

22> Ольга СКОРОБОГОВА
(Банк России)
Думать на стадии проектирования



30> Дмитрий СКОБЕЛКИН
(Банк России)
2018 год. Точки отсчёта

40> Иван ЯНСОН
(ПАО Сбербанк)
В пять кликов. Испытание уникального сервиса



82> Игорь ЛЕГЕЗИН
(Диасофт)
Бизнес-процессы под прицелом

121> Борис СТОЛПАКОВ
(историк криптографии)
Екатеринбургская трагедия: шифрованные телеграммы

ЦИФРОВАЯ ЭКОНОМИКА: СКАЧОК ЭВОЛЮЦИИ



VII симпозиум «Современные тенденции в криптографии»

Тематика симпозиума включает, но не ограничена следующими направлениями:

- исследование криптографических алгоритмов, в том числе анализ криптографических алгоритмов и протоколов, являющихся международными стандартами;
- эффективная реализация методов анализа криптографических алгоритмов и протоколов;
- оценка криптографической стойкости российских криптографических алгоритмов и протоколов;
- эффективная реализация российских криптографических алгоритмов и протоколов;
- перспективные направления в криптографии, в т. ч. квантовая криптография, постквантовые криптографические алгоритмы, протоколы консенсуса в распределенных реестрах.

ОРГАНИЗАТОРЫ



Академия
криптографии РФ



Технический комитет
«Криптографическая защита информации»



Математический институт
им. В.А. Стеклова РАН

ГЕНЕРАЛЬНЫЙ ПАРТНЕР



ОФИЦИАЛЬНЫЙ ПАРТНЕР



ПАРТНЕР ВЫСТАВКИ



ОРГПОДДЕРЖКА





Игорь НЕКРАСОВ
главный редактор
BIS Journal

Картинка на обложке не так проста, как кажется. Да, мы живем именно в тот краткий исторический миг, когда эволюция совершает свой скачок от человека разумного (в галстуке) к человеку цифровому (летит, открывает новый мир). Собственно, картинка фиксирует свершившийся факт: поколение Z, не знающее мира без интернета, уже живет — думает и действует в условиях перехода в цифровую вселенную. О непростом характере этих детей как раз и говорится в нашем номере — на круглом столе, посвященном проблеме кадров в сфере ИБ (рубрика «Образование и карьера»).

И все же эта картинка, да и весь номер BIS Journal, — не о них, летящих, а о нас — еще только бодро разбегающихся перед прыжком. О текущем моменте, о том, станет ли программа «Цифровая экономика РФ» порталом в новую вселенную. Поможет ли она стране и детям спокойно, с достоинством освоить новые цифровые миры? Или масштаб начатых преобразований, как бывало не раз, схлопнется до наномасштаба? В этом смысле полезно узнать мнения первых лиц государства и цифровых отраслей, заявивших себя лидерами диджитализации на последних парламентских слушаниях, посвященных цифровой экономике. И конечно, «Сарынь на кичку!» Натальи Касперской, разрушившее ровный гул лидеров, и прозвучавшее как тревожный народный набат. Ее выступление мы вполне осознанно публикуем в полном объеме (рубрика «Цифровая экономика: старт дан!»).

Но и вопрос строительства порталов в иные миры занимает в номере не так много места. Гораздо больше в нем о делах насущных, тех, что идут своим чередом: регуляторы регулируют, безопасники защищают... Новые нормы, стандарты, законы... Фишинг, удаленный доступ, искусственный интеллект... Интересны эксперименты Сбербанка и Ростелекома в области аутентификации... Слегка пафосны, но любопытны репортажи с форумов: Уральского, Инфофорума, Cyber Security-2018, ТБ-Форума...

Ну, и знакомые всем лица, наши любимые авторы. Фарит Музипов рассказывает, как искал работу после краха своего большого банка. Очень поучительно, хотя и весьма завуалировано. Марина Бродская выяснила, как заработать в нашем отечестве на ловле блох, то есть тестировании ПО. Оказывается, в плане мероприятий по ИБ программы «Цифровая экономика» на это дело предусмотрено 800 млн руб. А Александр Бодрик, как всегда, зрит в корень, и беспощадным анализом рисует некоторым безопасникам тревожное будущее. Его заметки так и называются: «Кому сушить сухари?»

Похоже, он прав и в результате тотальной диджитализации не всем предстоит взлететь. Пути эволюции неисповедимы. Но главное, третий человек на картинке (с дубиной) выглядит наиболее символично: подозрительно и непредсказуемо. Это — злоумышленник.

Так что будь внимателен, безопасник. Бди!

ОБЩЕСТВЕННЫЙ РЕДАКЦИОННЫЙ СОВЕТ

Емельянов Г.В. — член-корреспондент Академии криптографии РФ, действительный государственный советник РФ 3 класса

Сычев А.М. — заместитель начальника Главного управления безопасности и защиты информации Банка России, кандидат технических наук, доцент

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

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

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

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

Виноградов А.Ю. — начальник управления

информационной безопасности АО КБ «Златкомбанк»

Вихорев С.В. — заместитель руководителя направления

информационной безопасности НТЦ «Вулкан»

Дзержинский Ф.Я. — главный эксперт — координатор

системной экспертизы блока «информационные

технологии» ООО «ТехноСофт», CSDP

Зубков А.Н. — генеральный директор ООО «Медиа

Группа „Авангард“, директор Фонда содействия развитию

безопасных информационных технологий (ФСРБИТ)

Курило А.П. — заместитель генерального директора

компании «РНТ», кандидат технических наук

Левинов Д.О. — председатель Совета НП «Партнерство

специалистов по информационной безопасности»

Мельников С.Ю. — заместитель генерального директора

ООО «Лингвистические и информационные технологии»,

кандидат физико-математических наук

Некрасов И.В. — главный редактор журнала

Окулесский В.А. — руководитель департамента

ООО «ЦИБИТ», кандидат технических наук

Пазизин С.В. — начальник Управления по обеспечению

информационной безопасности ОАО Банк ВТБ, кандидат

физико-математических наук

Шумский Л.С. — руководитель направления ИБ

АО «Альфа-Банк»

Янсон И.А. — бизнес-партнер по информационной

безопасности, Департамент безопасности ПАО «Сбербанк

России», кандидат физико-математических наук

ЭКСПЕРТНАЯ ГРУППА

Одувалов М.В. — эксперт BIS Journal

Филипчук А.А. — технический директор ГК ЦРТ

Калашникова Е.В. — Банк ВТБ (ПАО)

РЕДАКЦИЯ ЖУРНАЛА

Главный редактор: **Некрасов И.В.**

Шеф-редактор: **Былевский П.Г.**

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

Арт-директор: **Мельников Н.С.**

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

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

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

Фото в номере: фотобанк DepositPhotos, **Виталий Вилкин**

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

Цветокорректор: **Наumenko М.Б.**

Корректор: **Бальтерманц Л.Ф.**

УЧРЕДИТЕЛЬ-ИЗДАТЕЛЬ

ООО «Медиа Группа „Авангард“»

Адрес: 127473, Россия, Москва, 3-й Самотечный переулок,

д.21 (м. «Достоевская»)

Координаты: 55.779380, 37.61150

Тел./факс: +7 499 271-70-85

Интернет-версия: journalib-bank.ru

E-mail: bis@ib-bank.ru

Отдел рекламы: reklama@ib-bank.ru

Отдел распространения: tirazh@ib-bank.ru

Зарегистрирован 13 августа 2010 года Федеральной

службой по надзору в сфере связи, информационных

технологий и массовых коммуникаций (Роскомнадзор).

Свидетельство ПИ № ФС77-55062 от 14 августа 2013 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 6.04.2018. Тираж 7000 экз.

Заказ № 236351. Цена договорная.

Отпечатан в «Типографии на Угрешской»

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

Тел.+7 495 720-62-28

© BIS Journal, 2018



НОВОСТИ

5 В мире, криминал, в России

ТЕМА НОМЕРА

- 8** **Цифровая экономика: старт дан!**
Немыслима без безопасности.
Репортаж из парламента
- 16** **Цифровая экономика: старт дан!**
Наталья КАСПЕРСКАЯ (ГК InfoWatch)
Риски цифровой колонизации

РЕГУЛЯТОРЫ

- 22** **Цифровая экономика**
Ольга СКОРОБОГАТОВА (Банк России)
Думать на стадии проектирования
- 30** **Стратегия**
Дмитрий СКОБЕЛКИН (Банк России)
Точки отсчета
- 35** **Стандартизация**
Александр БОНДАРЕНКО (ТК 26)
Запас прочности

БАНКИ

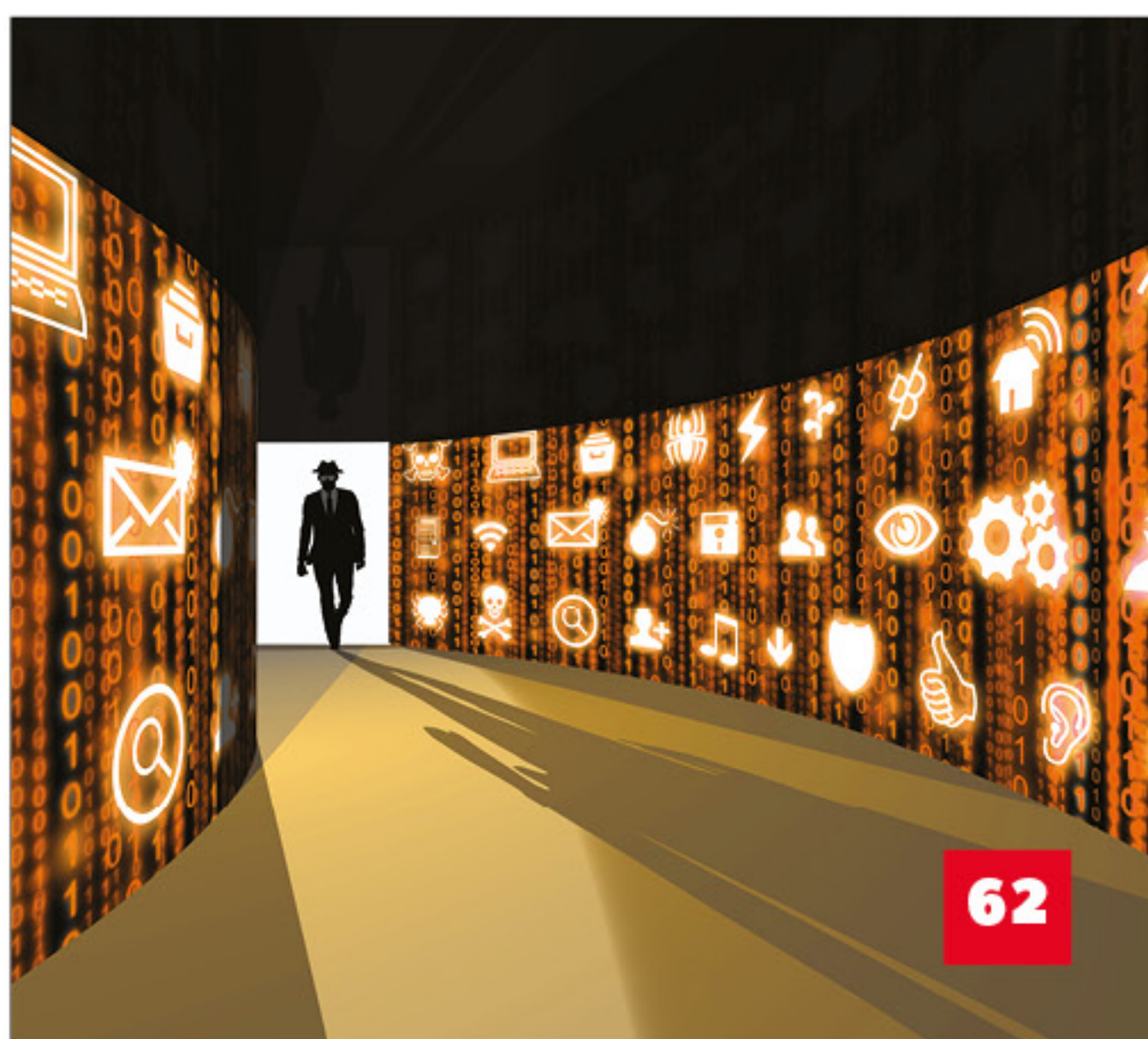
- 40** **Эксперимент**
Иван ЯНСОН (ПАО «Сбербанк»)
В пять кликов
- 46** **Идентификация**
Иван БЕРОВ (ПАО «Ростелеком»)
Селфи вместе с паролем
- 50** **Идентификация**
Александр БРОДСКИЙ (ПАО «Сбербанк»)
Риск-ориентированная аутентификация
- 54** **SWIFT**
Матвей ГЕРИНГ (SWIFT)
Программа безопасности пользователей SWIFT





УГРОЗЫ И РЕШЕНИЯ

- 58 Законодательство**
Антон СВИНЦИЦКИЙ, Игорь ТАРВИ
(АО «ДиалогНаука»)
БанКИИ
- 60 Искусственный интеллект**
Андрей ФИЛАТОВ (IBM)
Один в поле не воин
- 62 SecBigData**
Михаил САВЕЛЬЕВ (Информзащита)
Сколько стоит кибер-разведка?
- 64 Интеграция**
Алина СИДОРОВА (АМТ-ГРУП)
Централизованный удаленный доступ без проблем
- 68 Аутентификация**
Андрей КОНУСОВ (Аванпост)
На смену SSO
- 70 Медицина**
Александр ПОГРЕБНОЙ, Татьяна СТАНКЕВИЧ (ООО «Газинформсервис»)
Перелом в области защиты информации медицинской отрасли
- 73 Фишинг**
Сергей СТОРЧАК (ПАО «Тагмет»)
Красные метки в черных списках
- 76 Облачные сервисы**
Константин ЧУМАЧЕНКО (NGENIX)
DDoS-атаку остановит облако
- 78 Open source**
Дарья ОРЕШКИНА (WEB Control)
В защиту open source компонентов
- 82 Программное обеспечение**
Игорь ЛЕГЕЗИН (Диасофт)
Бизнес-процессы под прицелом



ИНФРАСТРУКТУРА

86 Деловые мероприятия
Алексей ЛУКАЦКИЙ (эксперт ИБ)
Уральский форум за 15 минут

92 Деловые мероприятия
Марк НОВОДАЧНЫЙ (BIS Journal)
ИНФОФОРУМ 2018

94 Деловые мероприятия
Николай КОЛЬСКИЙ (BIS Journal)
Cyber Security Forum 2018

96 Деловые мероприятия
Корней РЕУТ (BIS Journal)
ТБ Форум 2018

99 Деловые мероприятия
Николай КОЛЬСКИЙ (BIS Journal)
International Open Data Day



ОБРАЗОВАНИЕ И КАРЬЕРА

102 Круглый стол
Кадры решают все

108 HeadHunter
Александр БОДРИК (ANGARA Professional Assistance), **Фарит МУЗИПОВ** (АО «РЭЦ»)
На перепутье

110 Персонал
Игорь ДОЛОТИН (UBS)
Как повысить?

112 Обзор
Марина БРОДСКАЯ (BIS Journal)
Ловля блох за деньги

СУБЪЕКТЫ

115 История
Дмитрий ЛАРИН (ЗАО «Лаборатория „СКАТ“»)
Периодизация криптографической деятельности в России

121 История
Борис СТОЛПАКОВ (историк криптографии)
«Мир никогда не узнает, что мы сделали с ними»

126 Корифеи
Дмитрий ЛАРИН (ЗАО «Лаборатория „СКАТ“»), **Геннадий ЕМЕЛЬЯНОВ** (Академия криптографии РФ)
Советский криптограф Иван Верченко

128 Мысли вслух
Александр БОДРИК (ANGARA Professional Assistance)
Кому сушить сухари?

ПЛАНЕТУ ТЕРРОРИЗИРУЮТ ПЯТЬ ПРЕСТУПНЫХ ГРУПП

Согласно докладу компания Dragos, специализирующейся на промышленной кибербезопасности, существует, по меньшей мере, пять преступных групп, деятельность которых сосредоточена вокруг АСУ ТП.

Специалисты Dragos отслеживают группировки, которые либо атакуют АСУ ТП напрямую, либо проявляют интерес к сбору информации об этом типе систем. Например, группа Electrum стояла за деятельностью

вредоноса CrashOverRide/Industroyer, который использовался в декабре 2016 года в кибератаках, вызвавших перебои в подаче электроэнергии в Украине.

Electrum также связана с группой Sandworm Team, которая, как предполагают эксперты, ответственна за перебои в подаче электроэнергии в Украине в 2015 году. Специалисты убеждены, что Electrum продолжает оставаться активной, есть данные о том, что она расширила список своих целей.

Еще одна группа получила имя Covellite. Она связана с северокорейскими киберпреступниками Lazarus. В сентябре 2017 года злоумышленники провели широкомасштабную фишинговую кампанию против американской электросетевой компании. Позднее выяснилось, что киберпреступники Covellite также ответственны за покушения на организации в Европе, Северной Америке и Восточной Азии.



ПРЕЗИДЕНТА ВЫБРАЛИ С ПОМОЩЬЮ БЛОКЧЕЙНА

7 марта в Сьерра-Леоне впервые в мире выборы президента прошли с использованием технологии блокчейн. Подсчет результатов доверили стартапу Agoa.

С точки зрения избирателей процесс голосования ничем не отличался от обычных выборов. Затем результаты были занесены в компьютер вручную с помощью контролируемой технологии блокчейн.

В отличие от технологии блокчейн с открытым доступом, применяемой, например, при осуществлении операций с криптовалютой, блокчейном с контролируемым доступом могут пользоваться только уполномоченные лица. При выборах в Сьерра-Леоне такими лицами были представители компании Agoa, Красного Креста, Федеральной политехнической школы Лозанны и Фрайбургского университета.



Тем не менее, как с открытым доступом, так и в контролируемом блокчейне любой человек может посмотреть записанные операции. Это значит, что результаты голосования в Сьерра-Леоне после проверки компаниями по контролю за блокчейном, стали доступны всем.

Ранее в ходе президентских выборов в Сьерра-Леоне не раз случались беспорядки. Поэтому именно эта страна с высоким уровнем коррупции была выбрана для испытания новой технологии, призванной обеспечить честные выборы.

В ИСЛАНДИИ ПОХИТИЛИ 600 СЕРВЕРОВ

В Исландии из дата-центров похитили 600 серверов. Местная полиция назвала эту кражу одной из самых крупных в истории страны.

Четыре налета на ЦОДы произошли в декабре 2017 года и январе 2018-го. Ущерб от кражи оценивается в \$2 млн. Хотя 11 подозреваемых, включая охранника одного из ЦОДов, были арестованы, вернуть технику не удалось.

Полиция попросила энергетические компании и интернет-сервисы обратить внимание на необычные случаи использования энергии, причиной которых может стать работа похищенных серверов. По мнению следствия, их украли для добычи криптовалют.

В 2018 году объем электричества, используемого устройствами для майнинга криптовалют, впервые превысил количество энергии, потребляемой во всех жилых помещениях Исландии (население 348 тыс. человек).

ЦУКЕРБЕРГ БЬЁТ ТРЕВОГУ

Марк Цукерберг уверен, что «кто-то снова попытается» использовать Facebook для вмешательства в выборы в США.

«Я уверен, будет очередная версия того, что произошло в 2016 году... Но будет использована новая тактика», — заявил Цукерберг.

Ранее Цукерберг потерял \$6 млрд из-за снижения курса акций Facebook почти на 7%. Это произошло в результате действий британской аналитической компании Cambridge Analytica, которая работала над кампанией президента США Дональда Трампа. Организация собрала личные данные 50 млн пользователей Facebook и разработала алгоритм анализа их политических предпочтений.

Как пояснил Цукерберг, Cambridge Analytica обнаружила уязвимость в защите соцсети и некорректно воспользовалась личными данными пользователей.

ВОЛНА DDOS-АТАК

По Европе прокатилась волна memcache амплифицированных DDOS-атак.

Техника такой атаки — в прослушивании злоумышленниками UDP-трафика при условии установки параметров memcache по умолчанию. То есть фактически используется UDP-флуд — отправка множества поддельных UDP-пакетов в единицу времени от широкого диапазона IP-адресов.

Проблемы с безопасностью memcache известны как минимум с 2014 года, однако в 2018 году эта уязвимость проявилась особенно ярко: в ночь с 25 на 26 февраля специалисты Qrator Labs наблюдали такие атаки по всему интернету, включая атаки на крупнейшие в России сетевые ресурсы.

В конце марта были зафиксированы такие же атаки с вкраплениями ответов от DNS и NTP. Их источниками стали крупный провайдер OVH и множество меньших провайдеров и хостеров.

СДАЕТСЯ В АРЕНДУ... ВИРУС-ВЫМОГАТЕЛЬ

Уже через два дня после официального релиза массового сервиса-вымогателя Data Keeper в даркнете в Сети были зарегистрированы доказательства его эффективности.

Новое вредоносное ПО шифрует файлы на компьютерах жертв и требует выкуп в криптовалюте. Этот заражающий сервис выдает доступ к его коду по запросу и является разновидностью RaaS (Ransomware-as-a-Service — «вымогательство как услуга»). По мнению специалистов, файлы шифруются с помощью двойного алгоритма AES и RSA-4096. Data Keeper также вычисляет и пытается зашифровать все общие сети, к которым может получить доступ. При этом новая разновидность вируса не добавляет специальное расширение в зашифрованные документы, что лишает жертв возможности понять, какие файлы поражены.

Также зафиксирована новая, напоминающая аренду, форма эксплу-

атации и распространения сервиса-вымогателя. Любой желающий, зарегистрировавшись на специальном портале, может присоединиться к киберпреступникам и заниматься цифровым рэкетом, достаточно лишь делиться полученной добычей с разработчиками.



XI Межотраслевой Форум CISO FORUM 2020: взгляд в будущее

23–24 апреля 2018 г. · Москва



- 400+ участников
- 70+ спикеров; 80% — CISO, которые уже успешно защищают свои компании
- ТОП 10 кейсов от ТОП 10 CISO
- 3 параллельных потока: выбирайте темы, интересные именно вам!
- 2+ интервью на сцене с трендсетерами
- 3+ круглых стола — знакомься, общайся, обменивайся опытом
- 4+ уникальных мастер-классов: полное погружение в реальность бытия безопасника
- 30+ практических кейсов
- Вечерняя fuck up party — для закрепления дружбы участников

Больше информации на сайте www.infosecurity-forum.ru
и у Елены Проненко по тел.: +7 495 995-80-04, доб. 1272, или по e-mail: e.pronenko@infor-media.ru

ПРАВИТЕЛЬСТВО РФ БЕРЕТ КИИ ПОД КОНТРОЛЬ

Правительство РФ приняло постановление (от 17.02.2018 № 162), представляющее правила контроля за объектами КИИ. Госконтроль путем проведения плановых и внеплановых проверок будет проводиться в целях соблюдения субъектами КИИ требований закона о ее безопасности.

Основанием для плановой проверки может стать, в числе прочего, «возникновение компьютерного инцидента на значимом объекте критической информационной инфраструктуры, повлекшего негативные последствия».



Кроме того, риск-ориентированный подход будет применяться при проверке юридических лиц и индивидуальных предпринимателей в рамках федерального государственного транспортного надзора и федерального государственного контроля в области обеспечения транспортной безопасности. Это позволит повысить результативность и эффективность контрольно-надзорной деятельности в этой сфере и одновременно снизить избыточное вмешательство государственных органов в деятельность хозяйствующих субъектов.

Отметим, что в последнее время возросло число попыток кибератак на объекты КИИ и финансовый сектор России. Так, по сообщению Национального агентства финансовых исследований, потери российских компаний от кибератак в 2017 году оцениваются более чем в 115 млрд рублей.

ЦИФРОВАЯ ИЗНАНКА НА PHDAYS 8

15–16 мая в ЦМТ на Краснопресненской набережной пройдет восьмой форум Positive Hack Days.

Участников и гостей форума ожидают круглые столы, мастер-классы, практические демонстрации и, конечно, технические доклады от ИБ-специалистов со всего мира. Основные вопросы — роль государства и регуляторов в цифровизации экономики, диджитализация финансовых технологий, безопасность КИИ, меры по снижению рисков и др. В рамках конкурсной программы будут продемонстрированы потенциальные проблемы и угрозы современных городских, медицинских и промышленных инфраструктур; государственных информационных систем и электронного правительства; бытового и промышленного интернета вещей; технологии блокчейн; биометрических систем аутентификации.



PHDAYS 8
Positive Hack Days
DIGITAL BET
15 – 16 МАЯ, 2018

 **БИЛЕТЫ
УЖЕ В ПРОДАЖЕ**



Более 100 активностей: доклады и дискуссии по проблемным вопросам отраслей с участием лидеров рынка, мастер-классы и лабораторные практикумы от ведущих экспертов в сфере исследования безопасности информационных систем, конкурс научных работ, выставочная зона, конкурсы по анализу защищенности продуктов и устройств, музыкальный фестиваль и др.

Мир сделал ставку на «цифру». Есть ли шанс защититься в мире, целиком построенном вокруг технологий? На PHDays 8 вы увидите всю изнанку цифровой экономики:

- Роль государства и регуляторов в цифровизации экономики
- Подходы к ИБ в условиях диджитализации финансовых технологий
- Безопасность критической информационной инфраструктуры
- Противодействие киберпреступности, выявление и расследование инцидентов
- Инновации в области взлома ИТ-систем и методов практической безопасности
- Развитие методов безопасной разработки ПО

Практические соревнования в уникальном реалистичном формате «Противостояние» — грандиозная битва экспертов по взлому и защите информации.

5000 участников: элита хакерского мира, первые лица, CIO и CISO российских и зарубежных компаний, представители интернет-сообщества и госструктур, регуляторы, ученые и др.



facebook.com/PHDays
twitter.com/phdays_ru

Открыта регистрация СМИ.
E-mail для заявок:
ysorokina@ptsecurity.com

#PHDays phdays.com

POSITIVE TECHNOLOGIES

НЕМЫСЛИМА БЕЗ БЕЗОПАСНОСТИ

РАЗВИТИЕ ФЕДЕРАЛЬНОГО ЗАКОНОДАТЕЛЬСТВА
ДОЛЖНО ОБЕСПЕЧИТЬ БЕЗОПАСНОСТЬ
ЦИФРОВОЙ ЭКОНОМИКИ

20 февраля 2018 года в Государственной Думе РФ прошли парламентские слушания «Формирование правовых условий финансирования и развития цифровой экономики», организованные Комитетом по финансовому рынку. Обсуждались вопросы финансирования и формирования правовой базы развития цифровой экономики, включая обеспечение безопасности.

Среди участников были Первый заместитель Председателя Правительства РФ Игорь Шувалов, министр связи и информации РФ Николай Никифоров, первый заместитель Председателя Банка России Ольга Скоробогатова, руководители парламентских фракций — инициаторов слушаний и профильных комитетов, а также представители компаний — поставщиков решений. Вёл слушания Председатель Государственной Думы РФ Вячеслав Володин. Представляем читателям нашего журнала изложения наиболее важных и интересных для них выступлений.



