКСИ составляют основной костяк кадрового состава большинства практических подразделений соответствующего профиля. Многие из них награждены высокими правительственными наградами, стали ведущими специалистами и крупными руководителями.

### ДОВУЗОВСКАЯ ПОДГОТОВКА

В течение многих лет в ИКСИ реализуется программа «Абитуриент».

В рамках этой программы каждый год на базе вуза проводятся:

- ♦ письменные контрольные работы по математике и физике;
- ♦ Межрегиональная олимпиада школьников им. И. Я. Верченко по математике и криптографии;
- ♦ межрегиональные олимпиады школьников по физике и математике на базе ведомственных образовательных учреждений;
- ♦ олимпиада «Информатика и компьютерная безопасность».

ИКСИ приглашает всех заинтересованных потенциальных абитуриентов проверить свои знания, оценить уровень подготовки и, пройдя вступительные испытания, получить профильное образование в вузе, имеющем многолетние традиции в области подготовки специалистов для органов безопасности РФ.

### ДИСТАНЦИОННОЕ ОБУЧЕНИЕ

На сайте олимпиад [www.v-olymp.ru](http://www.v-olymp.ru) развёрнута общедоступная система дистанционного обучения (СДО). В СДО организованы курсы абитуриентов технических вузов для помощи в самостоятельной подготовке к сдаче ЕГЭ и дополнительных вступительных испытаний, а также участию в олимпиадах.

В online-режиме школьники со всей России могут получить квалифицированные консультации по решению задач и тематике олимпиады. Работа в СДО удобна пользователю, для прохождения обучения достаточно заходить в систему один-два раза в неделю. Изучение теоретической части и решение тестов в каждом выбранном курсе занимает около 40–50 минут.

### ЛИТЕРАТУРА

1. Зубов А. Ю., Зязин А. В., Никонов Н. В., Рамоданов С. М., Фролов А. А. Олимпиады по криптографии и математике. М.: МЦНМО, 2013.
2. [academy.fsb.ru](http://academy.fsb.ru)
3. [v-olymp.ru](http://v-olymp.ru)



13–14 МАЯ 2020

# POSITIVE HACK DAYS 10: НАЧАЛО

**Это случится снова:** крупнейший форум по практической кибербезопасности Positive Hack Days в десятый раз соберет на одной площадке энтузиастов и звезд из мира ИТ и ИБ.

Два дня докладов, горячих дискуссий, мастер-классов от ведущих экспертов в сфере исследования безопасности и конкурсов по анализу защищенности систем и технологий уже ждут своих посетителей.

Грандиозная битва red teams и blue teams — The Standoff — вновь развернется на площадке виртуального города в рамках практического соревнования по взлому и защите его инфраструктуры.

Только здесь собираются белые хакеры и ИБ-специалисты крупнейших компаний со всей планеты, представители интернет-сообщества и госструктур, регулирующих организаций, политик, деятели науки и искусства — чтобы вместе формировать благополучное цифровое будущее. Присоединяйтесь и вы!

**БИЛЕТЫ УЖЕ В ПРОДАЖЕ**

Открыта регистрация СМИ.

E-mail для заявок: [zbezzabotnova@ptsecurity.com](mailto:zbezzabotnova@ptsecurity.com)



# АВАНГАРД

## медиа группа



Организация  
мероприятий



Отраслевой  
журнал



Интернет-  
телекомпания



Образование  
и карьера

[ib-bank.ru](http://ib-bank.ru)