BIODATA НЕ ПРОТИВ ЧЕЛОВЕКА

Парламентские слушания по теме цифровой экономики в Российской Федерации проводятся своевременно. Правительство России этому вопросу уделяет много времени: принята и подписана программа «Цифровая экономика Российской Федерации» [утверждена Распоряжением Правительства РФ № 1632-р от 28 июня 2017 г. — прим. редакции].

В настоящий момент в экономической жизни нашей страны проходят самые разные процессы. Удалось за довольно короткое время от очень сложной, кризисной ситуации перейти к фазе экономического роста. Тем не менее на уровне высшего руководства страны, в Правительстве считают: по своему характеру и параметрам этот рост пока недостаточен, чтобы сделать жизнь рядового гражданина достойной, качественной, современной. Для этого нужно добиваться более высоких темпов. Практически все согласны: такие темпы и новые структуры экономики будут базироваться в первую очередь на развитии цифровой возможности.

Мы неоднократно в Правительстве обсуждали, что такое цифровая экономика. По мнению специалистов, это не только определённый уровень информатизации и владения соответствующими навыками. Цифровая экономика — целая совокупность различных элементов, придающих нашей жизни более высокое качество посредством новых технологий, нового технологического уклада. Мы понимаем, с какими сложностями сталкиваемся на этом пути и ещё будем сталкиваться.

На последнем Международном экономическом форуме в Санкт-Петербурге вопросам развития цифровой экономики было уделено много внимания в различных секциях. Одним из основных вопросов было законодательное обеспечение развития цифровой экономики. Выступали представители различных стран: из США, Евросоюза и других государств. Нормативно-правовое обеспечение развития цифровой экономики сегодня является одним из самых сложных вопросов для всех. Учитывая вопросы защиты прав человека — персональных данных, необходимо эффективно противодействовать киберпреступности, набирающей всё большие обороты.

Основной вывод по итогам дискуссий таков: принятие федерального законодательства, регулирующего формирование цифровой экономики, зависит от того, насколько быстро мы выработаем общую точку зрения. Все необходимые технологические решения существуют, проработаны вопросы приобретения отече-

**Игорь ШУВАЛОВ**

Первый заместитель
Председателя
Правительства РФ

БЕЗ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ, БЕЗ СОЗДАНИЯ ЦИФРОВОГО ОБЩЕСТВА НЕЛЬЗЯ ДОСТИГНУТЬ КАЧЕСТВА ЖИЗНИ ПЕРЕДОВЫХ СТРАН

ственного и зарубежного оборудования, обучения специалистов. Высокий уровень подготовки наших специалистов отвечает мировым стандартам, они востребованы в странах — лидерах развития цифровой экономики. Дело пока что за консенсусом в отношении законодательных вопросов.

Одним из основных итогов форума в Петербурге стало признание важной роли скорости, с которой национальные парламенты разрабатывают и принимают законы, обеспечивающие развитие цифровой экономики. Мы, в России и с партнёрами по ЕврАзЭС, готовы добиться ускорения законодательной работы для смены экономического уклада, «цифровизации» экономики и жизни домохозяйств.

Правительству РФ приходится решать довольно сложные вопросы, например, внедрение системы маркировки товаров, обеспечивающей прозрачную транспортировку грузов на единой таможенной территории ЕврАзЭС. Понятно, что это крайне важно для прекращения «серого» и «чёрного» импорта, контрабанды, для защиты отечественных производителей, принятия эффективных решений в производстве, логистике и торговле. Законодательным решением служит договор со всеми государствами ЕврАзЭС, который должен пройти ратификацию, а также другие нормативно-правовые документы на национальном уровне.

Правительство РФ провело эксперимент по маркировке меховых изделий, линейки из десятка наименований товаров. Уже предварительные дискуссии показали: есть силы, которые не заинтересованы в прозрачных торговых отношениях и оказывают серьёзное противодействие. А результаты продемонстрировали истинные масштабы товарооборота меховых изделий на территории единого таможенного пространства.

Следующим проектом стала маркировка лекарственных препаратов, а это вопрос не только экономики, но и безопасности здоровья человека. Здесь также пришлось сталкиваться с большими трудностями. Находились лоббисты, которые убеждали, что маркировка «вымоет» дешёвый сегмент из аптечных сетей, умень-

шит доступность лекарств. На деле введение маркировки сделает лекарства доступнее, пресечёт контрабанду и контрафакт, все они будут проверенными. Также была рассмотрена маркировка табачных изделий.

На основании проведённых экспериментов к концу 2018 года будет сделан выбор типа маркировки для России и всего пространства ЕврАзЭС. Нужна система, которая автоматически отслеживает движение маркированного товара от производителя через транспортировку и торговые сети до потребителя. Для этого все технологические возможности есть, но юридической базы пока нет.

Вместе с банковским сообществом запускается проект дистанционной идентификации пользователей. Клиент банка сможет, не посещая банковских учреждений, оформить обслуживание юридического лица, открыть счета, получить все виды услуг. Что может быть использовано для взаимодействия и с государственными органами, и с коммерческими организациями. Участие в этом начинании — дело добровольное, учитывая различные опасения по поводу безопасности хранения и передачи пользовательских данных. Ни одна страна в мире от этой преступной деятельности себя пока не застраховала, и этими вопросами обеспечения кибербезопасности также занимается Правительство РФ.

Цифровая экономика — основа совершенно новых решений, недоступных прежде. Граждане, в первую очередь в Москве, видят элементы цифровой экономики: работу новых систем слежения за движением и парковкой автотранспорта, развитие технологий получения государственных, образовательных и медицинских услуг. Идёт становление, которое в других странах занимало до двадцати лет. Мы в России, учитывая их опыт и опираясь на передовые технологии, можем гораздо быстрее достигнуть такого же и даже более высокого уровня цифровой экономики.

* * *

Есть и этические аспекты этого вопроса: при развитии цифровой экономики жизнь человека становится более и более «прозрачной». Но без использования цифровых технологий, без создания цифрового общества нельзя достигнуть качества жизни передовых стран. Поэтому один из главных вопросов — о надёжной защите каждого отдельно взятого человека, чтобы технологии больших данных не были использованы против него.

ПОТЕНЦИАЛ РАЗВИТИЯ ОГРОМЕН

У нас огромный потенциал для развития цифровой экономики, хотя пока её доля в ВВП России в два-три раза ниже, чем у ведущих стран. Не так давно известная международная консалтинговая компания McKinsey&Company провела исследования и оценила наши перспективы. Отмечен имеющийся у нас огромный потенциал в этой сфере, включая кадровый и другие заделы. Вывод: при условии целенаправленной работы властей, мы сможем за 6–7 лет по доле цифровой экономики в ВВП выйти на уровень США и ведущих европейских стран.

О потенциале говорят некоторые начинания, которые уже реализуются. Например, корпорация «МСП» создала бизнес-навигатор, который уже активно работает. Любой гражданин нашей страны может дистанционно определить адрес, где хочет начать свой бизнес. Сразу же появятся рекомендации, какое направление лучше развивать, примерный бизнес-план, банки для получения кредита и другая полезная информация. Из-за рубежа уже поступили предложения приобрести такой продукт. Подобных примеров у нас много.

Очень хорошо, что Правительство РФ приняло программу «Цифровая экономика», в которой определены пять базовых направлений работы. Для депутатов Государственной Думы РФ ключевым является направление нормативно-го регулирования: предусматривается принятие более 50 законов по разным аспектам цифровой экономики. Это очень важно и для бизнеса, и для государства — для снижения издержек и повышения производительности труда. Но депутаты также представляют избирателей, поэтому юридическая и технологическая защита их прав осуществляется при принятии всех законодательных решений.

Граждане России по-разному относятся к новым технологиям, поэтому очень важно следовать принципу добровольности, в том числе для финансовых услуг. Ни безналичные расчёты, ни платёжные карты административно не навязываются населению. Тем не менее за десять лет доля безналичных платежей с использованием платёжных карт выросла с 5% почти до 40%. Выражу уверенность: уже лет через пять практически все наши граждане будут пользоваться платёжными картами, оценивая их удобство и эффективность.

Мы, конечно, учитываем, что использование интернета у нас еще остается относительно низким, около 70% населения, в то время как в европейских странах — более 80% и даже к 90%. Сначала нужно добиться более широкого охва-

та наших граждан интернетом, чтобы можно было реализовывать проекты, связанные с его использованием.

Одно из ключевых направлений — большие данные. Есть проблемы: судебные иски о продаже некоторыми компаниями, использующими эти технологии пользовательской информации, которую иногда трактуют как персональные данные. Необходимо четко определить, что относится к персональным данным, а что к пользовательским данным, а также права и обязанности организаций, работающих с этими данными. Мы должны не просто максимально, а полностью защитить права наших граждан.

Необходим национальный стандарт работы с большими данными, регламентирующий формирование и обработку массивов информации, но технологически нейтральный, чтобы не препятствовать развитию. Государственное регулирование должно быть гибким, позволяя бизнесу находить новые решения при работе с большими данными.

Очень важное направление дистанционной идентификации. Недавно принят федеральный закон, позволяющий использовать биометрические данные для удаленной идентификации физических лиц. Подчеркну: дело это сугубо добровольное, такая идентификация может происходить только при согласии соответствующего лица, которое хочет получить удаленно определенные виды финансовых услуг. Пока мы эти возможности прописали только для кредитных организаций. После накопления опыта соответствующие нормы можно распространить на государственные организации: ФНС России, ПФР и другие, чтобы они также могли проводить удаленную идентификацию.

Необходимо максимально детализировать нормы, определяющие способы, порядок и процедуры дистанционной идентификации. Навести порядок в удостоверяющих центрах — устранить выявленные Счётной палатой РФ риски использования квалифицированной электронной подписи для фальсификации заявле-



Анатолий АКСАКОВ
Председатель Комитета
Государственной Думы
РФ по финансовому
рынку

**ОЧЕНЬ ВАЖНО СЛЕДОВАТЬ
ПРИНЦИПУ ДОБРОВОЛЬНОСТИ,
В ТОМ ЧИСЛЕ ДЛЯ ФИНАНСОВЫХ
УСЛУГ. НИ БЕЗНАЛИЧНЫЕ
РАСЧЁТЫ, НИ ПЛАТЁЖНЫЕ
КАРТЫ АДМИНИСТРАТИВНО НЕ
НАВЯЗЫВАЮТСЯ НАСЕЛЕНИЮ**



Выступление
Председателя Комитета
по финансовому рынку
Анатолия Аксакова. Фото:
<http://www.duma.gov.ru>

ний граждан о смене пенсионного фонда. На наш взгляд, выдавать такую подпись и предоставлять возможность ею пользоваться должны только государственные удостоверяющие центры.

Нужно дать в законодательстве чёткое определение, сформулировать требования к так называемой доверенной третьей стороне, которая проверяет подлинность электронной подписи. Существуют простая, неквалифицированная, квалифицированная и усиленная электронные подписи; следует чётко определить, в каких ситуациях они должны использоваться и каким образом — как мобильная, облачная и т. п.

Необходимо унифицировать требования к использованию усиленной квалифицированной электронной подписи, чтобы можно было использовать в работе с различными государственными структурами, в том числе для участия в торгах. Чтобы не приходилось каждый раз для разных случаев её получать в удостоверяющих центрах.

Есть также проблемы, связанные с недостаточным качеством работы с данными в государственных системах. Мы говорим о доступе коммерческих структур, в том числе кредитных организаций, к информации в государственных автоматизированных системах, в том числе к Единой системе идентификации и аутентификации. Однако недостоверная информация, — более 10% паспортных данных не актуальны, — может приводить к некорректным действиям.

* * *

Профильные Комитеты Государственной Думы РФ, работающие над законодательным обеспечением развития цифровой экономики, готовы плотно взаимодействовать с заинтересованными сторонами. Среди свежих результатов работы — подготовленные в тесном контакте с Правительством РФ и Банком России два законопроекта, касающимися цифровых финансовых активов, краудфандинга.

ЕДИНЫЕ ГОСУДАРСТВЕННЫЕ ПЛАТФОРМЫ

В эффективном построении цифровой экономики играют роль так называемые государственные платформы, выполняющие важнейшие, системообразующие функции, которые невозможно делегировать коммерческой структуре.

Чтобы и гражданам, и бизнесу пользоваться всеми возможностями цифровой экономики, нужно иметь собственный электронный профиль. То есть данные, позволяющие идентифицировать пользователя для любой электронной операции. И не просто идентифицировать, но и подтвердить неизменность этих данных, хранящихся в электронных архивах.

Такой электронный профиль является универсальным ключом для проведения электронных операций. Профиль содержит персональные данные, позволяя гражданину управлять доступом к ним, предоставлять их контрагентам для совершения операций. Электронный профиль гражданина в условиях цифровой экономики по сути — его alter ego, «второе я». Поэтому привязка таких профилей к конкретному гражданину должна быть исключительной прерогативой государства. Эту функцию нельзя делегировать негосударственным субъектам.

Хорошим средством доступа к электронному профилю гражданина может служить электронный паспорт. Часть данных, повседневно используемых, может быть записана на физическом электронном носителе гражданского паспорта, находящемся у его владельца. Весь объём его персональных данных может находиться уже в облачной среде, с определёнными правами доступа.

Пробором универсальной платформы электронной идентификации — аутентификации в России является единая система, функционирующая на сайте www.gosuslugi.ru. Доступом при помощи пары логин — пароль пользуются 65 млн зарегистрировавшихся наших сограждан. Недавно запущенная услуга для граждан — возможность проголосовать на выборах Президента России 18 марта 2018 года не по месту жительства, а выбрать удобный участок для голосования на сайте государственных услуг. Статистика такова: к середине февраля этой услугой при помощи системы идентификации — аутентификации воспользовалось более полумиллиона человек.

Для идентификации с июля 2018 года будет применяться также новейшая цифровая технология — биометрическая информация. Это принципиально иной подход к упрощению доступа граждан к электронным сервисам и услу-

гам. В некотором смысле цифровая биометрия постепенно будет вытеснять использование традиционной электронной подписи с отдельными ключами и носителями.

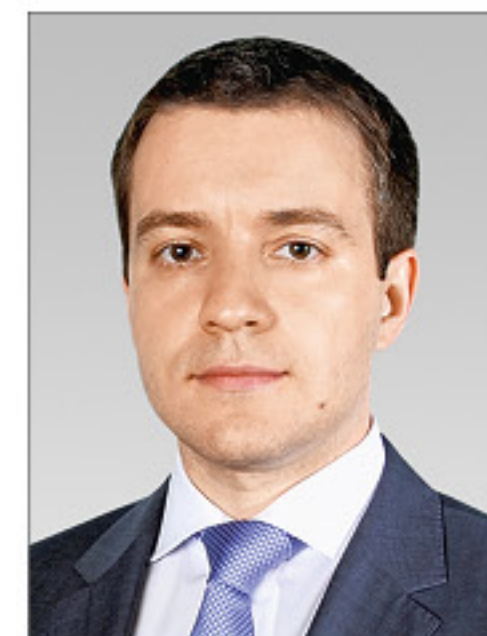
В цифровой экономике огромную роль играет передача данных, для которой необходимо выстроить единую систему — «цифровую магистраль» или «цифровое шоссе». За основу может быть взята уже успешно работающая в России система межведомственного электронного взаимодействия. С её помощью сегодня оказываются государственные услуги в электронном виде. В 2017 году между ведомствами, а также порталом государственных услуг, было передано более 20 млрд пакетов данных. Важно, чтобы наборы данных были машиночитаемыми, соответствовали единым стандартам и обрабатывались в автоматическом режиме.

У государственных органов сегодня действует более 5 000 официальных сайтов: региональных структур, федеральных, региональных, муниципальных и др. К сожалению, зачастую используемая на них информация, наборы данных, в том числе публикаций, не стыкуются между собой. Вместо такого разнообразия нужно постепенно приходить к единой государственной платформе представительства в интернете.

В качестве варианта предлагаем рассматривать единый портал государственных услуг. По популярности он занял 11-е место среди всех сайтов российского сегмента интернета, в котором лидируют также «Яндекс», «ВКонтакте» и Mail.ru, — это серьёзный результат. Единое представление государственных органов в интернете, объединив все официальные сайты, повысит эффективность взаимодействия. Будет сокращена ненужная трата времени на поиск информации и выстраивание электронного взаимодействия.

Получается, что ключевыми государственными платформами для построения цифровой экономики являются: первая — идентификационная, вторая — для обмена данными, и третья — для представительства, «витрина» в интернете. Можно добавить и единую геолокационную платформу, так как очевидно, что информация должна иметь привязку к местоположению.

Ключевые государственные платформы для развития цифровой экономики должны, в перспективе, обеспечить экономическую интеграцию в рамках ЕвразЭС, чтобы заранее избежать нестыковки данных и систем. Поэтому важно, чтобы проекты создания таких платформ в ближайшее время вошли в единую цифровую повестку сообщества и были реализованы.



**Николай
НИКИФОРОВ**
Министр связи
и массовых
коммуникаций РФ

Перечисленные нововведения требуют значительных инвестиций. То, что цифровые технологии и информатизация, перевод в электронный вид, является дешёвым удовольствием, — миф. Требуется создание базовой инфраструктуры. Остро стоит вопрос об использовании в сфере государственных информационных технологий механизмов государственно-частного партнёрства. Но финансирование базовых государственных информационных платформ, о которых шла речь должно вестись только из государственного бюджета, чтобы избежать конфликтов интересов и злоупотреблений.

Реализация перечисленных инициатив потребует серьёзного совершенствования нормативно-правовой базы. Здесь мы рассчитываем на поддержку депутатов Государственной Думы и профильных комитетов, с которыми традиционно ведётся взаимодействие. Такие задачи поставлены государственной программой «Цифровая экономика» по направлениям «Нормативное регулирование» и «Кадры и образование», координацию работ по которым осуществляет Министерство экономического развития РФ.

В течение 2018-го — первой половины 2019 года предстоит разработать более 50 за-

конопроектов по десяти тематическим разделам, касающимся формирования единой цифровой среды: пространства доверия, развития электронного гражданского оборота, внедрения и использования инновационных технологий на финансовом рынке, точечных налоговых льгот, преференций и множества других вопросов.

* * *

План по направлению «Кадры и образование», одобренный Правительством РФ, включает более 140 мероприятий. Это разработка новых форм образования с учётом задач цифровой экономики, развитие цифровой грамотности у широких слоёв населения, поддержка технологических образовательных процессов и так далее. Цель — к 2024 году число граждан, обучающихся по IT-направлениям, должно вырасти до 800 000; не менее 40% должна составить доля населения, обладающего цифровыми навыками. Ключевые направления программы «Цифровая экономика» утверждены правительственной комиссией во главе с Председателем Правительства РФ, мы приступаем к активной фазе реализации проекта.

Министр связи и массовых коммуникаций РФ
Николай Никифоров
и председатель
Совета директоров
АО «Тинькофф Банк»
Олег Тиньков. Фото:
<http://www.duma.gov.ru>



БЕЗОПАСНОСТЬ — НАШЕ ОБЩЕЕ ДЕЛО

Развитие цифровой экономики — вопрос перспектив нашей страны в конкуренции на мировом рынке. Об этом говорит настоящая гонка «цифровизации», которая развернулась во всём мире. Мы становимся свидетелями принципиально новых форм борьбы за экономическое и цифровое превосходство. В развитии цифровой экономики ключевую роль, без чего она попросту не может существовать, играет информационная безопасность, обеспечение гарантий надёжной и защищённой инфраструктуры.

Появляются широкие возможности влиять посредством технических устройств и программного обеспечения на критические точки экономики, системы управления государства и бизнеса. Что подтверждает атака в 2017 году вирусов-вымогателей, которая на некоторое время осложнила работу ряда государственных и коммерческих предприятий. Именно поэтому обеспечение информационной безопасности в промышленной и социальной сферах — острый вопрос.

Создатели и пользователи промышленного оборудования не всегда достаточно хорошо осведомлены о киберугрозах и связанных с ними рисках. Согласно исследованиям и экспертным оценкам, сегодня в мире около половины промышленных предприятий испытывают недостаток в квалифицированных специалистах по киберзащите. В России большинство промышленных предприятий тратят на информационную безопасность меньше, чем могут потерять за один день простоя, который может быть вызван кибератакой.

К сожалению, руководство многих российских компаний зачастую считает затраты на обеспечение кибербезопасности излишними. Поэтому необходимо повышать осведомлённость руководства компаний о существующих киберрисках, об обоснованности инвестиций в комплектацию штата специалистами по кибербезопасности, а также расширение знаний сотрудников об информационных угрозах.

Особое место в программе Правительства РФ «Цифровая экономика Российской Федерации» принадлежит направлению «Информационная безопасность». Наша задача как парламентариев продолжить развитие федерального законодательства для сферы информационных технологий.

Переход в России к информационному обществу заключается в том, что информационные технологии всё более широко применяются в государственном управлении и бизнес-процессах

в ключевых отраслях экономики. Система информационной безопасности должна надёжно защищать информационно-телекоммуникационную инфраструктуру, данные от кибероружия, информационного терроризма и криминала.

В государственных и корпоративных системах хранятся и обрабатываются огромные объёмы различной информации, в том числе персональных данных граждан. В 2017 году через единый портал государственных услуг было совершено более 25 млн платежей на общую сумму 30 млрд рублей. Вступил в силу закон о телемедицине¹. Персональные данные, в том числе медицинские, должны быть защищены государством, оно в состоянии обеспечить достаточный уровень киберзащиты.

Однако приводить к различным инцидентам способен и недостаток грамотности граждан в вопросах безопасного пользования интернетом на работе и дома. Согласно исследованиям РОЦИТ², федеральный индекс цифровой грамотности за 2016 год достиг 5,4 пункта, а по итогам 2017-го — почти 6 пунктов по десятибалльной шкале.

Для эффективного расширения применения цифровых технологий и интернета большое значение имеет повышение информационной грамотности населения. Не только знаний и умений пользоваться возможностями информационных технологий, но и соответствующих правил безопасности. Неслучайно в программе «Цифровая экономика» особое внимание уделяется созданию системы повышения грамотности населения в сфере информационной безопасности, медиапотребления и использования интернет-сервисов. Цифровая грамотность в обязательном порядке включает информационную безопасность.

* * *

По оценкам экспертов, увеличение количества пользователей интернета происходит и за счёт людей взрослых, представителей старших поколений. Только в 2017 году аудитория интернета увеличилась на 3 млн человек за счёт граждан старше 16 лет. Необходимо, чтобы граждане, уже получившие школьное и вузовское образование, имели возможность обучаться безопасному пользованию интернетом, чтобы не стать жертвами злоумышленников. Обеспечивать информационную безопасность развитие цифровой экономики необходимо для достижения её максимальной эффективности. Решение этой важной задачи — наше общее дело.



Леонид ЛЕВИН
Председатель Комитета
Государственной
Думы РФ
по информационной
политике,
информационным
технологиям и связи

¹ Федеральный закон от 29 июля 2017 года № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных технологий в сфере охраны здоровья»

² Региональный общественный центр интернет-технологий



Наталья
КАСПЕРСКАЯ
президент
ГК InfoWatch

РИСКИ ЦИФРОВОЙ КОЛОНИЗАЦИИ

ПОТОК НОВЫХ ТЕХНОЛОГИЙ

Нас всех в последние 2–3 года буквально захлестнул поток новейших технологий со страниц медиа. Мы постоянно слышим следующие уже знакомые до оскомины фразы: «новый технологический уклад», «индустрия четыре ноль», «новые технологии изменят мир», «экономика внимания», «экономика обмена», «устранение посредников» и т.п. Им сопутствуют статьи, доклады и новости о технологических прорывах, которые «изменяют мир», как то:

- ◆ Искусственный интеллект (далее — ИИ)
- ◆ Большие данные
- ◆ Блокчейн
- ◆ Криптовалюты
- ◆ Беспилотный транспорт
- ◆ Интернет вещей
- ◆ Телемедицина
- ◆ Мессенджеры
- ◆ Виртуальная реальность
- ◆ Уберизация
- ◆ И так далее.

Чем же плоха эта гонка за новейшими новинками?

ЧУЖОЙ КВЕСТ

Цели «прогресса» придумывает и «подсказки квеста» выкладывает кто-то другой, а не мы. Ещё два-три года назад никто не знал, что блокчейн или искусственный интеллект — это наше всё, что это единственное возможное будущее (тогда, если помните, все молились на «стартапы»).

А теперь это настолько же очевидно, как то, что Земля имеет форму шара и вращается вокруг Солнца. Откуда это взялось? Мы, в России, этого точно не вводили в дискурс и не закладывали в планы развития экономики. Тогда кто?

«Евангелисты новинок» вдохновенно втюхивают. В медийном пространстве внезапно появилось множество людей (очень часто — гуманитариев, журналистов, банкиров), которые вдруг оказались певцами и знатоками новых технологий.

Люди, в жизни не написавшие ни строчки кода и «владеющие технологиями» на уровне вызова «Убера» и написания постов со смартфона в модный мессенджер, внезапно стали знатоками и учат прогрессу нас всех — «ретроградов» и «консерваторов».

И многие ответственные люди, что называется, «ведутся» на это медийное давление.

Шумиха в прессе мешает трезво оценивать пользу технологий. Очень многие люди крайне медийно зависимы. Это касается и депутатов, и чиновников, и менеджеров крупного бизнеса. Не могут же все газеты и социальные сети ошибаться в том, что надо для всеобщего счастья сделать на блокчейне всё! И вот уже созываются важные совещания, составляются планы для регионов по внедрению новейших веяний и т.п.

При этом нагнетается истерия уходящего поезда: все уже там, одни мы опаздываем.

Специально создаётся ощущение, что главное — не опоздать. Чиновников, законодателей откровенно «прессуют» как можно быстрее принимать законы и внедрять новейшие технологии. Потому что якобы иначе всё пропало, остались буквально считанные недели.

Эта неестественная спешка и медийная «накачка» выдувает из голов ненужные мысли, не даёт времени задуматься и трезво оценить необходимость нового и риски.

Риски новой технологии сознательно замалчиваются или не обсуждаются. Довольно большой пласт уже известных проблем и рисков, связанных с криптовалютами, ИИ, блокчейном, Интернетом вещей просто не получает прессы, не обсуждается на профильных площадках и в Госдуме. Обсуждаются только сверкающие перспективы.

В результате происходит массовое бездумное заимствование чужого, опасного и ненужного. Обычный связанный список, пригодный только для очень формальных и узких применений (имеется в виду блокчейн) вдруг оказывается

применим где угодно — нотариат, медицина, выборы, госзакупки, земельный кадастр, государственное управление. Искусственному интеллекту, оказывается, надо также как можно быстрее поручить всё что угодно, включая сферы высокой человеческой ответственности: безопасность, транспорт, медицину и суды.

ВОЗМОЖНОСТИ И РИСКИ

Я четверть века занимаюсь информационной безопасностью. Сейчас являюсь главой Рабочей группы Программы «Цифровая экономика» по направлению «Информационная безопасность».

Информационная безопасность, в первую очередь, изучает технологические риски, а также приёмы людей, которые пытаются воспользоваться уязвимостями и незаконными возможностями новых технологий — и, наконец, методы, которыми можно противостоять этим людям и этим рискам.

Поэтому я смотрю на очередную волну «новых технологий» (уже четвёртую на моей памяти с начала 1990-х) с точки зрения сопутствующих им рисков.

Да, новые возможности — это хорошо. Но, как и в реальной жизни — каждой возможности всегда соответствует риск (таблица 1).

Как видим из этой таблицы, рисков достаточно хотя бы для того, чтобы сначала задуматься о стратегии и необходимости той или иной технологии.

ПОЧЕМУ НЕ СТОИТ СРАЗУ ВКЛЮЧАТЬСЯ В ГОНКУ НОВЫХ ТЕХНОЛОГИЙ

Чужая повестка: цели и средства нам навязывают. По сути, мы имеем дело с классическими ложными дилеммами. Нам следовало бы задаваться не вопросом, «как быстрее внедрить блокчейн в народное хозяйство», а вопросом: «какие проблемы и задачи есть в нашем народном хозяйстве, можно ли их решить средствами ИТ и какими именно», и уж потом «а не поможет ли тут нам в чём-то и блокчейн?».

А нам навязывают, в том числе с самых высоких трибун именно первую, ложную задачу.

Мы всегда в положении догоняющего. Если постоянно задаваться вопросом, «как быстрее внедрить очередную западную технологию» (а не вопросом, какие у нас есть задачи и как их решать), то мы всегда будем в положении догоняющего, вторичного игрока. И всегда будем заимствовать чужое — потому что оно уже готово.

То есть вместо производителей, мы будем потребителями чужих технологий. И дело тут не только в том, что мы будем всё больше платить за чужое — мы будем становиться всё более зависимыми.

Углубление зависимости: цифровая экономика разовьётся, но будет принадлежать не нам. Мы уже видим примеры того, что наша экономика, «подсевшая» на технологии предыдущих цифровых гонок — технологии Микрософт, Ора-

Возможности новых технологий	Риски внедрения новых технологий
Новые впечатляющие технологии, прорыв в ИИ, Интернете вещей, финтехе, анализе больших данных	Быстрое навязывание и заимствование западных технологий, деградация собственных компетенций
Новые функции, возможности общения, ускорение коммуникаций и платежей, новый уровень комфорта	Новые уязвимости, закладки, слежка, утечки персональных данных, потеря тайны личной жизни
Новые рынки, новые бизнес-модели, новые большие компании, новые массовые сервисы и информационные услуги	Риск быстрого захвата новых рынков транснациональными компаниями
Рост производительности труда, рост эффективности, внедрение ИИ, автоматизация, роботизация	Потеря рабочих мест, безработица, социальная напряжённость, возникновение слоя тунеядцев
«Экономика обмена», исчезновение посредников, повышение скорости и стандартизации услуг, уберизация медицины, образования, транспорта, сферы услуг	Юридическая неопределённость, этические проблемы, рост мошенничеств, снижение качества и ответственности, «роботизация» людей, рост социального отчуждения
Большие данные, анализ персональных данных, электронная идентификация и аутентификация личности, электронный двойник гражданина	Исчезновение приватности, навязчивая реклама, новый цифровой тоталитаризм, утечка персональных данных граждан за границу к мощным иностранным игрокам.
Инвестиции, стартапы, новые деньги, новые индустрии, «перелицовка» традиционных индустрий	Захват экономики более сильными и богатыми иностранными игроками. Внешнее управление экономикой.
Итог: новый технологический уклад, новая цифровая экономика, новое лицо традиционной индустрии и сельского хозяйства, государственного управления	Итог: новая стадия Цифровой колонизации, новая цифровая экономика принадлежит не нам, управляется извне, служит чужим интересам, а не Российской Федерации

Таблица 1. Возможности новых технологий и риски их внедрения

кл, Сименс — внезапно оказывается очень зависимой и уязвимой в новую эпоху ухудшения отношений с США.

Стоит американцам приказать — и крупные, красивые, публичные западные компании, которым мы верили, как себе, перестают выдавать обновления нашим корпорациям, отключают кредитные карты нашим банкам, отказываются работать в Крыму и т.п.

Новые технологии без должной гигиены усилят удалённый контроль и управление. Надо понимать, что все современные интернет-сервисы, смартфоны, планшеты, фитнес-браслеты, телевизоры, автомобили, самолёты, средства управления производством, прокатные станы, ЧПУ-станки и нефтедобывающие комплексы постоянно связаны с интернетом, скачивают обновления и управляются извне. Если это американские и европейские технологии — то и управляются они из США и Европы.

И после историй с отказом иностранных производителей поддерживать проданные ими продукты, мы не можем уже верить тому, что «публичная компания никогда-никогда не отключит сервис, потому что она заботится о клиентах». Публичная компания сделает так, как потребует правительство её страны.

Основные доходы ИТ уходят за рубеж. Надо понимать, что все без исключения продукты и сервисы в области информационных технологий переходят на модель подписки: даже если ты купил автомобиль, телевизор, смартфон, ты заплатил, по сути, только начальную сумму за установку — а потом ты продолжишь платить за подписку на обновления, ПО, расходные материалы и т.п.

И эти деньги практически не остаются в стране (за исключением относительно небольших расходов на службы продаж и поддержки).

Новый этап цифровой колонизации. Мы и так крайне зависимы от Windows, MS Office, Oracle, SAP, Facebook, Google. А если мы построим новую экономику на чужих криптовалютах, если нашим производством и транспортом станет управлять ИИ, разработанный Гуглом или Микрософтом, если мы отдадим большие данные о нашей экономике, наших АЭС и заводах, гражданах и госучреждениях западным игрокам — мы окончательно станем Цифровой колонией США.

ЕСТЬ ЛИ РИСК ОПОЗДАТЬ?

Мы привыкли к гонке технологий ещё со времён гонки между СССР и США. С тех времен мы помним, что в военных технологиях нельзя опаздывать. Именно ядерная гонка 1950–1980 годов дала современной России тот ядерный щит, который и сейчас позволяет нам быть независимыми.

Но что насчёт коммерческих технологий? Обязательно ли нам нужно быть «вровень» и с кем именно? Вообще-то, возможно, не все это знают, что в области ИТ мы во многом впереди многих, в том числе «развитых» государств Европы и Америки.

Например, в области широкополосного доступа в Интернет, в области оплаты услуг со смартфонов, в области мобильной связи. В 90-е мы перескочили довольно многие «малые» технологические уклады — например, факсы, пейджеры, автоответчики, которые до сих пор в ходу в США и Европе. А наши интернет-сервисы (поисковики, публичные почты, интернет-СМИ, социальные сети) не хуже американских и значительно лучше европейских и азиатских.

Это неспроста. На самом деле вовсе не все технологии, которые сейчас «на слуху», получат в будущем распространение и станут общепринятыми.

Вот как развивается почти всякая новая технология в области ИТ, согласно «кривой хайпа» от известной аналитической компании Гартнер (рисунок 1).

Сначала новая технология вызывает пик медийной шумихи, «хайпа», раскрутки. Это то, о чём я сказала в начале. Этот пик занимает обычно 2–3 года.

Именно на пике принимаются неверные решения и тратятся огромные деньги.

Затем наступает разочарование в новинке, «пузырь лопается», и внимание к новинке падает почти до нуля. В этот момент разоряется большинство компаний и инвесторов, поверивших в новинку.

Рисунок 1.
Кривая хайпа





Затем ИТ-индустрия переосмысливает новинку, ищет её прагматические применения, новые компании начинают строить на новинке настоящие, полезные сервисы и продукты.

Новинка выходит на «плато продуктивности» уже не в формате медийной приманки модной технологии, а в формате продукта. И начинает улучшать жизнь и зарабатывать деньги. Выход на плато — и есть самый лучший момент для заимствования или внедрения новинки в компаниях или госучреждениях.

К сожалению, в отношении большинства «новейших новинок», о которых мы говорим сейчас и которые считают основой будущей Цифровой экономики, можно сказать, что мы находимся на самом пике хайпа. То есть в «пузыре». Это видно невооружённым взглядом.

Это означает, что большинство вложенных сейчас в новинки денег будут потеряны впустую,

большинство основанных компаний и начатых проектов разорятся, а выигравшими будут игроки второй волны.

Мы хорошо помним пузырь «доткомов», бум «мобильного контента», бум социальных сетей, и другие классические примеры прохождения новинок по кривой Гартнера. Но индустрия, инвесторы и даже государственные чиновники почему-то ничему не учатся на этом опыте. А опыт говорит следующее:

◆ Опоздать особенно никуда нельзя. Средний срок выхода новинок на плато продуктивности — 4–6, иногда 7–10 лет. Например, за 10 лет существования технологии блокчейн никаких эффективных его применений, кроме изначального (криптовалют), создать, по сути, пока не удалось;

◆ Часть новинок вообще не взлетит (как не взлетели 3D-телевидение и виртуальная реальность, например);

Выступление Натальи Касперской на парламентских слушаниях «Формирование правовых условий финансирования и развития цифровой экономики». Фото: <http://www.duma.gov.ru>

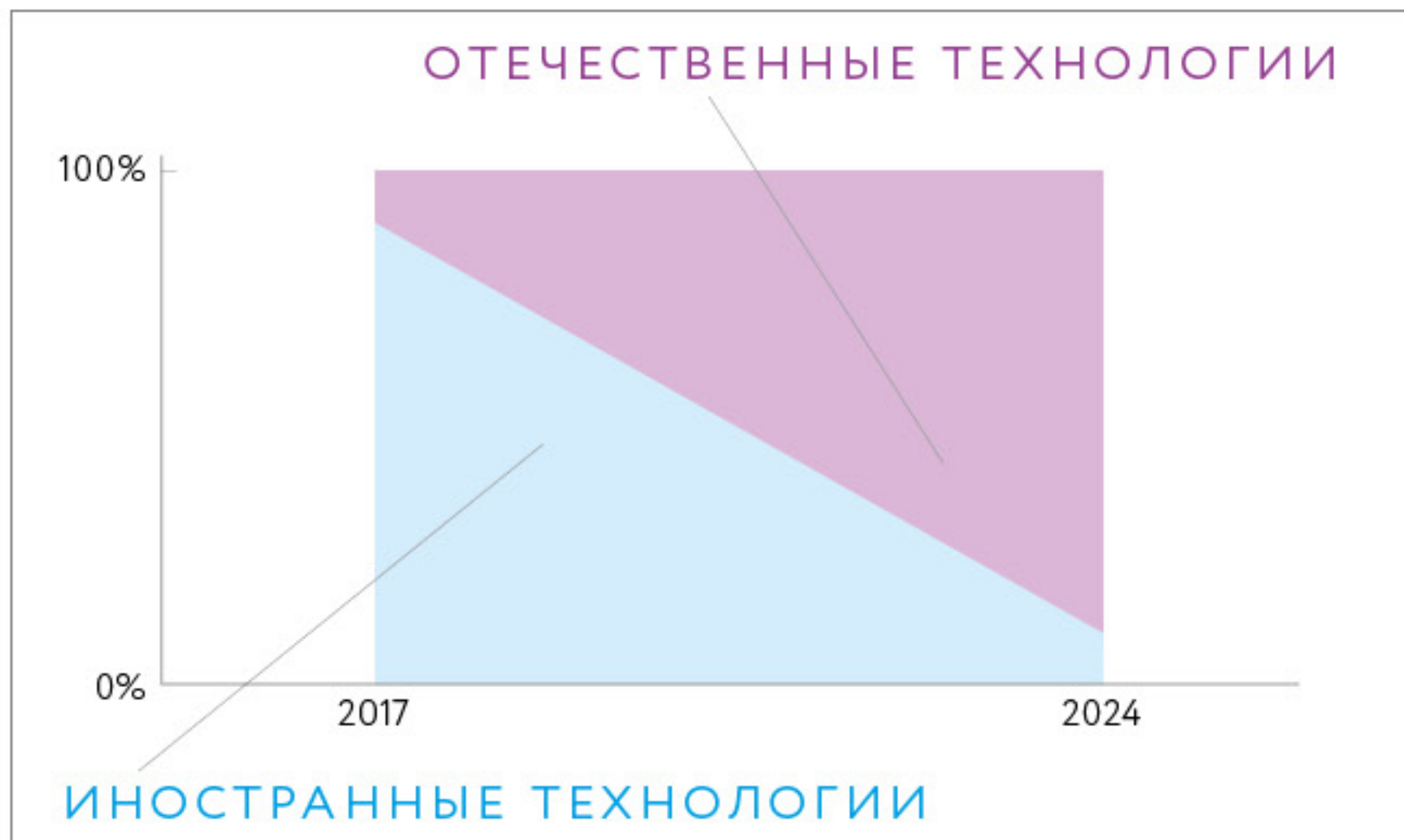


Рисунок 2. В этом идеальном случае от зависимости в районе 90% мы могли бы к 2024 году снизить свою зависимость от технологического импорта до 10–20%, что вполне терпимо

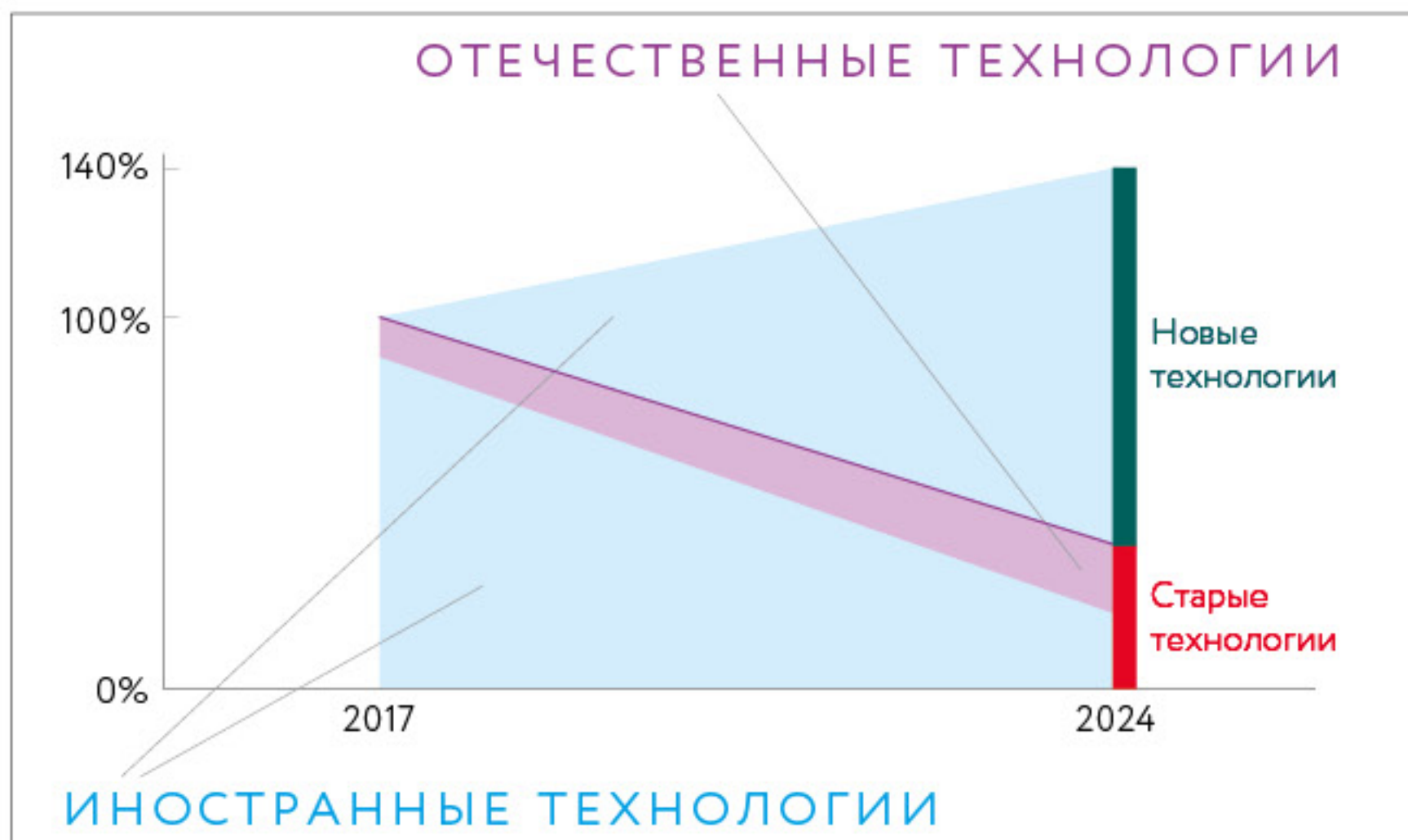


Рисунок 3. Новые технологии вытесняют старые, а поскольку из-за спешки и моды внедряются в основном западные новинки, зависимость только растёт, превращая РФ в цифровую колонию США.

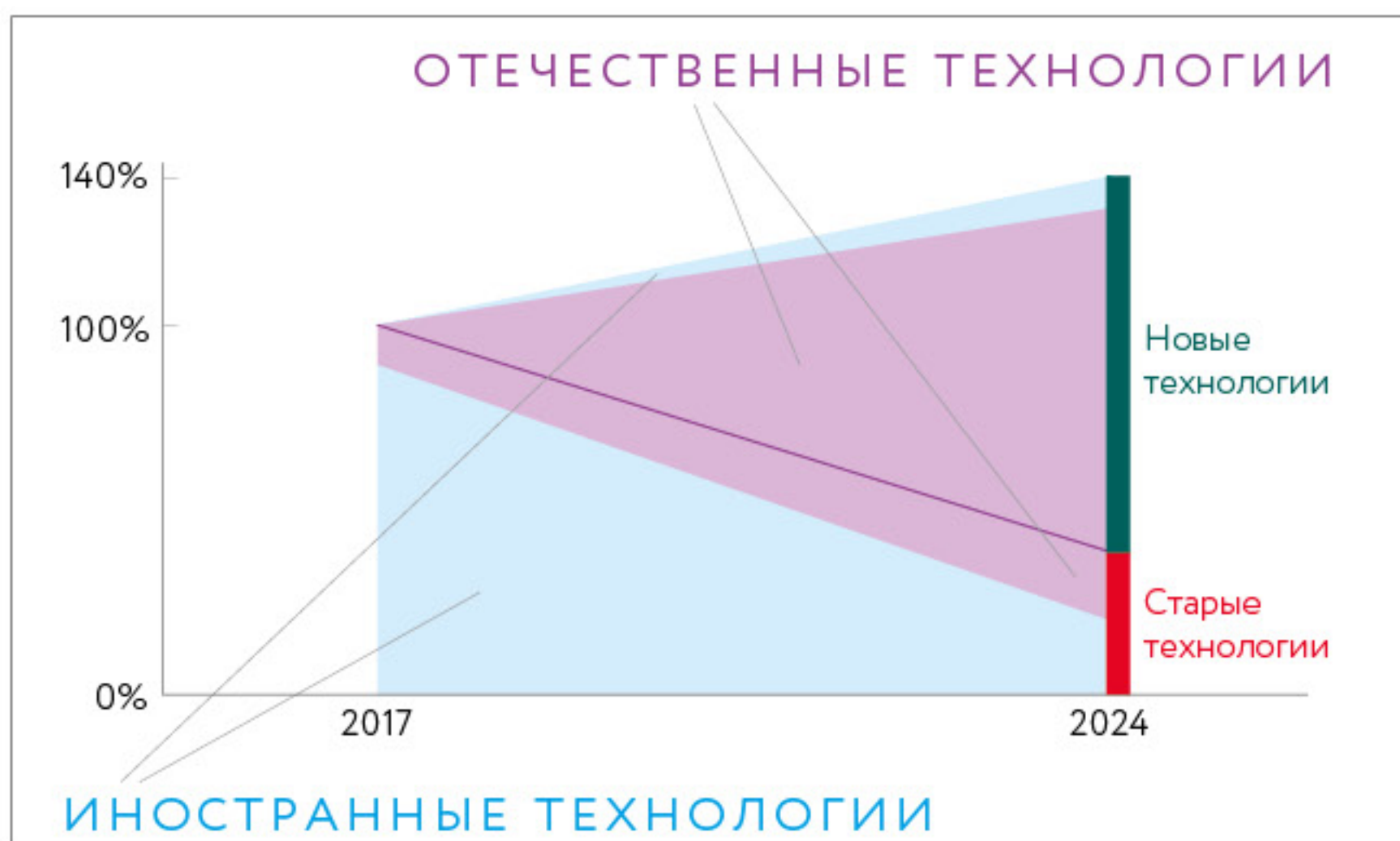


Рисунок 4. Если новые технологии будут преимущественно отечественными, то к 2024 году мы как раз и получим ту самую независимость на 80–90%.

◆ Гнаться надо не за «технологией», а за продуктом. «Голую» технологию нельзя применить в компании или госкорпорации, разве только для того, чтобы отрапортовать начальству, что менеджмент следует за модными веяниями;

◆ Чаще выигрывают осторожные прагматики, которые внедряют технологии от игроков второй волны, уже проверенные и развитые — и внедряют не из-за моды, а понимая конкретную пользу от внедрения. Здесь уместен упоминавшийся выше пример того, как РФ в мобильной связи перескочила сразу к стандарту GSM, миновав тех уродцев, которые до сих пор в ходу в США и Европе.

ЧТО ДЕЛАТЬ? НЕ ПОДДАВАТЬСЯ МАГИИ ТЕХНОЛОГИЙ

В условиях всеобщей медийной паники и даже истерии по поводу новейших технологий важно сохранять трезвость ума и спокойствие. Нужно помнить о следующих правилах:

- ◆ Идти не за хайпом, а от реальных потребностей общества, бизнеса и государства
- ◆ Идти не от модной «технологии», а от продукта, внедрять не «технологии», а средства повышения производительности, прозрачности управления.
- ◆ Не торопиться внедрить что угодно на пике популярности и моды, а ждать «плато производительности» новых продуктов и платформ.
- ◆ Помнить о цифровом суверенитете, как необходимом условии внедрения любых технологий.

РАЗВИВАТЬ СВОЁ

У нас поставлена задача импортозамещения в области ИТ. В идеале она могла бы выглядеть как на рисунке 2.

Однако, в связи с тем, что на самом деле происходит постоянное появление новых технологий, реальная картина их развития будет такая, как на рисунке 3.

На самом деле, правильный сценарий внедрения новейших технологий должен быть таким, как на рисунке 4.

Я лично являюсь членом Экспертного совета по отечественному программному обеспечению. За прошедшие 2,5 года работы я убедилась, что у нас в стране есть огромное число интересных программных продуктов — талантливых, актуальных.

В реестре отечественного ПО уже есть более 4000 отечественных программных продуктов, покрывающих весь спектр, всю технологическую линейку, или, как любят говорить программисты, «весь стек технологий»: опера-

ционные системы для серверов, компьютеров и смартфонов, офисные приложения, графические редакторы, системы автоматического проектирования, системы АСУ ТП, средства информационной безопасности, игры, поисковые системы и т.п.

Это значит, что мы можем развивать те или иные модные новые технологии практически полностью собственными силами:

♦ **Большие данные:** это очень чувствительная сфера, создающая много рисков нарушения прав граждан на защиту личной жизни, рисков слежки со стороны глобальных компаний и спецслужб иностранных государств; поэтому нам нужно использовать только свои продукты, у нас отличная научная база; при этом необходимо законодательно обеспечить ограничение оборота больших пользовательских данных и персональных данных граждан РФ для иностранных компаний (использовать и хранить их только на территории РФ, по утверждённым в РФ регламентам).

♦ **Искусственный интеллект:** у нас есть мощная научная школа в области ИИ, много разработчиков и учёных, большое количество малых и больших компаний в этой сфере; мы можем и должны использовать только свои технологии и продукты, заказывать разработки в области ИИ отечественным университетам и компаниям.

♦ **Интернет вещей, промышленный Интернет, радиометки RFID:** у нас в этой сфере есть свои разработчики, ассоциации, разрабатываются собственные протоколы и стандарты; это крайне чувствительная и опасная сфера, поэтому нам обязательно нужно использовать свои регламенты, протоколы и технологии, прекратить бездумную инфильтрацию и диффузию в страну чужих устройств, соединённых с Интернетом, нужно проверять и «стерилизовать» импортные устройства и технологии Интернета вещей.

♦ **Блокчейн:** здесь у русских одна из лидирующих позиций в мире; нам нужно серьёзно изучать применимость этой технологии в области финансов и госуправления, использовать только отечественные реестры на основе идеологии блокчейна, с российской криптографией, нельзя внедрять никаких глобальных реестров с внешним управлением.

♦ **Криптовалюты:** это сфера, серьёзно угрожающая экономическому суверенитету РФ, имеющая большой криминальный потенциал, поэтому здесь нужна крайняя осторожность. Мы не можем допустить оборота в РФ чужих валют с неконтролируемой эмиссией, оборо-

том и курсом. В РФ есть много специалистов и решений финтеха и криптовалют, нам нужно создавать собственные валюты и биржи, шлюзы во внешний рынок.

Безусловно, развитие Цифровой экономики и минимизация рисков для граждан, общества и государства требуют серьёзной законодательной работы.

ЗАКОНОДАТЕЛЬСТВО И ПРАВОПРИМЕНЕНИЕ

Есть еще один важный аспект развития новых технологий для того, чтобы предотвратить или максимально снизить, возможные риски. Это — регуляторные и законодательные ограничения. Тут, на мой взгляд, нам необходимо учитывать следующее:

♦ **Опережающее законодательство.** Нам нужно законодательство, упреждающее возникновение проблем и рисков. Чтобы не получилось, как с Интернетом, распространение которого, риски и влияние на жизнь сотен миллионов людей законодатели всего мира осознали на 10–15 лет позже, спохватились задним числом.

♦ **«Песочницы».** Для запуска новых технологий нам нужны своего рода «законодательные песочницы», отрасли или регионы, где разрешается развитие новых технологий без немедленной правовой ответственности, но под пристальным наблюдением регуляторов. Это нужно и для беспилотного транспорта, и для финтеха, и для анализа больших данных.

♦ **Быстрое реагирование и настройка.** Нам нужна процедура быстрой обратной связи, когда проблемы и риски, возникающие в области новых технологий, приводят к быстрому изменению законодательства, к постоянной точной настройке регулирования.

♦ **Поддержка импортозамещения и цифрового суверенитета.** Наше законодательство в области ИТ должно наконец стать национально-ориентированным. Нам нужно отбросить сантименты и вводить прямые ограничения конкуренции для иностранцев в области ИТ. Сейчас иностранные производители, как правило, находятся в лучшем положении, чем отечественные. Например, западные интернет-гиганты вроде Твиттера и Фейсбука не ведут здесь никакой официальной деятельности, не имеют юридических лиц или представительств — и при этом зарабатывают на нашей аудитории и ведут политическую пропаганду.

♦ **Защита граждан и частной жизни.** Нам нужен прямой запрет выкачивания больших данных о наших гражданах, обществе, экономике и государстве за рубеж.



**Ольга
СКОРОБОГАТОВА**
первый заместитель
Председателя Банка
России

ДУМАТЬ НА СТАДИИ ПРОЕКТИРОВАНИЯ

КАК ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
СТАНОВИТСЯ НЕОТЪЕМЛЕМОЙ ЧАСТЬЮ
ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Банк России принимает активное участие в реализации программы «Цифровая экономика Российской Федерации». В своем выступлении на X Уральском форуме первый заместитель председателя Банка России Ольга Скоробогатова рассказывает о новых подходах и основных направлениях деятельности Банка России в сфере финансовых технологий и информационной безопасности.

Публикуем стенограмму выступления в сокращенном виде.

ТРЕНДЫ И ВЫЗОВЫ В СФЕРЕ ИБ

Заметные изменения, которые мы наблюдаем на рынке технологий, влекут за собой возникновение массы новых проектов и экосистем. При этом вопрос «насколько эти технологии безопасны?» волнует инвесторов и потребителей в первую очередь.

Вопрос действительно не праздный. В 2017 г. число инцидентов ИБ в финансовой сфере увеличилось по сравнению с предыдущим годом в 2,3 раза (два года назад в 1,6 раза). Системы мониторинга показывают, что мошенники не просто развиваются вместе с технологиями, но делают это даже быстрее, придумывая все новые и новые способы фрода.

Мировые расходы на обеспечение ИБ коммерческих организаций в 2018 г. составят \$93 млрд (на 8% больше, чем в 2017 г.). Это общая цифра, охватывающая банковский и небанковский сектор экономики.

Финансовая отрасль является драйвером финансовых технологий, поэтому 58% кредитных организаций уже начали инвестирование в технологии для снижения киберрисков. Процесс этот неоднородный, кроме банков в создании новых безопасных платформ заинтересованы в первую очередь телеком и электронная коммерция. Представители

**В 2,3
раза**

увеличилось число инцидентов информационной безопасности в финансовой сфере в 2017 г.

40%

российских организаций* не имеют стратегии информационной безопасности

**93 млрд
долл. США**

мировые расходы на обеспечение информационной безопасности коммерческих организаций в 2018 г. (+ 8% по сравнению с 2017 г.)

48%

российских организаций* увеличили расходы на обеспечение безопасности из-за цифровой трансформации бизнес-моделей

58%

финансовых организаций инвестируют в технологии для снижения киберрисков

60%

финансовых организаций будут инвестировать к 2020 г. в инструменты защиты информации (+25% по сравнению с 2017 г.)

Источники: Trend Micro Security: Paradigm Shifts: Trend Micro Security Predictions for 2018; PwC: The Global State of Information Security 2018, Top financial services issues of 2018; Gartner
* Принявших участие в исследовании The Global State of Information Security 2018

Рисунок 1. Тренды и вызовы в сфере информационной безопасности



В ЕС 25 мая 2018 г. вступает в силу новый режим защиты персональных данных – **General Data Protection Regulation (GDPR)**

-  Защита персональных данных начинается **на этапе проектирования систем**
-  Клиент должен иметь право при получении услуги **не давать согласие на обработку данных**, которые не требуются для ее предоставления
-  Накопленные клиентом данные могут быть **переданы третьей стороне с его согласия**
-  Необходимо **уведомлять надзорные органы** в области защиты персональных данных **об инцидентах**



Европейской комиссией в 2017 г. разработан проект **FinTech Action Plan**, который содержит меры по развитию инновационных технологий в финансовом секторе ЕС

-  Главный приоритет FinTech Action Plan – **обеспечение кибербезопасности**, в том числе разработка единых подходов к тестированию механизмов противодействия киберугрозам

Рисунок 2. Новые подходы к защите информации

этих трех отраслей все чаще объединяются в т.н. партнёрства или экосистемы.

Финансовые организации по всему миру, понимая свою ответственность перед клиентами, разрабатывают отдельные программы создания инструментов киберустойчивости. В то же время в России 40% таких организаций не имеют своих стратегий ИБ. Стоит оговориться, эта цифра не касается банков. В банковской сфере 70–75% кредитных организаций имеют детально проработанную стратегию ИБ, а 30% кредитных организаций предлагают детализировать существующую стратегию кибербезопасности.

В целом уровень проработки стратегий ИБ в российских организациях небанковской сферы находится на довольно низком уровне. 48% компаний понимают, что нужно увеличивать расходы на ИБ и уже начали это делать, а 60% планируют вкладываться в инструменты защиты только к 2020 г.

ПРИОРИТЕТЫ 2018 ГОДА

Два года назад приоритетным направлением деятельности банков по нашим опросам было развитие цифровых технологий. Кибербезопасность стояла на четвертом месте. В 2018 г. банки поставили кибербезопасность и защиту данных на первое место (рис. 1). Соответственно и сами банки, и Центральный банк как регулятор должны понимать, как будет выстраиваться система киберзащиты на национальном уровне.

Но сфера мегарегулятора — это не только банки, но и некредитные финансовые организации, которые также должны иметь свои системы быстрого реагирования на возникающие угрозы. Актуализация и укрупнение задачи заставило Банк России принять решение о выделении направления информационной безопасности в отдельный департамент. Это связано как с прямым запросом рынка, так и с пониманием,

как и в каком направлении нужно развиваться в данной области. Кроме того, внедряя новые решения и создавая новые платформы, Банк России планирует встраивать элементы киберзащиты уже на стадии проектирования.

Второе место в списке приоритетов 2018 г. занимает цифровая трансформация. Но мы уверены, что в ближайшие 5–7 лет будет преобладать уклон в сторону ИБ, пока не выстроится абсолютно понятная, прозрачная система, гарантирующая максимальную защиту как потребителя, так и национальных интересов.

На третье место среди приоритетов неожиданно вышел сравнительно новый тренд — развитие кадров и поиск талантов. В 2016 г. он занимал только седьмую позицию. До последнего времени не так много компаний и банков понимало, что нужно не только искать людей, но и вкладываться в их развитие и обучение.

В МИРЕ

Что происходит в мире в сфере ИБ?

В Европейском Союзе уже давно была принята платежная директива № 2, которая разрешает банкам и любым компаниям получать информацию о счетах и остатках по счетам в случае, если клиент согласен. Эта директива действовала как теоретический документ и не содержала элементов информационной защиты.

25 мая 2018 г. вступает в силу другой документ — General Data Protection Regulation, в котором подробно прописаны основные правила защиты персональных данных (рис. 2). Правила сводятся к тому, что клиентов нужно правильно информировать о том, как их данные будут использованы, и получать их осознанное согласие на использование персональных данных в явной форме. В документе есть требования по защите информации как для кредитных организа-

В НАШЕМ ПОНИМАНИИ ИТ И ИБ ДОЛЖНЫ РАССМАТРИВАТЬСЯ НЕ КАК РАЗНЫЕ НАПРАВЛЕНИЯ, А КАК НЕРАЗРЫВНЫЕ ЭЛЕМЕНТЫ, ФУНДАМЕНТ ДЛЯ ЕДИНОЙ ЦИФРОВОЙ ЭКОНОМИКИ

ций, так и для компаний широкого профиля. Вводится новая отчетность, которая уведомляет надзорные органы в области защиты персональных данных.

Но самое интересное, что произошло при выпуске этого документа: часть положений по ИБ вошла в противоречие с платежной директивой. И теперь ЕС не понимает, как ему поступить: убрать часть положений из платежной директивы и серьезно корректировать оставшиеся или упростить требования в части нового закона. С профессиональной точки зрения нам очень важно и интересно, как решат эту проблему коллеги из ЕС. Как мне кажется, им придется корректировать и первый, и второй законы, т.к. их надо синхронизировать, в противном случае система вряд ли заработает.

Еще одна причина противоречий: кредитные организации и те, кто владеет большими данными о клиенте, не готовы делиться со стартапами или технологическими компаниями, которые могут составить им конкуренцию. Поэтому в General Data Protection Regulation есть пункты, ограничивающие возможность обслуживания клиентов маленькими и средними компаниями. Я думаю, что уже в следующем году мы увидим варианты решения этих проблем.

Почему нам это важно? Потому что мы движемся в область финтеха и желаем не просто ее регулировать, но и содействовать ее развитию, включая создание правильных механизмов защиты. Соответственно нужно уже на стадии законодательных документов, организационных и технологических мероприятий детально согласовывать планы по этим направлениям.

Более того, в нашем понимании информационные технологии и информационная безопасность должны рассматриваться не как разные направления, а как неразрывные элементы, фундамент для единой цифровой экономики.

ВНУТРЕННЯЯ СТРАТЕГИЯ БАНКА РОССИИ

Два года назад Банк России как мегарегулятор принял для себя важное решение: не просто надзирать и регулировать финансовую сферу, а содействовать отрасли в развитии конкуренции, появлении новых продуктов, услуг и т.д. То есть не запрещать новые платформы и технологии, а изучать их и, если это целесообразно, отражать новые задачи и тренды в нормативных документах, что должно приносить пользу и клиентам, и самому финансовому рынку.

В развитие такого подхода мы разработали внутреннюю стратегию «Основные направления развития финансовых технологий на период 2018–2020 годов», в которой определили семь направлений:

1. Правовое регулирование. Фактически мы уже живем в цифровом мире и активно пользуемся понятиями и определениями, которых тем не менее все еще не существует на уровне законодательной базы: смарт-контракты, распределенные реестры, валидация, майнинг и т.д. Чтобы использовать и осуществлять в реаль-

ной практике все то, что стоит за этими словами, нужно, как минимум на нормативном уровне, сформулировать что это такое и понять, как эти термины и определения могут использоваться в защите инвесторов и клиентов. Первый шаг — систематизировать новые понятия и дать им определения — мы делаем совместно с Минфином и Минэкономразвития. Закон называется «О цифровых активах». Сейчас он проходит обсуждение, есть разногласия, но в части основных понятий и определений стороны пришли к общему пониманию.

2. Развитие цифровых технологий на финансовом рынке. В 2016 г. Центробанк и участники рынка создали Ассоциацию «Финтех», поскольку в существующей парадигме развития невозможно двигаться вперед, не сотрудничая и не содействуя друг другу. На этой площадке мы обсуждаем перспективные технологии, проекты, платформы, вырабатываем подходы, устраивающие и регулятора, и рынок, планируем совместные мероприятия. Недавно мы договорились, что в рамках осуществления программы «Цифровая экономика РФ» все вопросы цифровых технологий в финансовой сфере будут обсуждаться на площадке Ассоциации «Финтех», т.к. в нее входят именно те участники, которые способны профессионально оценить предложения и оказать помощь в выработке планов по их реализации.

3. Переход на электронное взаимодействие между Банком России, органами государственной власти, участниками финансового рынка и их клиентами. Если говорить о Банке России и участниках рынка, то ситуация с электронным взаимодействием на данный момент выглядит не радостно. При огромном количестве данных, которые мы получаем как регулятор, мы продолжаем нагружать финансовую сферу запросами в бумажном виде. И тут у нас необъятное поле для деятельности. Предполагается, что за три года мы полностью переведем общение с участниками финрынка на электронный документооборот. В 2017 г. мы запустили личные кабинеты. В этом году вышли нормативные документы, разрешающие банкам передавать информацию в электронном виде. Но главная наша цель заключается в том, что, получив информацию от банка, дальше работать с ней только через инструментарий управления большими данными и машинного обучения. Чтобы самим делать отчеты, необходимые справки, не перекладывая это на участников рынка.

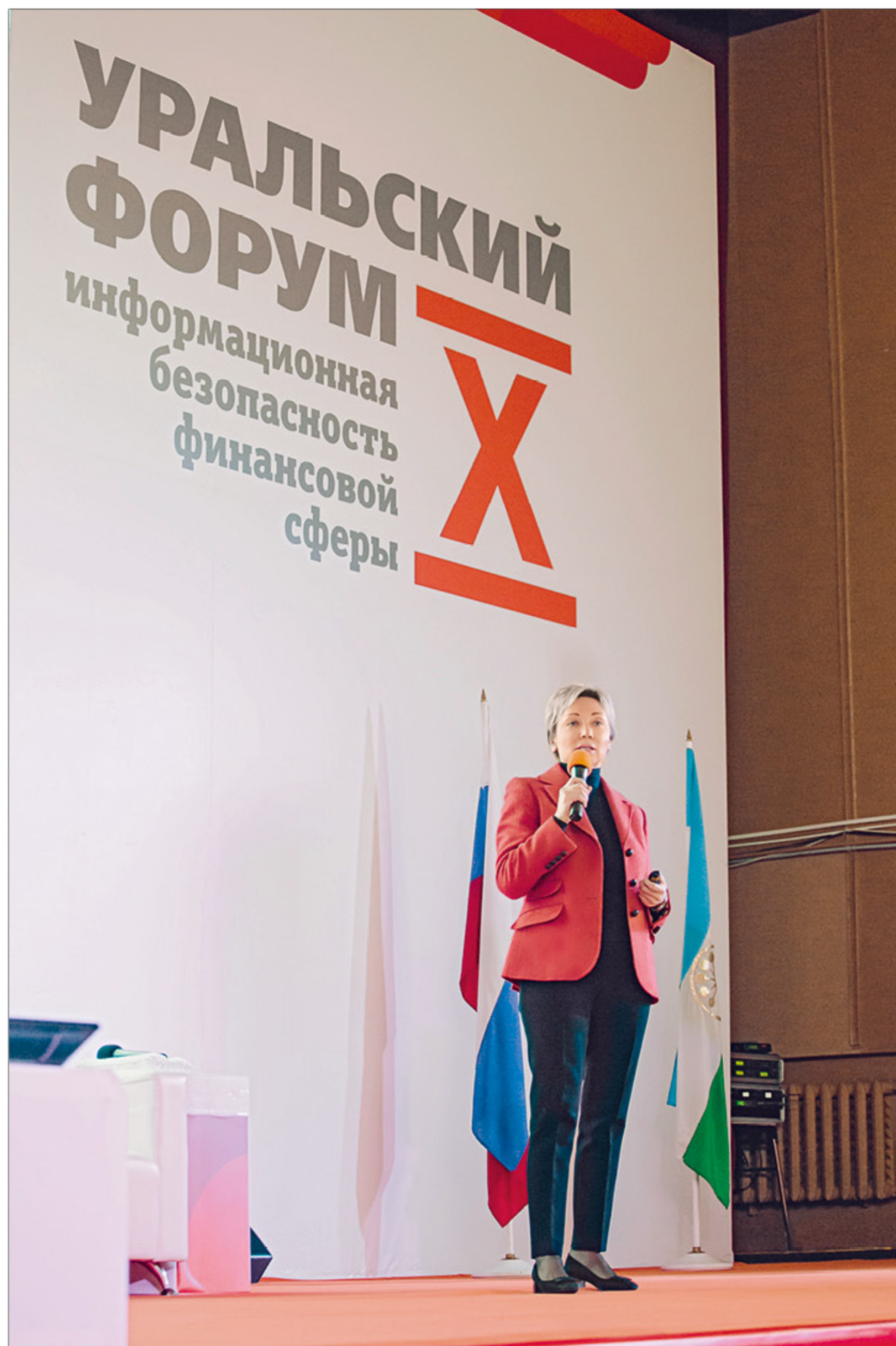
4. Создание регулятивной площадки Банка России. Мы изучили международный опыт регуляторов разных стран — Сингапура, Англии, Швейцарии и др. — и решили двигаться в два этапа. На первом этапе создаем песочни-

цу, она начинает свою работу во втором квартале 2018 г. Проекты в ней будут испытываться в тестовом режиме, без влияния на реальных потребителей. Почему? И Банку России, и участникам рынка, и многими министерствам и ведомствам надо понять, как этот механизм будет работать, отладить его, внести изменения в нормативные документы. В 2019 г. начнется второй этап — запуск проектов в реальном секторе, но сначала в ограниченном периметре.

5. Взаимодействие в рамках ЕАЭС. Эта тема обсуждается на всех конференциях и семинарах, но, к сожалению, на уровне ЕАЭС нам до сих пор не удалось создать какие-то общие прогрессивные решения. Причин, объективных и субъективных, много. Одна из них, например, — наши старые системы и платформы, которым сложно интегрироваться с европейским IT-ландшафтом. Но взаимодействовать необходимо. В этом направлении Банк России совместно с регуляторами ЕАЭС выработал план действий. В 2018 г. мы должны договориться по каким направлениям создавать новые платформы и какие технологии для этого применять. В 2019 г. планируем прописать дорожную карту по созданию общих решений.

6. Обеспечение безопасности и устойчивости. ИБ и киберустойчивость пронизывают все направления деятельности: и технологии, и инфраструктуру, и правовое... Тут на многое нужно взглянуть по-новому, поэтому мы специально выделили ИБ в отдельное направление. Зона постоянного внимания — это мониторинг и развитие собственной системы безопасности как для внутренних целей, так и при взаимодействии с участниками рынка.

7. Развитие кадров в сфере финансовых технологий. Чуда ждать бесполезно. Никто не приведет за руку готовые талантливые кадры. Поэтому мы экспериментируем с образовательными программами на разных уровнях: университеты, вузы и даже школы. Например, мы договорились со Школой талантов «Сириус» о создании площадок, на которых талантливые дети будут не только учиться, но и вполне серьезно тестировать инновационные технологии, конечно, пока в ограниченном периметре.



Выступление Ольги Скоробогатовой на X Уральском форуме

О ПЛАТФОРМАХ

Как регулятор мы понимаем, что на уровне государства возможна синергия по многим направлениям, и создание инфраструктуры национального масштаба интересно всем участникам рынка.

Например, **финансовый маркетплейс** и **платформа регистрации финансовых сделок** — это те две платформы, которые мы сейчас обсуждаем. Они направлены на создание службы одного окна, когда клиент не ищет по разным банкам нужную услугу или сервис, а заходит на один портал,



как в гипермаркет, и выбирает из множества продуктов разных производителей именно те, что ему подходят.

Финансовый маркетплейс поможет выбирать услуги и сервисы, а платформа для регистрации финансовых сделок — это личный кабинет, где хранится информация клиента о сделках как прошедших, так и текущих. Люди часто не помнят, сколько карт у них открыто, какие счета... И такая услуга-подсказка — в одном месте получить всю информацию о себе — будет крайне полезна.

Платформа быстрых платежей. Мы заметно опаздываем в этой области, потому что мировой опыт показывает, насколько быстро такие инфраструктуры становятся востребованными как на уровне клиентов, так и на уровне банков. Мы предлагаем свое решение, то есть возможность

для любого клиента, вне зависимости от того, в каком банке у него счет, переводить деньги по телефону или e-мэйлу. Банки же, предлагая эту услугу через свои порталы и по своим тарифам, будут подключены к общей инфраструктуре. Банковская карта тут — один из инструментов, но точно не единственный.

Национальная система платежных карт. Одна из наших задач — развитие новых инновационных услуг и возможность предоставления клиентам широкого спектра нефинансовых сервисов через программу лояльности, которую мы запускаем в этом году. По этой программе клиенты смогут получать кэшбеки в реальном выражении, а не в баллах. И за два года, с подключением всех участников, как торговых партнеров, так и банков, мы планируем вывести эту систему на качественно новый уровень.

Система передачи финансовых сообщений. Идея в том, чтобы уже на уровне ЕАЭС создать платформу по передаче сообщений между странами. Мы изучаем разные технологии, в том числе рассматриваем и свою, которую разработали на площадке АФТ. Это мастерчейн, переработанная версия, где за основу взят ethereum. Но при этом нам удалось решить несколько задач,

ПРИ РАЗРАБОТКЕ МАСТЕРЧЕЙНА НАМ УДАЛОСЬ РЕШИТЬ НЕСКОЛЬКО ЗАДАЧ, КОТОРЫЕ В ETHERIUM НЕ РЕШЕНЫ. НАПРИМЕР, ПОВЫШЕНИЕ ПРОИЗВОДИТЕЛЬНОСТИ И ВСТРАИВАНИЕ В СИСТЕМУ РОССИЙСКОЙ КРИПТОГРАФИИ

которые в ethereum не решены. Например, повышение производительности и встраивание в систему российской криптографии. Получилась хорошая отечественная разработка, которая может быть использована для многих проектов.

Единая система идентификации и аутентификации (биометрическая платформа). Мы разработали законопроект, и он подписан президентом. Теперь нужно решить две сложные задачи: детально прописать нормативы работы этой платформы и создать приложение, которое можно закатать на смартфон, чтобы через него входить на сайт банка и проводить удаленную идентификацию. При этом интерфейс нужно совместить со всеми элементами безопасности и в то же время сделать дружелюбным для клиента. Вся программа должна заработать в июле 2018 г.

Сквозной идентификатор клиента. В этом вопросе издавна борются две идеи. Первая: создать уникальный идентификатор, к которому будут привязаны все остальные идентификаторы физического лица. Но после анализа множества проблем, с которыми пришлось бы столкнуться, рабочей сегодня является вторая идея. У каждого гражданина уже есть идентификатор: СНИЛС, паспорт, другие документы. Можно связать их внутренним технологическим идентификатором. Человек не будет его видеть, даже не будет его знать, но на уровне системы, вне зависимости от того, с каким документом он пришел в нужную ему организацию, весь профиль клиента становится доступным оператору. Сейчас эта идея детально обсуждается с Минэкономразвития и Минкомсвязи. Этот инструмент может стать одним из элементов единой биометрической платформы.

Платформа для облачных сервисов. Пока это только задача. Тут мы имеем дело с тремя идеями, пришедшими к нам с рынка. Первая: создать юридическое лицо, которое будет заниматься развитием ИБ, выпускать готовые продукты, и потребители, в основном, малые и средние банки, станут их покупать. Вторая: вложиться в инфраструктуру со встроенными элементами ИБ. Третья идея — это полный аутсорсинг, включая IT-разработку, когда участник финрынка является только постановщиком задач.

Пока рынок обсуждает первый и второй варианты: или аутсорсинг продуктов ИБ, или аутсорсинг инфраструктуры со встроенными элементами ИБ. Возможна и комбинация, но пока еще ни одна компания не вышла с предложением взяться за такой проект. И сомнения тут понятны: такой проект потребует больших вложений, глубокого понимания работы рынка, а главное — гибкости при любом изменении в нормативных документах.

Платформа на основе технологии распределенных реестров. О Мастерчейне, как российской разработке, я уже упоминала. Сейчас эта технология запущена в трех проектах: электронные закладные, электронные аккредитивы и гарантии. Подписан закон, который определяет, что электронные закладные могут работать с июля 2018 г. Поскольку юридические нормы уже есть, в июле мы хотим попробовать в не-

СЕЙЧАС МЫ ВЫШЛИ НА УРОВЕНЬ, КОГДА ПРЕДСТАВИТЕЛИ РАЗНЫХ МИНИСТЕРСТВ И БИЗНЕСА СТАЛИ СМОТРЕТЬ НА ВЕЩИ ШИРЕ, МОЖНО СКАЗАТЬ, НАУЧИЛИСЬ ДОГОВАРИВАТЬСЯ

скольких банках аккредитивы и гарантии, а в 2019 г. распространить их на весь реальный сектор.

РАЗВИТИЕ ИБ В КОНТЕКСТЕ ЦИФРОВОЙ ЭКОНОМИКИ

Из пяти направлений программы «Цифровая экономика РФ» три являются наиболее важными для Банка России: нормативное регулирование, информационная безопасность и информационная инфраструктура.

Стоит отметить, что именно в этой точке впервые в нашей стране сделана попытка кросссекторально посмотреть сферы, которые важны для многих отраслей. Например, в части новых технологий у Банка России есть серьезные пересечения с Минкомсвязи. Нам нужно многое обсудить, и мы начали этот непростой процесс. В начале пути, не скрою, было очень сложно, все пытались продвинуть исключительно свои специализированные идеи. Сейчас мы вышли на уровень, когда представители разных министерств и бизнеса стали смотреть на вещи шире, можно сказать, научились договариваться.

Нормативное регулирование сегодня — наиболее продвинутое направление. Тут есть утвержденный план, документы и сроки. Информационная инфраструктура и ИБ находятся в стадии обсуждения и выработки планов. Задачи большие, начиная от выработки подходов к большим данным по стране в целом до определения стандартов по информзащите в части персональных данных.

Представляю основные мероприятия Банка России по направлению «Информационная безопасность»:

- ♦ Развитие нормативного регулирования в области информационной безопасности ЕАЭС;
- ♦ Определение перечня необходимых стандартов обработки массивов больших данных;
- ♦ Совершенствование законодательства в области персональных данных с учетом требований к ИБ;
- ♦ Мониторинг и предотвращение рисков применения перспективных технологий идентификации.

И этот список далеко не полный. Например, важная задача — стимулирование рынка к созданию российской продукции в области ИБ. И в этой области у нас хорошие заделы, на этом поле мы вполне можем конкурировать с другими странами.

* * *

Самое главное, чтобы российская продукция действительно выходила конкурентоспособной и с ценой, приемлемой для рынка.



Сергей КУЗНЕЦОВ
глава направления Gemalto Enterprise & Cybersecurity в России и СНГ

Вопрос о консолидации информации обо всех участниках рынка в рамках создания Финансового Маркетплейса и Платформы регистрации финансовых сделок — это отличная инициатива. Так, в США существует ряд Крупнейших Агентств, называемых «Большой тройкой». Однако стоит помнить об уроках 2017 года. Показательная история Американской компании Бюро Кредитных Историй Equifax, входящей в «Большую тройку», которая была успешно атакована в 2017 году. Представьте компанию, агрегировавшую информацию о более 800 млн частных лиц и 88 млн компаний, которая спустя 4 месяца после инцидента признала компрометацию информации о 145,5 млн клиентов, а также 209 тыс. кредитных карт. В результате расследования выяснилось: эти данные хранились в незашифрованном виде. И эта проблема касается не только Америки, деятельность таких компаний выходит далеко за рамки одной страны. В данном случае компания Equifax вела деятельность на территории РФ, хотя по опубликованной информации скомпрометированные данные касались исключительно граждан США.

Проводя параллели со вступающим в силу законом о Персональных Данных в Европейском Союзе, возникает вопрос об ответственности операторов данных и агрегаторов. Насколько будут защищены интересы и права граждан РФ, и какую финансовую ответственность будут нести создаваемые маркетплейсы и конкретные должностные лица этих организаций?

ЕДИНАЯ СИСТЕМА ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ (БИОМЕТРИЧЕСКАЯ ПЛАТФОРМА)

Решение о создании единой биометрической платформы, с одной стороны, вызывает гордость за такое стремительное появление на рынке и принятие на государственном уровне, с другой — обеспокоенность в связи с угрозой безопасности. Многие развитые страны нахо-

BIS-КОММЕНТАРИЙ

дятся на разных стадиях принятия био-аутентификации. В большинстве случаев мы видим определенную ограниченность использования биометрических платформ для государственных проектов: Био-паспорта, Пограничный контроль, Правоохранительные органы. Каждый такой сценарий имеет скорее замкнутые, изолированные системы с жестко прописанными регламентами по доступу, защите и использованию данных, все эти системы используют специализированное оборудование, созданное для решения конкретных задач.

Представленный подход ЕСИА предлагает использовать смартфоны как неотъемлемую часть процесса идентификации. В обществе уже появилось базовое понимание того, что смартфон — это не только удобное устройство с большим количеством функций, но и прекрасная цель для атаки злоумышленников. Сегодня ни дня не проходит без выявления новых вирусов, разработанных под платформу Андроид. Недавно опубликованная статья о выявленных 45 типах Андроид-устройств, имеющих встроенные уязвимости, это — шок. Платформа Apple не намного безопаснее, просто это закрытая для неспециалистов система, которая также периодически становится объектом атак злоумышленников.

Возвращаясь непосредственно к вопросу массового использования био-аутентификации на уровне страны, хочется обратиться к масштабному международному проекту UIDAI (Unique Identification Authority of India). Это агентство Индии по уникальной идентификации, которое отвечает за эксплуатацию системы электронной идентификации граждан Индии. По информации, ставшей достоянием общественности, в начале 2018 существенная часть базы стала доступна на 200 сайтах страны, а журналистам даже удалось купить всю базу с информацией об 1,3 миллиардах жителей страны за 8 долларов. Развивая эту тему, инструментарий для создания идентификационной карты любого жителя страны на базе похищенной информации стоит какие-то 5 долларов. Переводя этот случай в нашу плоскость, нужно осознавать, что возможность удаленного получения кредита, например, в Сбербанке по био-идентификатору может стать проблемой государственного масштаба.

* * *

В случае с Европейским Союзом и новыми законодательными тенденциями мы понимаем, чем грозит оператору, агрегатору и должностным лицам такая утечка данных. Есть повод задуматься над тем, чем рискуют ответственные руководители системы ЕСИА и государство в целом.



Дмитрий МИХЕЕВ
технический директор
компании «АйТи БАСТИОН»

BIS-КОММЕНТАРИЙ

Чему нельзя возразить, так это обоснованным планам развития финтеха, важности высокоуровневых автоматизированных систем. По опыту, такое развитие непременно изменит принятые методы работы как в части финансовых технологий, так и с точки зрения защиты от рисков ИБ. Уже сейчас описанные в законах требования уходят от примитивных периметровых уязвимостей к целевым атакам на конкретные подсистемы.

Естественно, что для таких атак злоумышленникам требуются специфические знания и опыт, получаемые подчас непосредственно внутри компаний или за счет коллаборации. Очевидно, что вырастут требования к квалификации специалистов ИБ, а также к организации процессов защиты.

Это, с высокой вероятностью, потребует не только проработки требований ИБ на этапе проектирования, но и организации взаимодействия между службами ИТ, ИБ, специалистами по применяемым платформам и государственными регуляторами — не на бумаге, а под конкретные задачи безопасности, в конкретной ситуации и в необходимый момент времени.

Похоже, будет интересно.

Тенденции и перспективы, перечисленные в статье, значительны и вдохновляют. Тем не менее стоит выделить некоторые моменты. Например, некоторую недоработанность законов. Они принимались достаточно долго и все равно конфликтуют с регулируемыми документами, проработка практик их применения сильно запаздывает, стоимость требуемых обязательных мер — совсем не мизерная, и все это вызывает заметное беспокойство у специалистов ИБ и ответственных лиц. Кроме того, данные законодательные инициативы описывают уже сложившиеся в индустрии подходы, и по сути отстали от жизни. Не успев появиться, они уже нуждаются в системных изменениях.

XII ЦИФРОВОЙ ФОРУМ ITSEF

24-25 МАЯ 2018, Казань

itsecurityforum.ru



**> 1000
УЧАСТНИКОВ**



**80
ГОРодОВ**



**> 70 ВЫСТУПЛЕНИЙ
ЭКСПЕРТОВ**



**БОЛЕЕ
25 ПАРТНЕРОВ**



**10 ТЕМАТИЧЕСКИХ
СЕКЦИЙ**



**70 ТЕМАТИЧЕСКИХ
СТЕНДОВ**

ТОЧКИ ОТСЧЕТА

АКТУАЛЬНЫЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПРИОРИТЕТНЫЕ МЕРЫ ПО ПРОТИВОДЕЙСТВИЮ ИНФОРМАЦИОННЫМ УГРОЗАМ В КРЕДИТНО-ФИНАНСОВОЙ СФЕРЕ



**Дмитрий
СКОБЕЛКИН**
заместитель
Председателя Банка
России

В программном выступлении заместителя председателя Банка России Дмитрия Скобелкина на X Уральском форуме обозначены стратегический вектор Банка России и основные направления развития информационной безопасности в кредитно-финансовой сфере в 2018 году. Предлагаем вашему вниманию стенограмму выступления в сокращенном виде.

ГОСУДАРСТВЕННЫЙ ВЕКТОР

В настоящее время вопросам обеспечения информационной безопасности Российской Федерации, в том числе в кредитно-финансовой сфере, уделяется большое внимание со стороны высшего руководства страны (рис. 1).

В соответствии с поручением Президента Российской Федерации от 5 декабря 2016 г. № Пр-2346, распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р утверждена программа «Цифровая экономика Российской Федерации», предусматривающая обеспечение правовых условий, для внедрения и использования инновационных технологий на финансовом рынке, включая совершенствование механизмов предоставления финансовых услуг и обеспечения информационной безопасности.

Одним из направлений программы определена нейтрализация рисков, связанных с киберустойчивостью финансовых организаций.

Обеспечение информационной безопасности финансовых организаций является одним из важных направлений работы Банка России по киберустойчивости.

В Доктрине информационной безопасности Российской Федерации и Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг. отмечается, что в настоящее время информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятель-

ности личности, общества и государства. Их эффективное применение является фактором ускорения экономического развития государства и формирования информационного общества.

Информационная сфера играет важную роль в обеспечении реализации стратегических национальных приоритетов Российской Федерации.

Кроме того, возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличивается число преступлений. При этом методы, способы и средства совершения таких преступлений становятся все изощреннее.

Основными задачами применения информационных и коммуникационных технологий для развития социальной сферы, системы государственного управления, взаимодействия граждан и государства являются совершенствование механизмов предоставления финансовых услуг в электронной форме и обеспечение их информационной безопасности.

Указанные факторы показывают, что обеспечение информационной безопасности и противодействие компьютерным атакам на финансовом рынке, в том числе при внедрении



Рисунок 1. Внимание со стороны высшего руководства страны



Выступление Дмитрия Скобелкина на X Уральском форуме

и использовании цифровых технологий, являются важной задачей государственного уровня.

В процессе реализации национальных интересов в области цифровой экономики предполагается обеспечить с использованием российской национальной платежной системы и элементов информационной инфраструктуры РФ безопасность финансовых операций, а также прозрачность трансграничных платежей (идентификация плательщика, получателя, назначение платежа).

При этом Доктрина информационной безопасности РФ определяет Банк России в качестве органа, входящего в организационную основу системы обеспечения информационной безопасности Российской Федерации, а организации банковских и иных сфер финансового рынка определяются в качестве участников данной системы.

Одним из значимых событий в 2017 г. в области совершенствования системы информационной безопасности стало вступление в силу Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». В соответствии с требованиями указанного федерального закона все информационные и автоматизированные системы, функционирующие в банковской сфере и иных сферах фи-

нансового рынка, относятся к объектам критической информационной инфраструктуры, что напрямую затрагивает все организации кредитно-финансовой сферы. При этом отдельные организации, являющиеся системно значимыми кредитными организациями, операторами услуг платежной инфраструктуры системно и/или социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка, будут отнесены к значимым объектам критической информационной инфраструктуры Российской Федерации. Показатели критериев значимости для организаций кредитно-финансовой сферы будут установлены соответствующим постановлением Правительства Российской Федерации, в основе которых предполагается учитывать среднеедневное количество операций, осуществляемых субъектом критической информационной инфраструктуры.

В соответствии с данными показателями к значимым объектам критической информационной инфраструктуры 3-й категории в кредитно-финансовой сфере могут быть отнесены информационные и автоматизированные системы Банка России, ПАО «Сбербанк», АО «Национальная система платежных карт», Московской биржи, а также других значимых кредитных и финансовых организаций.

За 2017 год было не менее 21 волны атак «Кобальт Страйк»

атакам подверглись более 240 кредитных организаций

успешных атак только 11

8 из 11 организаций являлись участниками информационного обмена

сумма хищений: более 1 млрд 156 млн рублей

ФинЦЕРТ направил индивидуальные предупреждения более чем 400 организациям (из них 240 – участники информационного обмена) с указанием конкретных электронных почтовых адресов организаций, на которые поступали электронные письма группы «Кобальт».



Рисунок 2. Компьютерные атаки преступной группы «Кобальт»

СОЗДАНИЕ ЦЕНТРА КОМПЕТЕНЦИИ

Одним из основных направлений работы Банка России в рамках этого федерального закона является содействие предоставлению данных в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (ГосСОПКА), которая, среди прочего, предусматривает организацию информационного обмена о компьютерных инцидентах между Национальным координационным центром по компьютерным инцидентам и субъектами критической информационной инфраструктуры РФ. По мнению Банка России, указанный обмен целесообразно осуществлять через отраслевой центр ГосСОПКА, функции которого предполагается возложить на Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России (ФинЦЕРТ).

В этих целях Банком России планируется работа по следующим направлениям:

1. Создание Центра компетенции по обеспечению киберустойчивости организаций кредитно-финансовой сферы, основными задачами которыми будут являться:

- ♦ определение потребностей рынка в совершенствовании вопросов киберустойчивости;
- ♦ организация и осуществление информационного обмена о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении финансовых операций по определенной технологии и в установленных форматах электронных сообщений;
- ♦ нормативное регулирование вопросов киберустойчивости финансовых организаций;
- ♦ ведение базы данных о выявленных инцидентах, связанных с нарушением киберустойчивости финансовых организаций;
- ♦ организация и координация работ по совершенствованию форм и методов взаимодействия финансовых организаций по вопросам обеспечения информационной безопасности и повышение их готовности к противостоянию информационным угрозам.

ИНФОРМАЦИОННЫЙ ОБМЕН

Основной задачей Центра компетенции по обеспечению киберустойчивости организаций кредитно-финансовой сферы в 2018 году будет развитие информационного обмена с финансовыми организациями об инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств. С этой целью Банком России проводится следующая работа:

- ♦ по состоянию на 1 февраля 2018 года в информационном обмене с ФинЦЕРТ Банка России на добровольной основе участвует 419 кредитных организаций, 17 небанковских кредитных организаций и 128 некредитных финансовых организаций. Тут ярким

примером служит отражение атак преступной группировки «Кобальт» (рис.2).

- ♦ с 1 июля 2018 года изменениями в Положение Банка России от 9 июня 2012 г. № 382-П устанавливается обязанность операторов по переводу денежных средств и операторов услуг платежной инфраструктуры по осуществлению информирования Банка России по установленной форме о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств;

- ♦ разработан проект стандарта Банка России «Обеспечение информационной безопасности финансовых организаций Российской Федерации. Технология подготовки, направления и форматы электронных сообщений для информирования Банка России о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств», на базе которого в 2019 г. будет разработан и введен в действие национальный стандарт Российской Федерации;

- ♦ на базе ФинЦЕРТ Банка России, как отраслевого центра ГосСОПКА, создается автоматизированная система противодействия хищениям денежных средств на финансовом рынке, с использованием которой планируется осуществлять информационное взаимодействие с Национальным координационным центром по компьютерным инцидентам.

Банк России полагает, что в процессе общественных обсуждений будут выработаны соответствующие подходы по реализации планируемого информационного обмена.

НОРМАТИВНАЯ ПРАВОВАЯ ДЕЯТЕЛЬНОСТЬ

2. Одним из важных направлений работы Банка России по повышению уровня киберустойчивости финансовых организаций, является деятельность по совершенствованию законодательства РФ и развитию методологии обеспечения информационной безопасности финансового рынка РФ.

В этих целях Банком России подготовлены предложения по внесению изменений в действующее законодательство (рис. 3):

	Проект федерального закона № 296412-7 «О внесении изменений в отдельные законодательные акты Российской Федерации (в части противодействия хищению денежных средств)». Основная цель законопроекта заключается в снижении роста числа несанкционированных операций, совершенных с использованием систем дистанционного банковского обслуживания, а также предотвращении потерь кредитных организаций с банковских счетов юридических и физических лиц. ➤ легализация антифрод-систем кредитных организаций; ➤ возврат несанкционированно переведенных денежных средств юридическим лицам; ➤ легализация обмена информацией о компьютерных атаках с использованием сервисов ФинЦЕРТ; ➤ расширение полномочий Банка России по регулированию обеспечения защиты информации на финансовом рынке Законопроект принят Государственной Думой в первом чтении 17 января 2018 года
	Проект федерального закона «О внесении изменений в статью 15¹ Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Цель законопроекта заключается в защите прав и законных интересов граждан Российской Федерации – потребителей финансовых услуг, предотвращении прямых финансовых потерь в результате пользования сайтами сети информационно-телекоммуникационной сети «Интернет», содержащими противоправную информацию, а также повышении доверия к деятельности финансовых организаций и финансовому рынку Российской Федерации в целом. ➤ блокировка по решению Банка России фишинговых сайтов ➤ блокировка по решению Банка России сайтов, предоставляющих финансовые услуги без соответствующей лицензии Банка России Законопроект внесен Министерством связи и массовых коммуникаций Российской Федерации в Правительство Российской Федерации на рассмотрение и согласование
	Проект федерального закона «О внесении изменений в Федеральный закон от 7 июля 2003 года № 126-ФЗ «О связи (в части защиты прав и законных интересов пользователей услуг)». Цель законопроекта заключается в противодействии мошенничеству в сфере дистанционного банковского обслуживания, в том числе при осуществлении операций по переводу денежных средств, а также расширении способов удаленной идентификации при оказании финансовых и иных услуг. ➤ подтверждение принадлежности абонентского номера конкретного клиента кредитной организацией в единой информационной системе Законопроект готов к согласованию с Минкомсвязью

Рисунок 3. Нормативная правовая деятельность

♦ направленных на противодействие хищениям денежных средств (соответствующий законопроект рассмотрен Государственной Думой в первом чтении);

♦ предусматривающих ограничение по требованию Банка России доступа к сайтам в информационно-телекоммуникационной сети «Интернет», используемым с нарушениями законодательства РФ, регулирующего отношения на финансовом рынке, в том числе для совершения мошеннических действий на финансовом рынке;

♦ направленных на противодействие мошенничеству в сфере дистанционного банковского обслуживания и расширение способов удаленной идентификации при оказании финансовых и иных услуг.

Большое внимание Банком России уделяется формированию и совершенствованию комплекса отраслевых документов, устанавливающих требования по обеспечению информационной безопасности и управлению киберрисками, а также состав и содержание технологических, технических и организационных мер, реализующих такие требования.

В дополнение к введенному в действие с 1 января 2018 г. национального стандарта, устанавливающего базовый состав организационных и технических мер защиты информации финансовых организаций Банком России разработан и с 1 июля 2019 года планируется к вводу в действие национальный стандарт, определяющий методику оценки соответствия защиты информации финансовых организаций.

В 2018 году Банком России в рамках Подкомитета № 1 «Безопасность финансовых (банковских) операций» Технического комитета по стандартизации «Стандарты финансо-

вых операций» № 122 планируется разработка проектов национальных стандартов, определяющих:

♦ общие подходы к обеспечению информационной безопасности и управлению рисками реализации информационных угроз;

♦ требования и меры к организации управления инцидентами информационной безопасности.

Кроме того, в 2018 году планируется ввести в действие стандарт Банка России, «определяющий технические форматы электронных сообщений для информирования Банка России о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств», на базе которого в 2019 году будет разработан и введен в действие национальный стандарт, определяющий требования к организации взаимодействия с ФинЦЕРТ Банка России.

Банком России предполагается, что указанные стандарты будут использоваться как основные документы, регламентирующие технические вопросы защиты информации в организациях кредитно-финансовой сферы и методику их оценки. Обязанность применения стандартов планируется обеспечивать путем установления на них нормативных ссылок в нормативных актах Банка России, регулирующих деятельность разных категорий организаций кредитно-финансовой сферы.

В СФЕРЕ ОБРАЗОВАНИЯ

3. Одним из приоритетных направлений работы Банка России в целях повышения киберустойчивости финансовых организаций является совершенствование системы професси-



Рисунок 4. Образование по направлению ИБ в кредитно-финансовой сфере

ональной подготовки специалистов в области обеспечения информационной безопасности в организациях кредитно-финансовой сферы.

В настоящее время высшие учебные заведения, по информации Банка России, не готовят специалистов со специализацией по данному направлению, а проводят обучение в рамках повышения квалификации объемом не более 72 учебных часов, что в современных условиях явно недостаточно.

В качестве первоочередных направлений по подготовке и аттестации специалистов и руководителей подразделений информационной безопасности (кибербезопасности) планируется реализовать в рамках переподготовки лиц с высшим образованием по следующим направлениям:

- ♦ переподготовка специалистов (от 500 учебных часов) — лиц с высшим образованием для цели формирования компетенций, позволяющих полноценно участвовать в процессах обеспечения информационной безопасности и управления киберрисками наравне со специалистами и магистрами, получившими высшее профильное образование в области информационной безопасности в финансовых организациях;
- ♦ переподготовка руководителей подразделений информационной безопасности финансовых организаций (от 500 учебных часов) — лиц с профильным высшим образованием или прошедших переподготовку по направлению «специалист информационной безопасности в финансовых организациях» для цели формирования компетенции, позволяющей организовать работу подразделений информационной безопасности финансовых организаций.

Дополнительно планируется разработать методики и программы тестирования специалистов и руководителей подразделений информационной безопасности (Рис. 4).

Кроме того, Банком России планируется начать разработку профессионального стандарта «Специалист по кибербезопасности» (совместно с Советом по профессиональным квалификациям финансового рынка).

4. Неотъемлемой частью работы по обеспечению киберустойчивости финансовых организаций является кон-

трольно-надзорная деятельность по оперативной и объективной оценке состояния информационной безопасности финансовых организаций.

При этом особое внимание Банк России уделяет вопросам повышения достоверности данных, получаемых в результате контроля вопросов информационной безопасности финансовых организаций. В этих целях планируется:

- ♦ создание системы оценки соответствия информационной безопасности финансовых организаций требованиям национальных стандартов путем проведения внешнего аудита;
- ♦ установить обязанности участников национальной платежной системы по использованию для осуществления

переводов денежных средств прикладного программного обеспечения автоматизированных систем и приложений, сертифицированных в соответствии с законодательством РФ на отсутствие уязвимостей или в отношении которого проведен анализ уязвимостей;

- ♦ развитие вопросов регулирования операционных рисков в части киберрисков финансового рынка в целом на основе метрик (показателей), характеризующих управление киберрисками, а также совершенствование нормативных актов Банка России в части резервирования капитала для обработки операционных рисков.

Для оптимизации и повышения достоверности отчетности, предоставляемой по форме 0403203 «Сведения о выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств», Банком России подготовлены изменения в Указание Банка России от 9 июня 2012 г. № 2831-У, целью которых являются:

- ♦ исключение из отчетности вопросов технической реализации инцидентов защиты информации и реализации сбора информации о технических способах реализации инцидентов защиты информации по каналам взаимодействия, организованным ФинЦЕРТ;
- ♦ установление в новой форме отчетности только экономических показателей;
- ♦ повышение достоверности предоставляемой отчетности, в том числе путем анализа изменений по счетам бухгалтерского учета.

Все указанные направления планируются к детальному обсуждению профессиональной общественностью. Всестороннее обсуждение будет традиционно способствовать определению оптимальных решений, которые в перспективе позволят преодолеть негативные явления, вызванные деятельностью киберпреступников.



**Александр
БОНДАРЕНКО**
технический комитет
по стандартизации
«Криптографическая
защита информации»

ЗАПАС ПРОЧНОСТИ

О ТЕХНИЧЕСКИХ ТРЕБОВАНИЯХ ПО БЕЗОПАСНОСТИ К КОМПОНЕНТАМ ПЛАТЕЖНОЙ ИНФРАСТРУКТУРЫ

В рамках вех, предусмотренных направлением «Информационная безопасность» программы «Цифровая экономика», утвержденной Распоряжением Правительства Российской Федерации от 28 июля 2017 года № 1632-р, предусматривается создание системы стимулов использования национальной платежной системы. Разделом IV программы «Цифровая экономика» определено, что реализация мероприятий должна базироваться на основополагающих принципах информационной безопасности, включающих использование российских технологий и преимущественное использование отечественного программного обеспечения и оборудования, а также технологий защиты информации с использованием российских криптографических стандартов.

ТЕХНИЧЕСКИХ ТРЕБОВАНИЙ ПО БЕЗОПАСНОСТИ

В рамках Плана мероприятий по направлению «Информационная безопасность» программы «Цифровая экономика» предусмотрена разработка технических требований по безопасности к компонентам платежной инфраструктуры (изделиям микроэлектроники, а также всему комплексу средств ИТ и ИБ) на основании гармонизации зарубежных и национальных требований по безопасности (далее — технические требования) в период с января 2018 года по июль 2019 года. Разработка данных технических требований должна быть осуществлена совместными усилиями Минпромторга России (ответственный исполнитель), Минкомсвязи России, ФСТЭК России, ФСБ России и Банка России.

УКАЗАНИЕ БАНКА РОССИИ № 3342-У

В настоящее время требования к информационным технологиям, используемым операторами услуг платежной инфраструктуры, для целей признания платежной системы национально значимой платежной системой, определяются

Указанием Банка России от 25 июля 2014 года № 3342-У (далее — Указание). Данные требования можно логически разделить на следующие группы:

- ♦ требования к разработчикам программных средств;
- ♦ требования к материальным носителям платежных карт;
- ♦ требования к криптографическим модулям, используемым в интегральных схемах платежных карт;
- ♦ требования к процессу изготовления (сборки) платежных карт;
- ♦ требования к значению качественной оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств.

В части материальных носителей платежных карт Указание ссылается на требования национальных стандартов Российской Федерации, разработанных в процессе гармонизации с одноименными международными стандартами ISO/IEC 7810, ISO/IEC 7811 и ISO/IEC 7816. Следует отметить, что некоторые из определенных в Указании национальных стандартов в настоящее время не актуализированы с соответствующими международными стандартами. Например, гармонизация национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 7811-2-2002 датируется 2002 годом, а в 2014 году был разработан новый международный стандарт ISO/IEC 7811-2:2014.

В части криптографической защиты информации в Указании определено, что криптографические модули должны иметь сертификат в системе сертификации федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, и (или) иметь сертификат (сертификаты) соответствия стандартам безопасности не менее двух иностранных платежных систем, в рамках которых осуществляются переводы денежных средств по операциям с платежными картами.

Дальнейшее раскрытие и детализация технических и функциональных требований в части реализуемых механизмов защиты, в том числе криптографических методов защи-

ВЫДВИГАЕМЫЕ В MODULAR SECURITY REQUIREMENTS ТРЕБОВАНИЯ НЕ МОГУТ БЛОКИРОВАТЬ ВСЕВОЗМОЖНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, НО НАПРАВЛЕННЫ НА СНИЖЕНИЕ ВЕРОЯТНОСТИ ТАКИХ УГРОЗ

ты информации, в компонентах платежной инфраструктуры в Указании не производятся.

КОМПОНЕНТЫ ПЛАТЕЖНОЙ ИНФРАСТРУКТУРЫ

Платежная инфраструктура является сложной распределенной информационно-телекоммуникационной системой, объединяющей в себе средства хранения и передачи информации, каналы передачи данных, средства защиты информации и т.д. Некоторые из этих компонентов платежной инфраструктуры обладают встроенными механизмами защиты информации, а некоторые — выполняют только узкоспециализированные функциональные задачи, например, телекоммуникационные или аккумулирующие функции. Рассмотрим наиболее значимые, с точки зрения доступности платежной системы для владельцев платежных карт, компоненты платежной инфраструктуры, которые реализуют криптографические методы защиты информации:

- ♦ платежные карты;
- ♦ POS-терминалы (Point-of-Sale);
- ♦ аппаратные модули защиты (Hardware Security Modules — HSM).

Производство данных элементов осуществляется международными и российскими компаниями. Например, производство платежных карт осуществляется компаниями — Gemalto, АО «НовоКарт» и др., производство POS-терминалов осуществляется компаниями HyperCom, CyberNet, VeriFone и др., производство HSM осуществляется компаниями Gemalto, Thales и др.

Для каждого такого изделия на рынке представлено значительное количество вариантов изделий, производимых различными компаниями. Вместе с тем, некоторые компании осуществляют «крупноузловую» сборку изделия из готовых компонентов (например, некоторые отечественные производители платежных карт), а некоторые компании осуществляют проектирование, разработку и сертификацию конечных изделий, используемых в дальнейшем при производстве.

Разрабатываемое оборудование должно иметь одинаковые интерфейсы для взаимодействия между собой и обеспечения встречной работы, а также иметь заданный уровень защиты информации для обеспечения единого уровня безопасности всей платежной системы в целом, достаточного для противодействия современным угрозам безопасности информации.

ЗАРУБЕЖНЫЕ ТРЕБОВАНИЯ

Технические требования к реализуемым механизмам информационной безопасности и криптографической защиты информации к таким компонентам определяются различными документами по стандартизации, например, Payment Card Industry Data Security Standards (PCI DSS).

Данные стандарты разрабатываются советом — PCI Security Standards

Council. Членами учредителями данного совета являются American Express, Discover Financial Services, JBC International, MasterCard и Visa Inc. Аффилированными членами совета являются региональные и национальные платежные системы — Австралийская платежная ассоциация, Датская платежная ассоциация, Национальная платежная система Индии, а также Национальная система платежных карт (Платежная система «МИР») и другие.

Одним из основных изделий, занимающих ключевую роль в обеспечении конфиденциальности, целостности и/или аутентичности данных финансовых транзакций, является аппаратный модуль защиты — HSM, используемый в составе платежной системы. Логично предположить, что наряду с высокими эксплуатационными свойствами, например, по количеству обрабатываемых транзакций в единицу времени, данный аппаратный модуль защиты должен обладать высокими защитными характеристиками, которые позволяют гарантировать невозможность построения современных атак в отношении него.

В июне 2016 года PCI Security Standards Council опубликовал третью версию требований по безопасности к аппаратным модулям защиты (HSM) — «Payment Card Industry. PIN Transaction Security. Hardware Security Module. Modular Security Requirements» Version 3.0 (далее — Modular Security Requirements). По заявлению авторов Modular Security Requirements, данные требования являются минимально приемлемыми для снижения риска возможности проведения успешных атак. Таким образом, выдвигаемые в Modular Security Requirements требования не могут блокировать всевозможные угрозы безопасности информации, но направлены на снижение вероятности таких угроз и локализации их последствий в случае их успешного проведения.

Основными разделами Modular Security Requirements являются следующие:

Core Requirements («Основные требования»), содержит подразделы:

- ♦ A — Physical Security Requirements («Требования к физической безопасности»);
- ♦ B — Logical Security Requirements («Требования к логической безопасности»);
- ♦ C — Policy and Procedures («Политика и процедуры»);

Key-Loading Devices («Устройства ввода-вывода»), содержит подраздел:

- ♦ D — Key-Loading Devices («Устройства ввода-вывода»);



Remote Administration («Удаленное администрирование»), содержит подразделы:

- ♦ E — Logical Security («Логическая безопасность»);
- ♦ F — Devices with Message Authentication Functionality («Изделия с функцией аутентификации сообщений»);
- ♦ G — Devices with Key-Generation Functionality («Изделия с функцией генерации ключей»);
- ♦ H — Devices with Digital Signature Functionality («Изделия с функцией электронной подписи»);

Device Management Security Requirements («Требования к безопасности устройств»), содержит подразделы:

- ♦ I — Device Security Requirements During Manufacturing («Требования к безопасности изделий в процессе производства»);
- ♦ J — Device Security Requirements Between Manufacturer and Point of Initial Deployment («Требования к безопасности изделий между производителем и местом первоначального развертывания»).

ОТЕЧЕСТВЕННЫЕ ПРИНЦИПЫ

Приказом Федерального агентства по техническому регулированию и метрологии (Росстандарт) от 22 декабря 2017 года № 2068-ст утверждены рекомендации по стандартизации 1323565.1.012-2017 «Информационная технология. Криптографическая защита информации. Принципы

разработки и модернизации шифровальных (криптографических) средств защиты информации» (далее — Принципы), которые вводятся в действие с 1 мая 2018 года. Принципы разработаны на площадке технического комитета по стандартизации «Криптографическая защита информации» (ТК 26), с участием федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, а также организаций членов ТК 26, и аккумулировали и систематизировали накопленный опыт создания и разработки шифровальных (криптографических) средств защиты информации, не содержащей сведений, составляющих государственную тайну (далее — СКЗИ).

Данный документ носит методический характер и содержит в себе принципы, на которых должна основываться разработка и/или модернизация действующих СКЗИ. Настоящие Принципы позволяют сориентироваться и ознакомиться с:

- ♦ проблемами, возникающими при разработке (модернизации) и эксплуатации СКЗИ;
- ♦ правилами классификации классов разрабатываемых СКЗИ, а также совокупностями возможностей, которые могут быть использованы при создании способов, подготовке и проведении атак, для каждого класса защищенности;
- ♦ перечнем необходимых для создания и/или модернизации СКЗИ работ.

СУЩЕСТВЕННЫЕ ОСОБЕННОСТИ

При более детальном рассмотрении Modular Security Requirements и его сравнительном анализе с существующими отечественными нормативно-методическим документами в области криптографической защиты информации, в том числе Принципами, можно сделать несколько существенных замечаний:

1. Некоторые требования, определенные Modular Security Requirements, основаны на американских требованиях FIPS PUB140-2 «Security Requirements for Cryptographic Modules», которые определяют общие требования к СКЗИ, сертифицируемые NIST.

2. Проанализировав структуру Modular Security Requirements, представленную выше, можно сделать вывод о том, что по аналогии с существующей отечественной практикой¹ средства криптографической защиты информации, в том числе, разделяются на средства имитозащиты (подраздел F), средства электронной цифровой подписи (подраздел H) и средства изготовления ключевых документов (подраздел G).

3. При более детальном ознакомлении с Modular Security Requirements и Принципами, нетрудно заметить, что множество требований, определенных Modular Security Requirements, и соответствующее множество, определенное Принципами, в значительной части пересекаются или практически дословно совпадают. Так, например:

♦ требование B6 Modular Security Requirements говорит о том, что устройство должно автоматически очищать или повторно инициализировать свои внутренние буферы, которые хранят конфиденциальную информацию до повторного использования буфера². Пункт 6.1.11 Принципов определяет, что в состав СКЗИ должны входить компоненты, обеспечивающие очистку областей памяти, используемых СКЗИ для хранения защищаемой, ключевой, исходной ключевой и криптографически опасной информации, при освобождении и/или перераспределении областей памяти, путем записи в области памяти случайной информации, вырабатываемой датчиком случайных чисел;

♦ требование B10 Modular Security Requirements говорит о том, что устройство должно использовать разрешенные криптографические алгоритмы, режимы и размеры ключей³. В качестве допустимых к использованию криптографических алгоритмов Пункт 5.1.1 Принципов определяет, что при разработке (модернизации) СКЗИ должны использоваться криптографические механизмы, утвержденные в качестве национальных стандартов Российской Федерации или рекомендаций по стандартизации Росстандарта.

Определенные выше требования достаточно схожи по смыслу и у читателя, возможно, создается ощущение, что

требования Modular Security Requirements не настаивают на использовании каких-либо определенных криптографических алгоритмов. Однако, это заблуждение. В технических комментариях к данным требованиям «Payment Card Industry. PTS HSM Security Requirements. Technical FAQs», опубликованных в июне 2016 года, определяется⁴, что для обеспечения безопасности любых данных приемлемы только криптографические алгоритмы TDES, RSA, ECC, DSA и AES для операций шифрования или формирования/проверки электронной подписи, функции SHA256 или выше могут также использоваться для хэширования. Таким образом, с точки зрения Modular Security Requirements, в качестве разрешенных к реализации в HSM криптографических алгоритмов допускаются к использованию только зарубежные криптографические алгоритмы, некоторые из которых уже давно не обладают «абсолютными» криптографическими характеристиками;

♦ требование B13 Modular Security Requirements определяет, что устройство должно гарантировать, что каждый криптографический ключ используется только для одной криптографической функции⁵. Пункт 5.4.7 Принципов определяет, что для различных криптографических механизмов необходимо использовать различную ключевую информацию;

♦ требование I2 Modular Security Requirements говорит о том, что сертифицированное программное обеспечение должно быть защищено от несанкционированного изменения в течение его жизненного цикла, например, с использованием процедур дублирующего контроля или стандартизированных процедур аутентификации⁶. Пункт 6.1.9 Принципов определяет, что должен быть обеспечен контроль целостности СКЗИ на этапах хранения, транспортирования, ввода в эксплуатацию и эксплуатации всего жизненного цикла СКЗИ, а также контроль целостности среды функционирования СКЗИ на этапе эксплуатации СКЗИ. При этом для СКЗИ, начиная с класса КСЗ, рекомендуется использование криптографических механизмов контроля целостности.

Список пересекающихся требований Modular Security Requirements и Принципов можно продолжить далее. Такие пересечения не ограничиваются приведенными выше несколькими примерами.

4. По мнению автора, Принципы являются более общим документом, так как не ограничивают область приме-

⁴ Q 24. September 2015. What are the algorithms and associated minimum key lengths that are acceptable for use with the default operation of any open protocol used in a HSM? The minimum requirements for cryptographic algorithms use to provide security to any confidential data, including transmitted using open protocols, is specified in DTR B11. Only TDES, RSA, ECC, DSA and AES are acceptable for encryption or signing operations. SHA256 or above may also be used for hashing purposes.

⁵ The device ensures that each cryptographic key is only used for a single cryptographic function.

⁶ The certified firmware is protected and stored in such a manner as to preclude unauthorized modification during its entire manufacturing lifecycle — e.g., using dual control or standardized cryptographic authentication procedures.

¹ Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ — 2005)».

² The device must automatically clear or reinitialize its internal buffers that hold sensitive information prior to reuse of the buffer.

³ The device uses accepted cryptographic algorithms, modes, and key sizes.

ния и форм-фактор разрабатываемых СКЗИ, а требования Modular Security Requirements определяют только требования HSM, предполагаемых к использованию в платежных системах для защиты финансовых транзакций. Поэтому некоторые положения, заданные в Принципах, могут являться либо более жесткими по отношению к аналогичным требованиям, определенными Modular Security Requirements, либо не содержаться в Modular Security Requirements.

СИНТЕЗ МЕХАНИЗМОВ

В части методического обеспечения криптографических решений для платежных систем в рамках Подкомитета 3 «Криптографические алгоритмы и механизмы в национальной платежной системе Российской Федерации» экспертами ТК 26 с 2016 года проводятся работы по синтезу российских криптографических механизмов во всех сегментах платежной системы, а также исследования по их анализу. Решение данной задачи осложнялось отсутствием возможности внесения радикальных изменений в существующие протоколы функционирования платежных систем.

В течение 2016–2017 гг. были предложены соответствующие криптографические механизмы, которые базируются на существующих национальных стандартах в области криптографической защиты информации. В отношении данных решений были проведены необходимые исследования как посредством изучения применимости конкретных классов методов криптографического анализа, так и в парадигме доказуемой стойкости. Данный анализ проводился в моделях нарушителя, релевантных для практики использования разрабатываемых протоколов. Для всех протокольных решений удалось получить полный комплект обоснований, некоторые из полученных научных результатов⁷ докладывались на конференциях РусКрипто 2017 и СТ Crypt 2017.

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

В результате этой деятельности, в конце 2017 года — начале 2018 года ТК 26 был завершен комплекс работ, позволивший своевременно обеспечить утверждение восьми рекомендаций по стандартизации, определяющих наиболее актуальные криптографические механизмы в платежных системах:

- ♦ алгоритмы блочного шифрования при формировании прикладных криптограмм в платежных системах;
- ♦ алгоритмы блочного шифрования при формировании проверочного параметра платежной карты и проверочного значения PIN;
- ♦ функции диверсификации для формирования производных ключей платежного приложения;

⁷ Liliya Ahmetzyanova, Evgeny Alekseev, Grigory Karpunin, Stanislav Smyshlyaev. On cryptographic properties of the CVV and PVV parameters generation procedures in payment systems. СТ Crypt 2017 proceedings, pp. 10–35.

В ОТНОШЕНИИ HSM ПРОЦЕСС РАЗРАБОТКИ ТЕХНИЧЕСКИХ ТРЕБОВАНИЙ ПО БЕЗОПАСНОСТИ ЦЕЛЕСООБРАЗНО ОСУЩЕСТВЛЯТЬ НА ОСНОВАНИИ ГАРМОНИЗАЦИИ ЗАРУБЕЖНЫХ ТРЕБОВАНИЙ И ОТЕЧЕСТВЕННЫХ РЕКОМЕНДАЦИЙ ПО СТАНДАРТИЗАЦИИ

- ♦ режимы алгоритма блочного шифрования в защищенном обмене сообщениями между эмитентом и платежным приложением;
- ♦ алгоритмы согласования ключа и блочного шифрования при офлайновой проверке PIN;
- ♦ режимы алгоритма блочного шифрования в протоколе защищенного обмена сообщениями в процессе эмиссии платежных карт;
- ♦ режимы алгоритма блочного шифрования, алгоритмов электронной подписи и функции хэширования в процедуре офлайновой аутентификации платежного приложения;
- ♦ параметры алгоритмов электронной подписи и функции хэширования в профиле сертификатов открытых ключей платёжных систем.

ГАРМОНИЗАЦИЯ

На основании проведенного анализа, можно сделать вывод, что в отношении HSM процесс разработки технических требований по безопасности к ним целесообразно осуществлять на основании гармонизации зарубежных требований — «Payment Card Industry. PIN Transaction Security. Hardware Security Module. Modular Security Requirements» и отечественных рекомендаций по стандартизации, в том числе — «Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации».

* * *

В заключение стоит отметить, что значительная часть механизмов криптографической защиты информации, реализуемых в современных отечественных HSM, спроектированных и разработанных в соответствии с Принципами, реализована с существенным запасом прочности и потенциально может соответствовать большинству положений международных требований «Payment Card Industry. PIN Transaction Security. Hardware Security Module. Modular Security Requirements». В настоящее время, на отечественном рынке средств защиты информации ряд российских компаний предлагают аппаратные модули доверия — HSM, которые имеют действующие сертификаты соответствия ФСБ России по требованиям к безопасности.

В ПЯТЬ КЛИКОВ

ТЕХНОЛОГИИ СБЕРБАНКА ДЛЯ ДИСТАНЦИОННОЙ РЕГИСТРАЦИИ БИЗНЕСА И ОТКРЫТИЯ СЧЕТОВ



Иван ЯНСОН
бизнес-партнер
по информационной
безопасности Сбербанка

15 февраля 2018 года на Российском инвестиционном форуме в Сочи был запущен в опытную эксплуатацию уникальный сервис полностью дистанционной регистрации бизнеса и открытия счетов в кредитных организациях (далее РБ и ДОС). Он использует квалифицированную электронную подпись, которая формируется и применяется с помощью Специализированной защищенной автоматизированной системы (далее СЗАС). Эту систему разработали Сбербанк и его дочерняя компания «Деловая среда» совместно с 8 Центром ФСБ России при участии других федеральных ведомств и организаций согласно Постановлению Правительства от 29.10.2016 № 1104. В этой статье мы расскажем о том, как создавалась технология, заложенная в основу СЗАС.

ПРОЕКТ И ГОСУДАРСТВЕННЫЕ ЗАДАЧИ

В 2012 году был издан указ Президента РФ от 07.05.2012 № 596 «О долгосрочной государственной экономической политике», который наряду с другими мероприятиями предусматривал улучшение позиции Российской Федерации в рейтинге Всемирного банка по условиям ведения бизнеса со 120-й в 2011 году до 50-й — в 2015 году и до 20-й — в 2018 году. Рейтинг составляется на основании десяти индикаторов регулирования предпринимательской деятельности, один из которых носит название «регистрация предприятий». В 2017 году Россия заняла 28 место в мире по этому показателю. При измерении индикаторов Всемирный банк проверяет, насколько развито законодательство для соответствующего индикатора, а также можно ли это законодательство реально применять на практике.

В 2017 ГОДУ РОССИЯ ЗАНЯЛА 28 МЕСТО В РЕЙТИНГЕ ВСЕМИРНОГО БАНКА ПО УСЛОВИЯМ ВЕДЕНИЯ БИЗНЕСА ПО ПОКАЗАТЕЛЮ «РЕГИСТРАЦИЯ ПРЕДПРИЯТИЙ»

Для улучшения этого индикатора необходимо создать условия, во-первых, для электронной, полностью дистанционной регистрации бизнеса без необходимости очного посещения органов ФНС, и, во-вторых, для дистанционного открытия счетов.

Таким образом, вопрос дистанционной регистрации бизнеса и открытия счёта является вопросом развития экономики в стране в целом, вопросом улучшения макроэкономических показателей страны. Хотя, конечно, нельзя умалять и значение развития такого сервиса для кредитных организаций, так как его внедрение позволит улучшить эффективность процессов открытия счетов и повысить удовлетворённость клиентов.

НОРМАТИВНЫЕ ПРЕДПОСЫЛКИ ПРОЕКТА

Закон «О государственной регистрации юридических лиц и индивидуальных предпринимателей» от 08.08.2001 № 129-ФЗ позволяет дистанционные действия по регистрации предприятий. Согласно пункту 1 статьи 9 указанного закона, «в регистрирующий орган документы могут быть направлены в форме электронных документов, подписанных электронной подписью, с использованием информационно-телекоммуникационных сетей общего пользования, в том числе сети Интернет...». При этом если заявление и документы подписаны квалифицированной подписью, то очный визит в регистрирующий орган не требуется в принципе.

Что касается дистанционного открытия счетов, то открытие счёта без личного присутствия открывающего счёт представителя клиента запрещается законом «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» от 07.08.2001 № 115-ФЗ. Но есть одна оговорка в пункте 5 статьи 7 этого закона, согласно которой личное присутствие не требуется, если ранее этот представитель клиента был идентифицирован при личном присутствии. При этом согласно п. 5.4 этой же статьи 7 для проведения идентификации клиента — юридического лица при открытии ему банковского счёта клиент может направлять документы и сведения в форме



электронного документа, подписанного его квалифицированной электронной подписью. Упомянутые подпункты, позволяющие дистанционное открытие счёта, были специально внесены законом 191-ФЗ от 23.06.2016.

Таким образом, если физическое лицо планирует зарегистрировать бизнес, в котором оно будет единоличным исполнительным органом, ранее стало клиентом банка и было идентифицировано, то потенциально можно открыть счёт соответствующему юридическому лицу без его личного присутствия.

ЭКСПЕРИМЕНТАЛЬНЫЙ СЕРВИС РБИДОС

Исходя из приведённых выше соображений правового характера, Сбербанк совместно с дочерней компанией «Деловая среда» ещё до запуска эксперимента по Постановлению Правительства от 29.10.2016 № 1104, разработал систему РБИДОС. При этом предполагался следующий порядок действий: клиент заходит на портал компании «Деловая среда», регистрируется в личном кабинете и далее выбирает услугу РБИДОС. Далее он вводит личные и паспортные данные, СНИЛС, виды экономической деятельности, указывает систему налогообложения. После этого производится аутентификация клиента с помощью интернет-банкинга для физических лиц Сбербанк Онлайн.

Если аутентификация в Сбербанк Онлайн прошла успешно, то производится сверка персональных данных в заявлении с теми, что соответствуют введённым логину и паролю в Сбербанк Онлайн. В случае совпадения данных клиенту формируется ключ электронной подписи (далее ЭП) и запрос на выпуск квалифицированного сертификата ЭП, который направляется в Удостоверяющий центр. Саму ключевую пару (закрытый и открытый ключи) при этом первоначально планировалось формировать на отдельном сервере электронной подписи (далее СЭП).

Удостоверяющий центр проверяет пользовательские данные (паспорт РФ, СНИЛС, ИНН) через СМЭВ, и в случае положительного результата формирует сертификат квалифицированной электронной подписи.

Подготовленное заявление на регистрацию бизнеса должно быть подписано только что выпущенной электронной подписью. Для подтверждения применения подписи на телефон пользователя предполагалось направлять СМС-сообщение с информацией о заявлении и с разовым паролем для подтверждения этого заявления. Если данные в СМС-сообщении соответствуют заявлению, то клиент вводит СМС-пароль, а СЭП подписывает дистанционной подписью заявление клиента. После этого пользователь оплачивает государственную по-

шлину и услуги и ожидает принятия решения со стороны ФНС¹.

В случае успешной регистрации бизнеса клиент может воспользоваться и услугой дистанционного открытия счёта. Заявление на открытие счёта первоначально планировалось формировать отдельно² там же, в ранее заведённом личном кабинете.

Для подписи этого заявления новоиспечённому ООО или ИП также планировалось формировать квалифицированную ЭП на СЭП. Подтверждение применения ЭП тоже должно было обеспечиваться с помощью разового СМС-пароля.

ОБЛАЧНАЯ ПОДПИСЬ И СЛОЖНОСТИ

Слабым местом в первоначальной схеме реализации РБ и ДОС оказался сервис облачной ЭП — по двум причинам. Первая из них лежит в нормативно-правовой плоскости. Согласно статье 18 закона 63-ФЗ «Об электронной подписи» при выдаче квалифицированного сертификата аккредитованный удостоверяющий центр обязан установить личность заявителя — физического лица, обратившегося к нему за получением квалифицированного сертификата. Заявитель должен предоставить основной документ, удостоверяющий личность (далее ДУЛ) либо его надлежащим образом заверенную копию. Описанная выше аутентификация по паролю в Сбербанк Онлайн является недостаточно надёжной для целей выпуска квалифицированного сертификата ЭП.

Вторая причина невозможности использования облачной ЭП в описанном варианте связана с уровнем безопасности этого сервиса. В нём применение ЭП подтверждается с помощью СМС-паролей, но сейчас нельзя признать такой способ управления ЭП безопасным. Существует ряд атак на этот канал — подмена сим-карты, перехват СМС-сообщений, возможны атаки на сигнальные сети операторов сотовой связи. То есть нельзя быть абсолютно уверенным в том, что СМС-сообщение исходит от владельца электронной подписи, а значит, нельзя быть уверенным в том, что волеизъявление по применению электронной подписи исходит от владельца ЭП.

¹ В итоговой реализации сервиса клиент оплачивает пошлину сразу после ввода данных, необходимых для формирования заявления на регистрацию бизнеса и на открытие счёта, и перед формированием ключей ЭП.

² В итоговой реализации сервиса клиент сразу перед регистрацией бизнеса вводит всю необходимую информацию, и повторно заходить в личный кабинет ему не приходится. Сделано это для уменьшения числа шагов, затрачиваемых на регистрацию бизнеса и открытие счёта.

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА И СЗАС

При обсуждении проблемы на межведомственном уровне был поставлен вопрос о необходимости создания специализированной защищённой автоматизированной системы (СЗАС) для дистанционного применения электронной подписи. Соответствующее решение было закреплено в Постановлении Правительства № 1104 от 29.10.2016 «О проведении в 2016–2018 гг. эксперимента в целях обеспечения направления электронных документов для государственной регистрации юридических лиц и индивидуальных предпринимателей и открытия ими счетов в кредитных организациях...». Участники эксперимента должны были решить следующие задачи:

- ◆ Разработать модель угроз информационной безопасности СЗАС;
- ◆ На основе модели угроз разработать и утвердить временные требования к СЗАС;
- ◆ Создать СЗАС в соответствии с временными требованиями;
- ◆ Провести эксплуатацию СЗАС в течение эксперимента, провести оценку результатов эксперимента и представить соответствующий доклад в Правительство РФ.

При этом СЗАС должна обеспечивать безопасность:

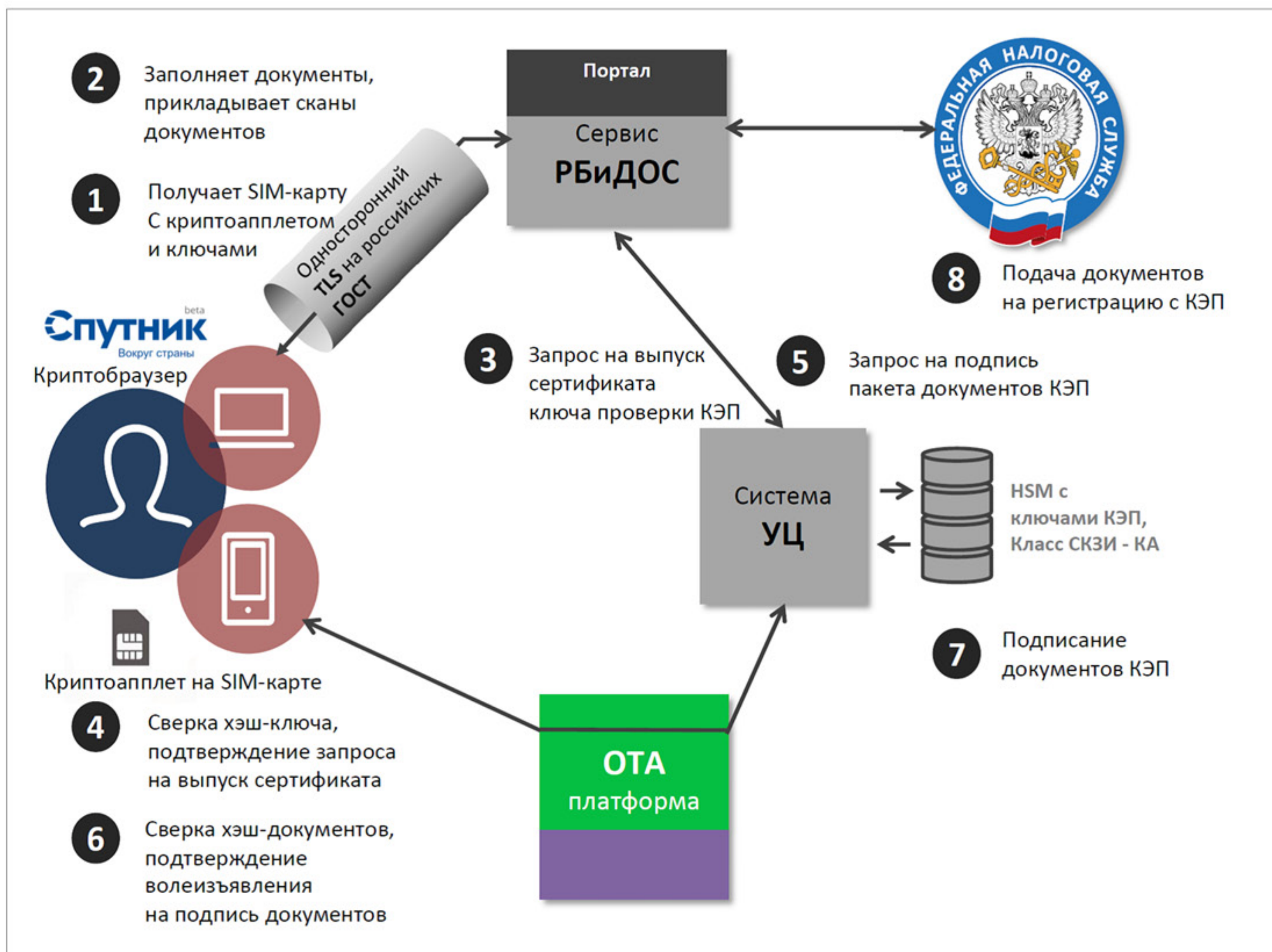
- ◆ при хранении ключей усиленной квалифицированной ЭП (УКЭП);
- ◆ при дистанционной идентификации (аутентификации) владельцев квалифицированных сертификатов ключа проверки ЭП (КСКПЭП);
- ◆ при передаче информации по каналу дистанционного взаимодействия между владельцами КСКПЭП и аккредитованным УЦ;
- ◆ при автоматизированном создании УКЭП по дистанционному поручению владельцев КСКПЭП.

Кроме того, СЗАС должна обеспечивать возможность доказательства неотказуемости владельцев КСКПЭП от поручения на автоматизированное создание УКЭП таких владельцев.

ЗАЩИЩЕННОЕ ВОЛЕИЗЪЯВЛЕНИЕ И ИДЕНТИФИКАЦИЯ

Технология защищённого дистанционного применения ЭП создавалась совместно с сотрудниками 8 Центра ФСБ. При этом нужно было решить две задачи: создание криптографического средства дистанционного управления ЭП и обеспечение надёжной первичной дистанционной аутентификации владельца усиленной квалифицированной ЭП.

По первому направлению было выработано два способа дистанционного управления



ЭП. Первый из них основан на использовании сим-карты со специализированным криптографическим апплетом, второй — на применении криптографического мобильного приложения на смартфоне клиента. В случае СИМ-карты с криптографическим апплетом клиент управляет своей облачной ЭП, находящейся на сервере ЭП, с помощью аутентификационного ключа на СИМ-карте. Этот аутентификационный ключ вместе с криптографическим апплетом должен был бы записываться в банке, и сама СИМ-карта в такой схеме тоже должна была бы выдаваться при личном визите клиента в офис банка.

Формирование и подписание документа со стороны клиента выглядело бы следующим образом. Клиент сначала формирует ЭД на своем ПК, далее этот документ или его хэш передается через ОТА-платформу на смартфон клиента, где ключевые поля документа или его хэш отображаются в апплете. Если значения на ПК и смартфоне совпадают, то клиент нажимает в апплете кнопку «Подписать». Формируется со-

общение о согласии клиента, подписанное ключом аутентификационной подписи, хранящейся на СИМ-карте. Далее оно отправляется через ОТА-платформу на сервер ЭП в банке, где проверяется аутентификационная подпись клиента под сообщением-командой о подписи. Если результат проверки является положительным, то электронный документ подписывается облачной подписью (рис. 1).

ПЛЮСЫ И МИНУСЫ СХЕМЫ «КРИПТОАППЛЕТ НА СИМ-КАРТЕ»

Схема с сим-картой в целом получилась достаточно цельной и логичной, но, к сожалению, не совсем удобной и для клиентов, и для банка: клиентам нужно было бы приходить в банк, а банку пришлось бы обеспечить возможность выдачи сим-карт всех основных операторов связи, чтобы не ограничивать клиентов каким-то одним оператором. Отметим, что в ходе эксперимента межведомственная рабочая группа старалась изучить и современный опыт в других странах. В том числе был рассмотрен опыт

Рисунок 1. Схема «Криптоапплет на сим-карте»

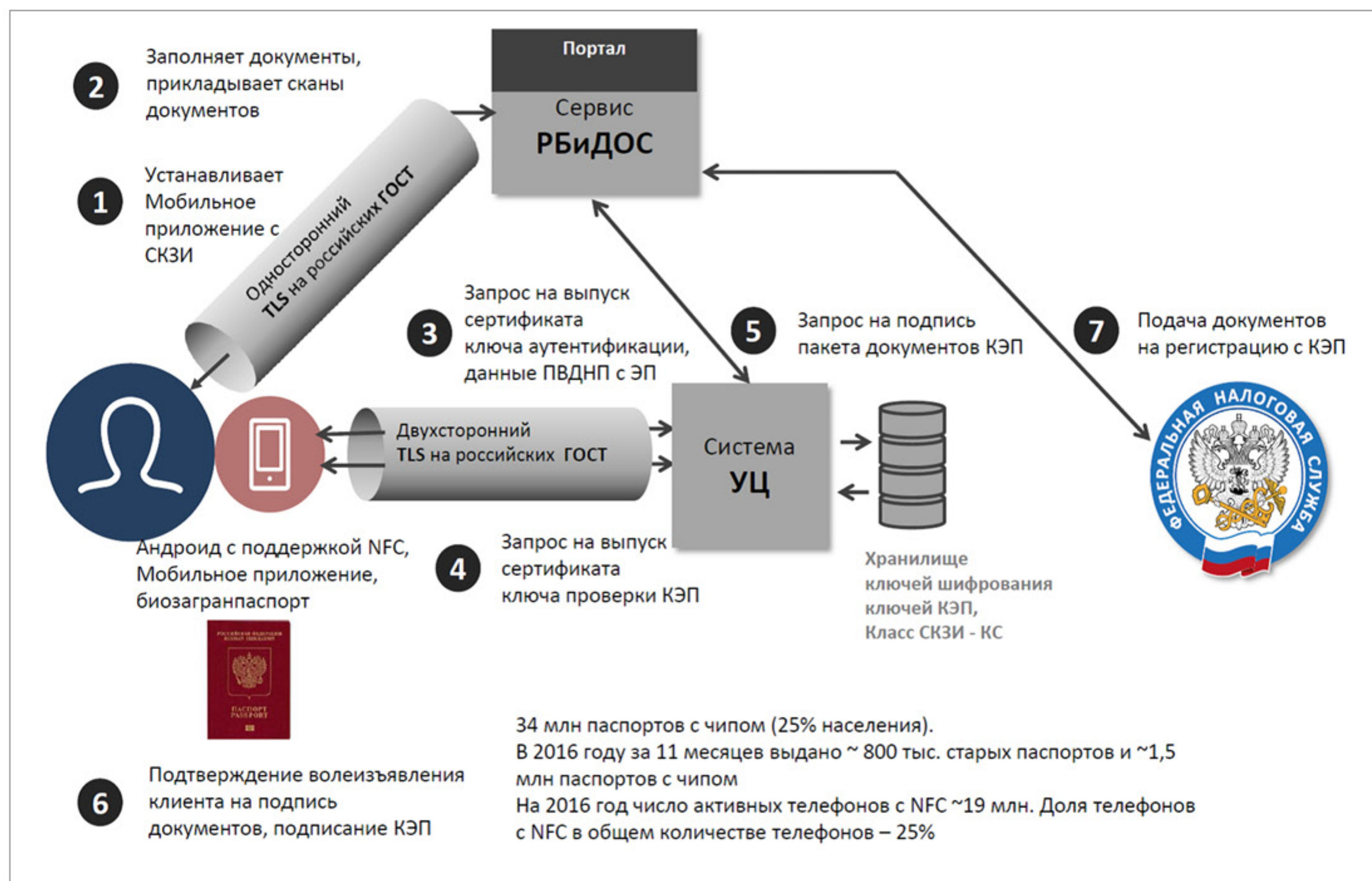


Рисунок 2. Схема «Мобильное приложение с удалённой идентификацией по ПВДНП»

Республики Казахстан, где довольно широкое распространение получили сервисы на основе электронной подписи. Там был проведён эксперимент по внедрению электронной подписи на сим-картах. Однако этот сервис оказался не вполне востребованным — за полтора года эксперимента (с конца 2015 года) было выдано только около тысячи сим-карт с электронными подписями. В связи с этим Сбербанк не стал реализовывать схему «Криптоапплет».

СХЕМА «МОБИЛЬНОЕ ПРИЛОЖЕНИЕ» И ЕЕ ЭВОЛЮЦИЯ

Схема управления ЭП с помощью криптографического мобильного приложения (далее МП) сначала также предполагала использование технологии облачной подписи, управляемой с помощью аутентификационного ключа. Только этот ключ должен был храниться не на сим-карте, а в криптографическом МП, расположенном на смартфоне клиента. В остальном идея похожа на только что рассмотренную для сим-карт. Клиент формирует заявление на регистрацию бизнеса и на открытие счёта на ПК, далее заявление отправляется с сервера в МП на смартфон по защищённому каналу. Заявление отображается в МП, клиент его проверяет, и если результат положительный, нажимает кнопку «Подпи-

сать» в МП. На сервер ЭП уходит подписанное аутентификационным ключом сообщение о согласии клиента использовать облачную подпись. Сервер ЭП проверяет аутентификационную подпись и при положительном результате подписывает облачной подписью ЭД.

В отличие от сим-карты с криптоапплетом МП можно выдать клиенту дистанционно. Клиент может скачать его с выделенных точек дистрибуции, а целостность приложения можно подтвердить с помощью проверки контрольных сумм, опубликованных на сайте банка. Аутентификационный ключ и его сертификат для МП также могут быть сформированы дистанционно.

Для надёжной дополнительной аутентификации клиента при выпуске сертификата квалифицированной ЭП, а также при последующей подписи ЭД указанной квалифицированной ЭП было предложено использовать биометрические загранпаспорта³. Для аутентификации можно с помощью МП по протоколу NFC считать с чипа ПВДНП персональные данные клиента и, во-первых, сравнить их с персональными данными в системе банка, а, во-вторых, проверить подпись под этими данными с помо-

³ Имеются в виду загранпаспорта с чипом на борту, относящиеся к категории паспортно-визовых документов нового поколения (далее ПВДНП).

щью специализированного сервиса⁴ проверки ПВДНП (рис. 2).

Однако для применения этой схемы есть два ограничения. Во-первых, у клиента должен быть ПВДНП и телефон с поддержкой NFC, а, во-вторых, пока речь идет только об операционной системе Android: модуль NFC в смартфонах производства компании Apple используется преимущественно в интересах технологии Apple Pay и недоступен для иных применений. Загранпаспортов нового поколения выдано более 30 миллионов, но всё же указанным требованиям соответствует относительно немного клиентов. Тем не менее схема представляется очень перспективной, так как планируется расширение числа типов ПВДНП и масштаба их распространения. Речь идёт и о водительских удостоверениях с чипом, и о планах по развитию общегражданских биометрических паспортов. Если же компания Apple откроет возможность использования NFC-модуля для мобильного приложения в нашем эксперименте, то схема будет пригодна для большинства потенциальных клиентов.

ХРАНИЕНИЕ КЛЮЧЕЙ ЭП В ОБЛАКЕ VS ОБЛАЧНАЯ ЗАЩИТА КЛЮЧЕЙ ЭП В МОБИЛЬНОМ ПРИЛОЖЕНИИ

Кроме описанных возможностей по созданию полностью дистанционного сервиса РБидОС, исследование схемы с МП дало нам ещё одну интересную возможность, которая и была реализована при внедрении сервиса в опытную эксплуатацию.

При рассмотрении схемы мы поняли, что в мобильном приложении можно хранить сам ключ квалифицированной ЭП, а не аутентификационный ключ. В базовом варианте предполагалось, что ключ КЭП хранится на сервере ЭП, зашифрованный на индивидуальном ключе шифрования в мобильном приложении у клиента. Это было сделано для того, чтобы защитить ключ КЭП клиента на сервере ЭП от несанкционированного использования сотрудниками банка, имеющими доступ к серверу ЭП. Предполагалось, что в момент использования ключа подписи ключ шифрования будет передаваться из МП на сервер ЭП, ключ КЭП будет расшифровываться на этом ключе шифрования на сервере ЭП и использоваться для подписания ЭД. Реализован же был такой вариант: ключ подписи хранится в МП в зашифрованном виде, а ключ шифрования, на котором зашифрован ключ подписи, хранится на сервере. В этом случае, строго говоря, нет об-

ОПЫТНАЯ ЭКСПЛУАТАЦИЯ СЕРВИСА РБидОС ПРОВОДИТСЯ В ТРЁХ РЕГИОНАХ РФ. В МАЕ ПЛАНИРУЕТСЯ РАСПРОСТРАНИТЬ ЭКСПЕРИМЕНТ НА ТЕРРИТОРИЮ ВСЕЙ СТРАНЫ

лачной подписи, а есть облачный сервис по защите клиентских электронных подписей. Для использования ключа подписи МП запрашивает ключ шифрования в облаке и, получив его, расшифровывает хранимый внутри себя ключ подписи и далее применяет его. Такая схема позволяет понизить требования к криптографическому модулю HSM — на нём хранятся только технические ключи шифрования, а обладание ими мало что даёт нарушителю.

ОПЫТНАЯ ЭКСПЛУАТАЦИЯ

В результате эксперимента было создано две технологии защищённого дистанционного управления ключами ЭП, предложена технология дистанционной дополнительной аутентификации клиентов с помощью ПВДНП и на их основе спроектирована технология полностью дистанционного создания квалифицированной ЭП в мобильном приложении, защищённой с помощью облачного сервиса шифрования.

15 февраля была начата опытная эксплуатация сервиса РБидОС и СЗАС в её составе. Входящее в состав СЗАС криптографическое мобильное приложение прошло тематическое исследование и получило положительное заключение ФСБ. Для системы СЗАС 8 Центром ФСБ были разработаны временные требования, и СЗАС была реализована в соответствии с ними.

Опытная эксплуатация сервиса РБидОС проводится в трёх регионах РФ: Калужской, Тверской и Тульской областях. В мае планируется распространить эксперимент на территорию всей страны, а в конце года подвести его итоги.

* * *

Проект поможет решить целый ряд важных задач. Онлайн-регистрация бизнеса и дистанционное открытие расчётного счёта позволят увеличить число малых и средних предприятий в России. Благодаря новым удобным сервисам банк может повысить удовлетворённость своих корпоративных клиентов. И, пожалуй, самое главное — этот проект внесёт свой вклад в выход экономики нашей страны на новый уровень развития.

⁴ В эксперименте используется сервис проверки ПВДН, предоставленный ФГБУ НИИ «Восход».

СЕЛФИ ~~ВМЕСТО~~ ВМЕСТЕ С ПАРОЛЕМ

«РОСТЕЛЕКОМ» РАЗРАБАТЫВАЕТ ЦИФРОВУЮ
ПЛАТФОРМУ УДАЛЕННОЙ ИДЕНТИФИКАЦИИ



Иван БЕРОВ

директор по цифровой
идентичности
ПАО «Ростелеком»,
руководитель
направления
по развитию удаленной
идентификации
и цифровому профилю
Ассоциации ФинТех

1 июля в России будет запущена Единая биометрическая система — цифровая платформа, которая позволит гражданам удаленно открывать счета, вклады и получать кредиты без личного посещения отделения банка. Как биометрия обеспечит цифровое доверие между гражданами и банками? Как система поможет выявлять мошенников и какие новые возможности получат банки? Давайте разбираться.

С БИОМЕТРИЕЙ БЕЗОПАСНЕЕ

Удаленная идентификация для каждого из нас не является чем-то новым: мы давно привыкли получать услуги в «цифре». Каждый день мы вводим пароли для открытия социальных сетей, электронной почты, заказа гаджетов или продуктов питания в интернет-магазинах. Быстро вводя свои персональные данные в формы регистрации, мы мало заботимся об их сохранности и редко интересуемся, какие варианты защиты использует сервис. Как результат — каждый день появляются новости об утечках персональных данных из организаций различного масштаба. Специалисты по безопасности традиционно линчуют пользователей за безответственное отношение к предоставлению своих персональных данных, но давайте подумаем: если система в большинстве случаев работает плохо, где проблема, в пользователях или самой системе? Факты показывают, что в большинстве случаев проблема лежит в подходах к идентификации и аутентификации. Рассмотрим некоторые из них.

Пара «логин-пароль». Из-за сложившейся среди пользователей практики вводить один и тот же пароль на множестве сайтов, записывать пароли на бумажку или сохранять в слабо защищенных системах управления, пара логин/пароль уже давно не является достаточным фактором защиты при проведении важных операций. Мы наблюдаем порочный круг: чем важнее для пользователя сохранность данных, тем более сложный и уникальный пароль к системе он использует и тем в большем количестве

мест он в дальнейшем сохранит запись «логин/пароль» для оперативного доступа к данным. Попыткой повлиять на ситуацию и сделать парольную защиту более эффективной стало изменение в NIST в 2017 году подходов к парольной политике организаций. Однако, повсеместным применение этих правил станет еще нескоро, а повышение защищенности даже после ввода изменений будет не столь значимым.

Чтобы подтвердить личность пользователя в критических системах необходимо использовать многофакторную аутентификацию: такой подход предусмотрен и в недавно вступившем в силу стандарте проведения карточных транзакций PCI DSS 3.2, и в новом гайдлайне NIST, и в ряде других документов и стандартов в области информационной безопасности. Классическая парадигма аутентификации в системе включает три фактора:

- ♦ то, что ты знаешь (например, пароль);
- ♦ то, чем ты владеешь (идентификатор, цифровой сертификат);
- ♦ то, чем ты являешься (биометрические данные пользователя системы).

Усиленная аутентификация пользователя достигается использованием двух или более факторов.

Цифровые сертификаты — надежный метод аутентификации и его легко использовать. Но все же он имеет серьезный недостаток: токен легко украсть или потерять. В результате злоумышленник может так же просто воспользоваться токеном, как его и легальный владелец. Кроме того, сама процедура выдачи и обслуживания цифрового сертификата для доступа к массовым системам является сложной и дорогостоящей.

Проще и дешевле аутентифицировать пользователя в системе с помощью **SMS-кода** или **push-уведомления** в качестве второго фактора. Однако, такие способы подтверждения личности аналитики информационной безопасности считают недостаточно надежными, так как перехватить SMS-сообщения с кодом им удастся в 100% случаев.

Наиболее надежным и простым в использовании способом аутентификации является применение **биометрических данных** вместе с парой логин/пароль. Биометрия при этом является «ключом», который невозможно потерять и крайне сложно подделать.

БИОМЕТРИЯ В МИРЕ

Биометрические системы для идентификации граждан при решении различных государственных задач все чаще применяются по всему миру. Граждане различных стран уже сегодня используют электронные паспорта и визы, цифровые водительские удостоверения и так далее. На 2017 год по оценке J'Son & Partners половина всех проектов по биометрии является государственными. Внедрение биометрических систем позволяет улучшить системы противодействия мошенничеству при пересечении границы, позволяет проводить полноценные электронные выборы. Примерами массового использования биометрии являются национальные программы «биометрической переписи» населения, такие как SIBIOS в Аргентине и Aadhaar в Индии. В последней зарегистрировано свыше 80% граждан страны. Такая высокая глубина проникновения биометрических технологий дает практически неограниченные возможности в создании новых цифровых услуг, биометрические системы становятся плацдармом для создания полноценного цифрового общества.

Параллельно мы наблюдаем рост числа коммерческих проектов с использованием биометрии, в первую очередь — в финансовом секторе, где вопросы эффективного взаимодействия с клиентами и защиты от фрода стоят наиболее остро. По прогнозам J'Son & Partners, к 2022 г. на финансовые организации будет приходиться цифровых сервисов 27,5% против 15% в 2017 году. В целом по оценке аналитиков к 2022 году 2/3 проектов по биометрии будут реализованы в коммерческих целях (рис. 1).

СЕЛФИ ДЛЯ БАНКА

В России, как и во всем мире, финансовый сектор является технологически наиболее зрелым. В последние годы кредитные организации реализовали ряд проектов с использованием биометрии и продолжают активно развивать это направление. Новые системы позволяют кредитным организациям усовершенствовать антифрод-системы и улучшить качество взаимодействия с клиентами банка (например, при работе колл-центров).

В то же время в России применение биометрии в финансовом секторе для привлечения новых клиентов до недавнего времени имело серьезные правовые барьеры: банки не могли дис-

танционно открывать счета, вклады и кредиты. Ситуация в правовом поле изменилась 31 декабря 2017 г.: Президентом РФ был подписан Федеральный закон № 482-ФЗ, который вносит поправки в закон № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». В результате с 1 июля 2018 года банки смогут удаленно идентифицировать граждан на основе их биометрических характеристик и открывать счета без необходимости лично прийти в отделение банка.

Механизм удаленной идентификации очень прост. Чтобы воспользоваться услугами любого интересующего банка, гражданину нужно будет лишь зарегистрироваться в Единой биометрической системе, сдав свои данные (фото и запись голоса) в ближайшем отделении любого банка, использующего Единую биометрическую систему. В дальнейшем на открытие счета в другом банке у гражданина уйдет не более минуты: достаточно будет скачать на мобильное устройство приложение банка, авторизоваться на портале Госуслуг и верифицироваться в Единой биометрической системе, отправив видео со своим изображением и произношением указанных на экране смартфона цифр, и принять условия соглашения с банком (рис. 2).

ПРИНЦИПЫ ПОСТРОЕНИЯ ЦИФРОВОЙ ПЛАТФОРМЫ УДАЛЕННОЙ ИДЕНТИФИКАЦИИ

Чтобы реализовать внешне простой механизм удаленной идентификации, «Ростелеком» разрабатывает цифровую платформу. Драйвером для создания системы стала принятая недавно государственная программа «Цифровая экономика»: повысить доступность цифровых сервисов, обеспечив при этом высокий уровень защиты информации, возможно только внедрив новые принципы предоставления доступа к ус-

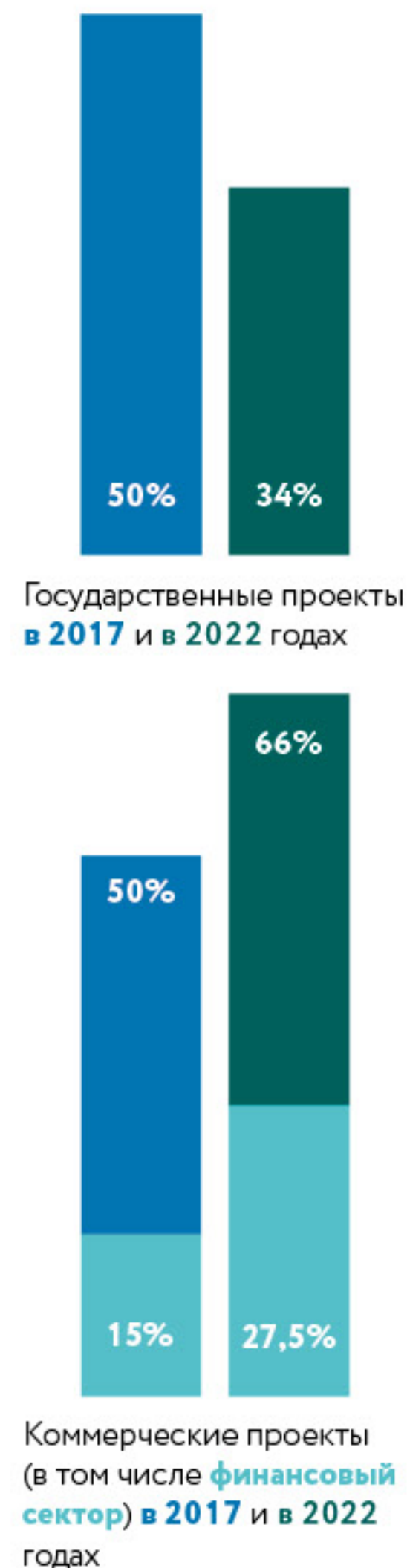


Рисунок 1. Тенденции применения биометрии в мире. Источник: исследование J'son & Partners Consulting, 2017

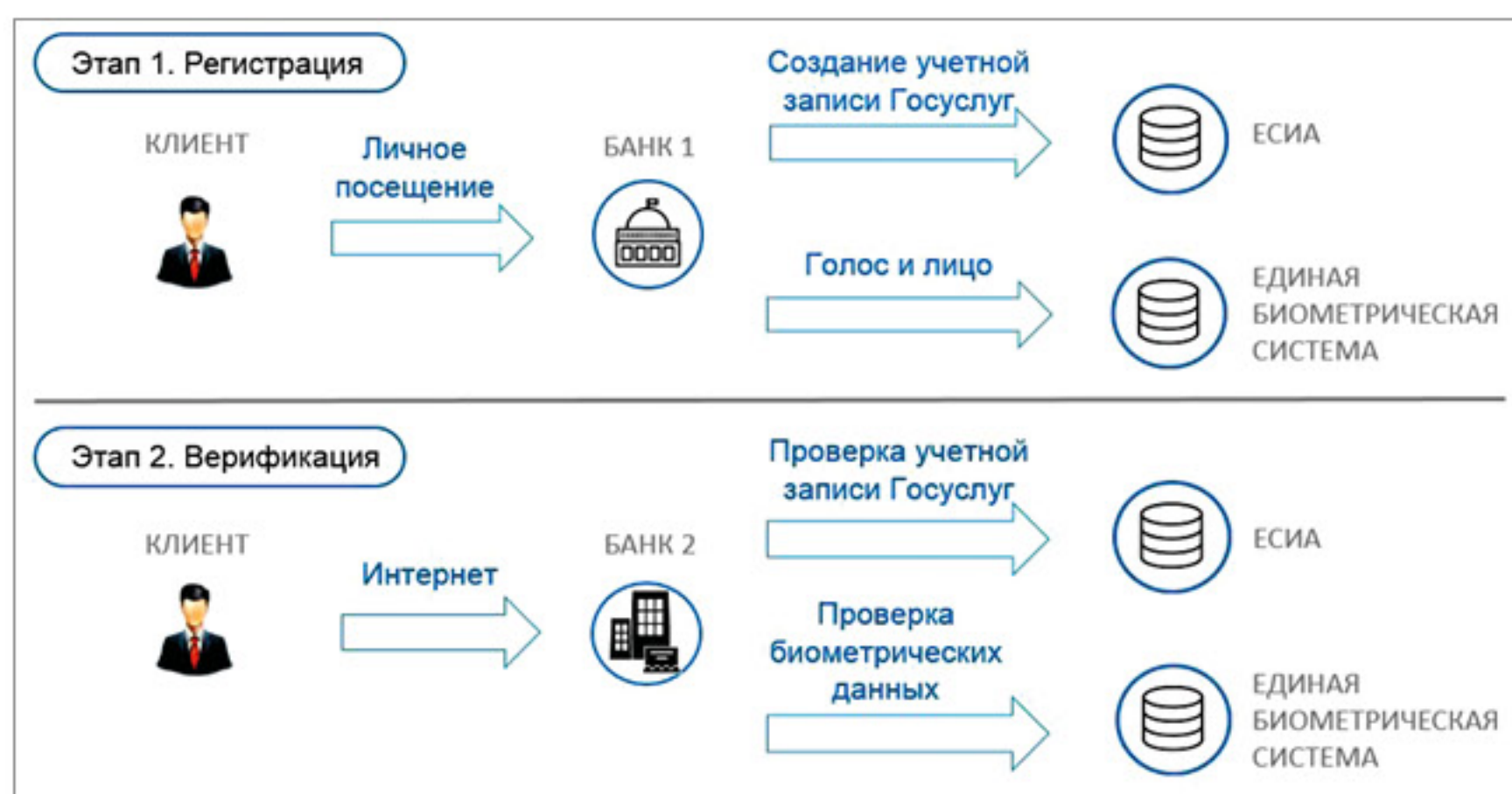


Рисунок 2. Механизм использования Единой биометрической системы

лугам, традиционно реализуемым в ходе личного визита гражданина в организацию. Единая биометрическая система по сути является сквозной технологией, которая может быть применена в любой отрасли экономики.

Чтобы сделать Единую биометрическую систему максимальной удобной и обеспечить высокий уровень безопасности, в платформе заложен ряд принципов.

Мультимодальность. Для проекта выбраны два типа биометрии: голос и лицо, причем не по отдельности, а вместе, поскольку две модальности позволяют определить «живого человека», а не имитацию его биометрии в цифровом канале. Лицо и голос — самые доступные и распространенные технологии на сегодняшний момент. Идентификация по рисунку вен, сетчатке глаза или отпечатку пальцев требует наличия специального считывающего оборудования, недоступного в массовом сегменте. Стоит отметить, что доступность технологий на сегодняшний день не является ограничивающим фактором для их применения в будущем. В перспективе в платформу можно будет добавить и другие модальности.

Мультивендорность. К участию в проекте привлечены ведущие российские разработчики в области биометрии, их программные продукты по результатам независимых международных тестов занимают призовые места. В рамках каждой модальности Единая биометрическая система работает с технологиями нескольких вендоров. Лучшие технологии на текущий момент выбираются на основе открытого тестирования по методике, разработанной Русским биометрическим обществом. Такой подход позволяет обеспечить лучшее распознавание биометрии сейчас и в будущем. Единая биометрическая система — это открытая платформа, присоединиться к ней могут любые вендоры биометрии и на любом этапе, если качество работы их алгоритмов будет соответствовать заданным нами критериям.

Liveness. Способность детектировать подделку вместо «живого человека» — это одна из ключевых возможностей Единой биометрической системы. В цифровой платформе комбинируются различные методы детектирования и определяются лучшие из них на текущий момент времени; в клиентском сценарии различные методы динамически комбинируются. Результатом такого подхода становится выявление мошеннических действий при использовании системы и возможность оперативного реагирования на них.

Выявление аномалий. Единая биометрическая система сможет не только определять мо-

шенников во время удаленной идентификации, но и усилить банковские системы защиты от фрода. Каждый пользователь обладает определенным профилем поведения: об этом говорят параметры его устройства, данные о местоположении, информация о проводимых ранее процедурах верификации в Единой биометрической системе и т.д. Чтобы с высокой точностью определять, какое поведение является аномальным, Единая биометрическая система использует технологии машинного обучения и анализирует подробные сведения о действиях и операциях.

Безопасность данных. Безопасности данных в Единой биометрической системе уделяется особое внимание. «Ростелеком» является одним из лидеров на рынке кибербезопасности, поэтому система будет обеспечена высоким уровнем защиты. Важным является и то, что данные в Единой биометрической системе хранятся в обезличенной форме и отдельно от персональных данных, включенных в базы ЕСИА (Единая система идентификации и аутентификации). Связка между системами осуществляется по уникальному идентификатору. Для защиты от MITM-атак биометрические данные гражданина в Единую биометрическую систему будут передаваться по защищенному отечественными криптоалгоритмами каналу связи. Для этого «Ростелеком» разрабатывает специальное мобильное приложение со встроенными криптографическими средствами защиты информации.

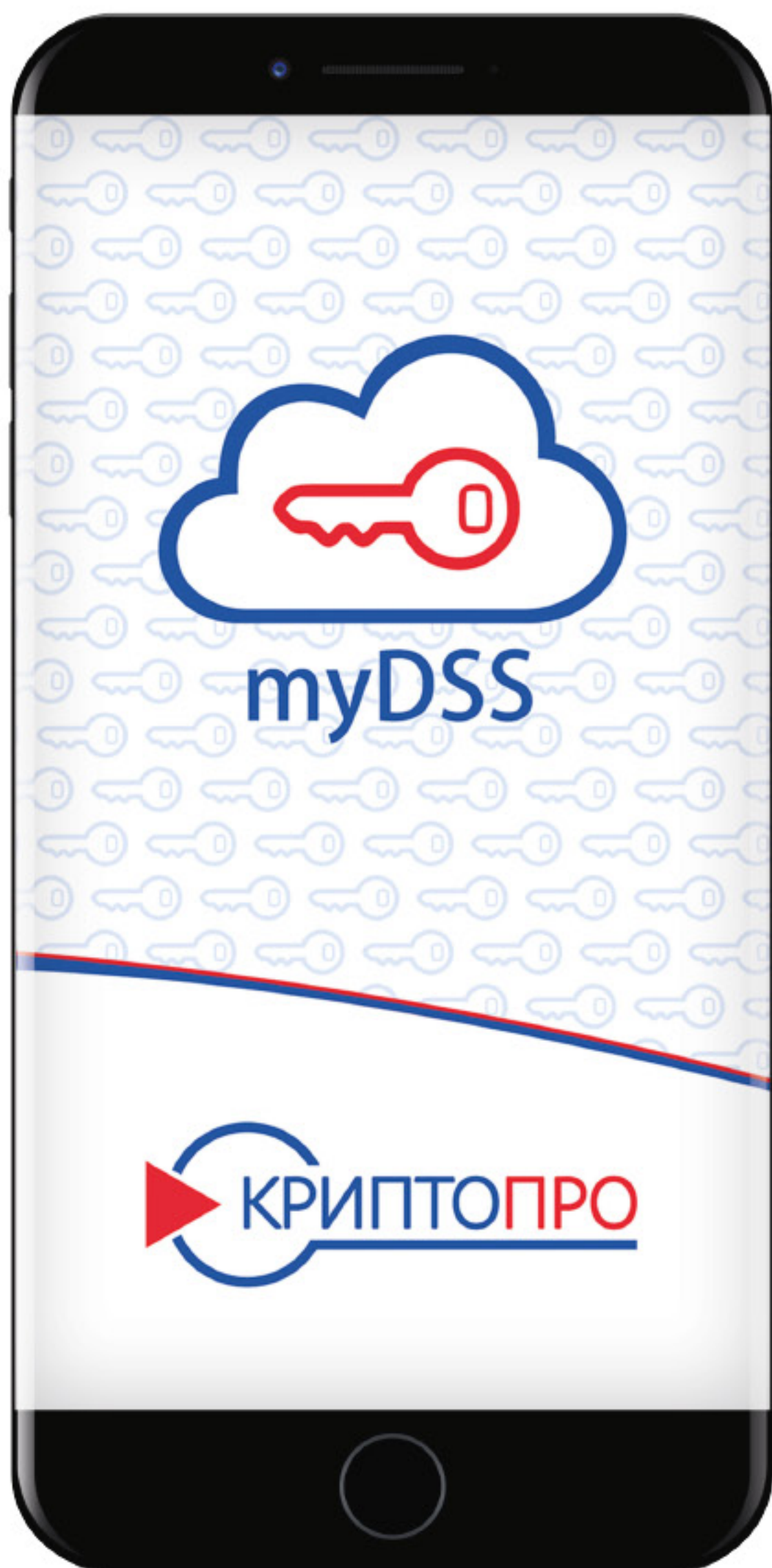
Обеспечить безопасность биометрических данных и выявлять мошеннические действия — важные аспекты работы Единой биометрической системы, но при этом очень важным является и тот факт, что использование биометрии не отменяет необходимости выстраивать эшелонированную систему защиты в банке или любой другой организации, которая планирует использовать Единую биометрическую систему.

* * *

Единая биометрическая система — один из первых шагов к построению цифровой экономики России. Задача системы — дать равный доступ к цифровым услугам гражданам, проживающим во всех регионах страны и людям с ограниченными возможностями. Мы создаем платформу для безопасной удаленной идентификации, которая позволит не просто открывать счета в банках. В будущем эта система станет основой для получения любых цифровых услуг — государственных, муниципальных, коммерческих — удаленно, «не вставая с дивана», что значительно повысит качество жизни каждого из нас.



КриптоПро myDSS



Квалифицированная электронная подпись в системах электронного документооборота при помощи смартфона.

Мобильное приложение myDSS является частью решения КриптоПро DSS и позволяет обеспечить строгую аутентификацию пользователя и контроль подписываемых документов.

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

Что такое myDSS

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

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

Безопасность

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

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

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

Юридическая значимость подписи

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

КриптоПро myDSS

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

РИСК- ОРИЕНТИРОВАННАЯ АУТЕНТИФИКАЦИЯ

ПУТЬ СБЕРБАНКА



Задача аутентификации пользователей информационных систем и клиентов при доступе к банковским сервисам — одна из самых традиционных и по-прежнему востребованных в области обеспечения информационной безопасности.

КЛЮЧЕВОЕ НАПРАВЛЕНИЕ

Согласно ежегодному исследованию компании Verizon «Data Breach Investigations Report», в 2015 году скомпрометированные учётные записи стали причиной 50% всех взломов информационных систем и утечек данных. Это число выросло до 66% в 2016 году и до 81% — в 2017 году. Показателен пример со взломом в прошлом году компании Equifax, в результате которого киберпреступники получили доступ к данным 143 млн человек. Последствием был уход из компании ряда топ-менеджеров, подача исков к компании и падение котировок акций на 35%, что привело к снижению капитализации на \$4 млрд.

Таким образом, развитие технологий и сервисов аутентификации, адекватных непрерывному росту киберугроз и при этом удобных для клиентов, — одно из ключевых направлений деятельности любой современной финансовой организации.

Традиционные способы решения задачи аутентификации начинаются от методов парольной аутентификации в различных модификациях (статические текстовые или графические пароли, одноразовые пароли через СМС-сообщения, программные и аппаратные генераторы) до многофакторной аутентификации, включающей комбинацию факторов аутентификации категорий «То, что ты знаешь» (Something You Know), «То, что ты имеешь» (Something You Have), «То, чем ты являешься» (Something You Are).

КАК НАЙТИ БАЛАНС?

Классическая парольная аутентификация уже давно не считается надёжной и повсеместно вытесняется многофакторной аутентификацией. Однако эта парадигма защиты основана на статических правилах и приводит к жёстким ограничениям вне зависимости от личности клиента и реальных рисков. Например, каждый раз при входе в интернет-банк клиенту необходимо вводить логин/пароль и одноразовый пароль, полученный в СМС-сообщении или от аппаратного генератора. Это требование не зависит от устройства и места, с которого осуществляется вход. Кроме того, при подтверждении перевода клиент должен всегда вводить одноразовый пароль, даже если это

регулярный перевод своему родственнику или партнёру.

Каждая организация сталкивается с одной и той же дилеммой: как найти баланс между удобством для клиента и надёжностью? В этой статье мы хотели бы поделиться опытом Сбербанка в решении этого вопроса.

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ

Риск-ориентированная модель аутентификации (RBA — risk-based authentication) решает проблему противоречия между безопасностью и удобством. Необходимость аутентификации, набор и тип факторов, требуемых для аутентификации данного клиента, определяются на основе оценки риска события и клиента «здесь и сейчас». Таким образом, процесс аутентификации адаптируется под клиента, его окружение и устройство. При высоком уровне доверия к этим факторам процедура аутентификации вообще незаметна (по сути, это просто идентификация) или минимальна для клиента. В случае выявления риска клиент должен пройти аутентификацию с применением одного или нескольких факторов, а при высокой вероятности фрода доступ к сервисам будет полностью заблокирован.

Такой адаптивный подход позволяет снизить действующие ограничения на выполнение высокорисковой операции при помощи метода повышения уровня доверия (Step-up authentication). Например, если вход в систему интернет-банка осуществляется с известного устройства, из типичного для клиента места, а система узнаёт клиента по клавиатурному почерку, то есть по тому, как он набирает символы, то для входа клиенту достаточно просто ввести свой логин.

Если платёж выполняется из личного кабинета, то дополнительное подтверждение при низкорисковой операции, например, если это налоговый платёж или регулярный платёж родственнику, не требуется. Дополнительное подтверждение с помощью одноразового пароля или биометрии может потребоваться, если клиент переводит деньги новому получателю.

Этот подход обеспечивает необходимый уровень информационной безопасности и удобен для клиентов, поэтому эксперты ожидают, что такие технологии появятся в составе комплексных решений кибербезопасности уже в 2018 году.

БОЛЬШЕ ТЕХНОЛОГИЙ

Для полноценного применения риск-ориентированного подхода требуется набор факторов аутентификаций. Традиционные факторы ау-



Александр БРОДСКИЙ
управляющий директор Центра
внутрикорпоративного взаимодействия
Сбербанка

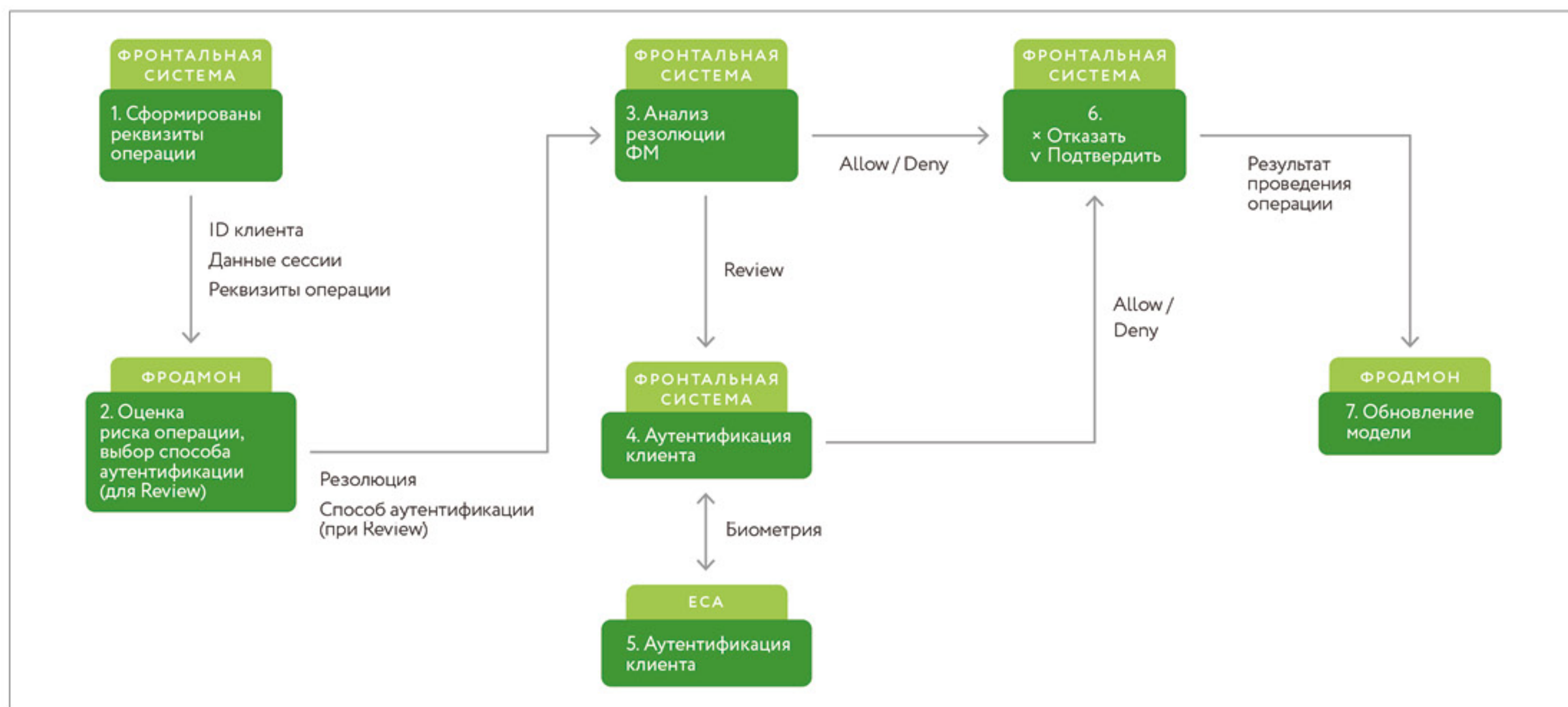


Рисунок 1. Step-up аутентификация (ЕКА — Единый сервис аутентификации)

тентификации не отличаются большим разнообразием — это пароли и контрольные вопросы, различные PKI-токены и генераторы одноразовых (OTP — One Time Password) паролей. При этом факторы аутентификации, основанные на знании, на текущий день признаны неэффективными и непривлекательными для клиента, а всевозможные токены имеют слишком большие накладные расходы, чтобы применять их широкомасштабно.

Развитие и распространение технологий распознавания человека по персональным физическим или поведенческим признакам существенно расширяют возможности при проектировании современной риск-ориентированной системы аутентификации.

Биометрические факторы аутентификации в отличие от традиционных, основанных на знании и владении, нельзя разгласить, потерять или передать другому лицу. Однако биометрические технологии — это не «серебряная пуля» в вопросе надёжности аутентификации. И дело даже не в ошибках первого (отказать своему) и второго (принять чужого за своего) рода при распознавании. Вопрос скорее в рисках, связанных с доверием к каналу обслуживания, в котором осуществляется снятие биометрических данных в момент биометрической верификации или регистрации.

Такие риски возникают в первую очередь для удалённых каналов обслуживания, когда считывателем биометрических характеристик выступает неконтролируемое банком мобильное устройство клиента, и процесс снятия биометрических характеристик также не контролируется банком. В этих условиях могут быть

реализованы различные атаки по подмене биометрических характеристик, что требует применения специальных методов выявления таких атак (так называемый PAD — Presentation Attack Detection).

ПУТЬ СБЕРБАНКА

Риск-ориентированная аутентификация в концепции Сбербанка предполагает, что у любого фактора аутентификации есть уровень доверия, а выбор фактора аутентификации зависит от уровня риска события или операции.

При формировании уровня доверия к фактору аутентификации учитываются различные аспекты, например: канал регистрации, способ аутентификации, который был пройден при регистрации, тип фактора. В частности, Американский институт стандартов и технологий (NIST) собирает и систематизирует опыт такой оценки в документе SOFA-B (Strength of Function for Authenticators — Biometrics). В нашей модели уровень доверия фактора аутентификации — динамическая величина, которая зависит от статистики успешных/неуспешных входов и транзакционной активности клиента с использованием данного фактора аутентификации.

Для вычисления уровней риска событий и уровней доверия факторов аутентификации Сбербанк использует внедрённую в банке систему фрод-мониторинга на базе продукта RSA Adaptive Authentication & Transaction Monitoring. Это кросс-канальная система, которая подключена ко всем каналам банковского обслуживания. Фактически, это базовый уровень многофакторной, риск-ориентированной системы аутентификации.

Пример того, как данная связка может использоваться в процессе дополнительной step-up аутентификации, приведён на рисунке 1.

Вместе с тем система фрод-мониторинга анализирует в основном транзакционную активность клиента, поскольку её главной целью является выявление финансового фрода. Поэтому необходимо дальнейшее развитие модели риск-ориентированной аутентификации, учитывающей и другие параметры работы клиента в системах банка.

ДАЛЬНЕЙШИЕ ПЛАНЫ РАЗВИТИЯ РВА В СБЕРБАНКЕ

Мы планируем реализовывать многоуровневую модель риск-ориентированной аутентификации, оценивающую событие входа клиента в систему банка по пяти доменам (рис. 2).

Каждый уровень этой модели должен повысить надёжность процесса аутентификации. Их группировка выглядит следующим образом:

Уровень 1 — анализ окружения и устройства доступа (Endpoint):

- ◆ геолокация устройства и проверка его цифрового отпечатка (Geolocation & Device Fingerprinting);
- ◆ выявление факта использования устройства ботом (Bot Detection);
- ◆ оценка безопасности устройства (Mobile Security Assessment);
- ◆ построение профиля использования телефона (Phone-Printing).

Уровень 2 — поведение и биометрия (Behavioral & Biometrics):

- ◆ оценка сессии работы с системой (Session Behavior);
- ◆ проверка физиологических и биологических характеристик субъекта (биометрии) (Face, Voice, Fingerprint Biometrics);
- ◆ проверка личностных поведенческих характеристик субъекта (Behavioral Biometrics).

Уровень 3 — анализ данных о пользователе (User Data):

- ◆ внешних (не хранящихся в банке) персональных данных, обработка которых регулируется законодательством (External Personal Identified Information — PII);
- ◆ внешних персональных данных, не относящихся к категории регулируемых законодательно (External Non-PII personal);
- ◆ данных социальных сетей (External Social Network);
- ◆ внутренних баз данных (Internal Records).

Уровень 4 — связи и аналитика (Linkages & Analysis):

- ◆ анализ поведения и выявление в нем аномалий (Behavioral Analysis & Anomaly);



Рисунок 2.
Многоуровневая модель аутентификации

- ◆ выявление групповых связей (Detection Individual and Peer Group);
- ◆ применение аналитических методов и машинного обучения (Advanced Analytics and Machine Learning);
- ◆ анализ взаимосвязей (Graphs and Link Analysis).

Важная особенность поведенческой биометрии заключается в том, что проверка происходит не однократно на входе, а постоянно в течение сессии. При этом доверие к обычной биометрии находится на высоком уровне только в момент проверки. С течением времени этот уровень падает (за компьютером может находиться уже не тот субъект, который прошёл аутентификацию при входе). При проведении поведенческой биометрии всё наоборот — уровень растёт по мере наблюдения за субъектом на всем протяжении сессии.

Мы ожидаем, что при реализации данного многоуровневого подхода большая доля операций аутентификации будет осуществляться без вовлечения клиента. Анализируя уровни надёжности аутентификации и риска события, мы получаем возможность реализации различных сценариев. Например, вход в систему для клиента может быть простым и прозрачным, однако при совершении рискованной операции могут потребоваться дополнительные действия для прохождения Step-up аутентификации дополнительным фактором.

* * *

Таким образом, это позволит достичь того самого баланса между удобством для клиента и надёжностью с точки зрения безопасности, о котором мы говорили в начале статьи.



Матвей ГЕРИНГ
директор SWIFT
по Центральной
и Восточной Европе

ПРОГРАММА БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЕЙ SWIFT

УСИЛЕНИЕ БЕЗОПАСНОСТИ ФИНАНСОВОЙ ЭКОСИСТЕМЫ

Как глобальный кооператив, SWIFT стремится играть значительную роль в поддержке своих пользователей и сообщества. В 2016 году SWIFT представил Программу безопасности пользователей (CSP) — специализированную программу поддержки клиентов в усилении безопасности их инфраструктуры, связанной со SWIFT. Программа работает эффективно, но, поскольку пользователям SWIFT предстоит повторно пройти аттестацию и подтвердить полное соблюдение обязательных элементов контроля безопасности до конца 2018 года, стоит о ней напомнить.

Программа CSP включает в себя обязательные элементы контроля безопасности пользователей, новые сервисы, помогающие пользователям предотвращать и обнаруживать мошенническую деятельность, а также инициативы по обмену информацией в рамках всего сообщества для усиления защиты посредством обмена разведывательными данными.

Программа CSP устанавливает ряд ключевых сроков по обеспечению соблюдения обеспечения контроля безопасности клиентов и связанных с ними действий:

31 декабря 2017 г. — первоначальный срок, в течение которого все пользователи SWIFT должны были самостоятельно подтвердить свой уровень соблюдения обязательных элементов контроля безопасности.

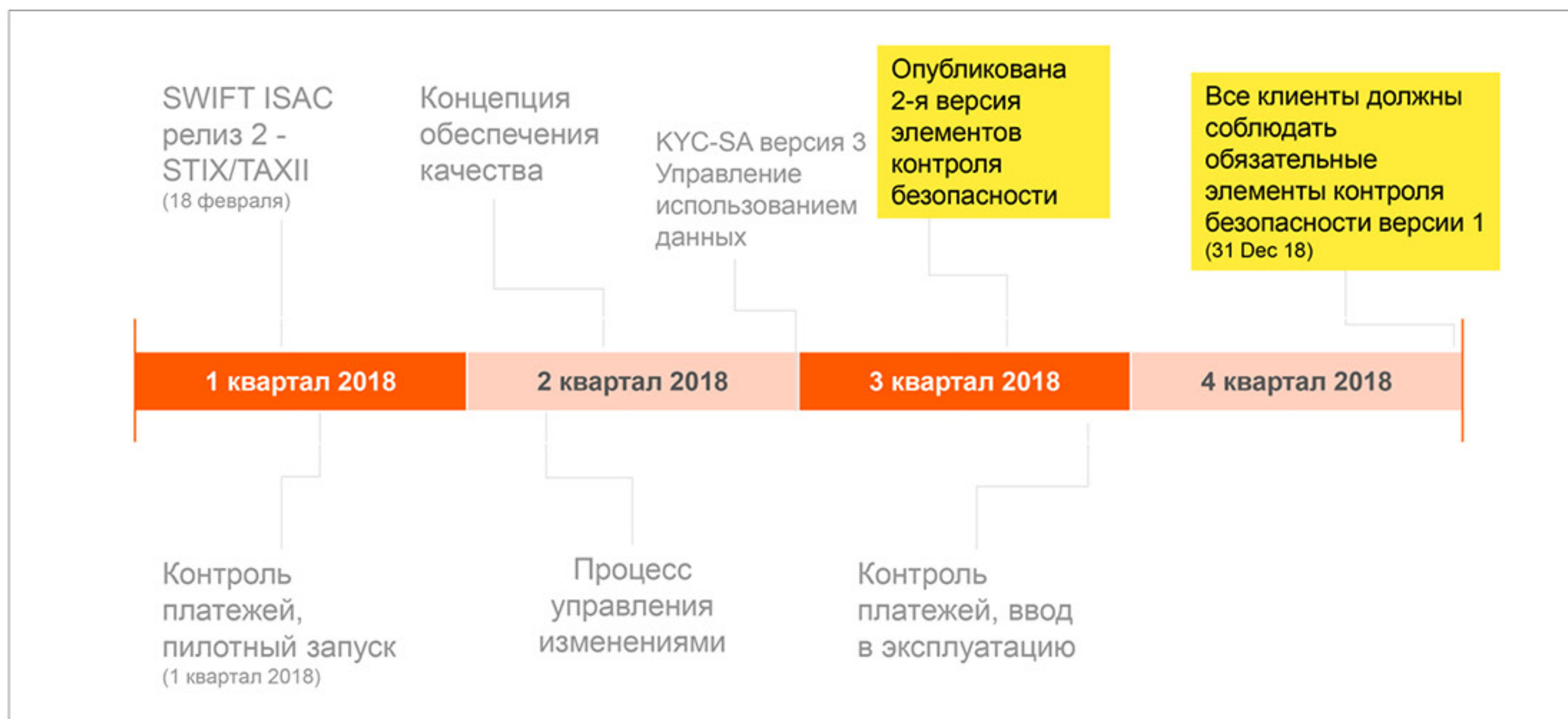
1 января 2018 г. — с января 2018 г., SWIFT оставляет за собой право сообщать о пользователях, которые не предоставили данные по самоаттестации.

31 декабря 2018 г. — крайний срок для всех пользователей повторной аттестации и подтверждения полного соблюдения обязательных элементов контроля безопасности.

1 января 2019 г. — с января 2019 г. SWIFT оставляет за собой право сообщать о пользователях, которые не обеспечили несоблюдение всех обязательных элементов контроля безопасности (или которые подключены через не

Рисунок 1. Развитие CSP. Основные этапы в 2017 г.





соблюдающих их сервис-провайдеров), в течение следующих двух лет.

ТРИ ВЗАИМОДОПОЛНЯЮЩИЕ ОБЛАСТИ

Программа CSP охватывает три ключевых аспекта: безопасность и защита локальных сред пользователей, предотвращение и обнаружение мошеннических действий при взаимодействии с контрагентами и совместную работу в сообществе для предотвращения будущих кибератак.

Вы — безопасность и защита

Основополагающая идея CSP заключается в том, чтобы каждая организация обеспечивала защиту своей локальной среды, включая физическую защиту локальной инфраструктуры, связанной со SWIFT. Идея также включает в себя формирование соответствующих политик и практик по предотвращению кибермошенничества. Нарушения в локальной инфраструктуре стали общей отправной точкой для известных кибератак.

Чтобы помочь клиентам соответствовать своим требованиям безопасности, SWIFT внедрил в свое программное обеспечение новые функции по обеспечению безопасности, такие, как обязательное использование двухфакторной аутентификации (2FA), и будет продолжать делать это (внедрять новые функции) в рамках планов развития своих продуктов. SWIFT также продолжает выпускать регулярные обновления для системы безопасности продуктов SWIFT и планирует делать это на ежеквартальной основе. SWIFT разработал документацию по обеспе-

чению безопасности для каждого из своих интерфейсов, включая расширенные руководства, опубликованные для Alliance Access и Entry, для Alliance Lite2 и для сертифицированных интерфейсов сторонних производителей. Целью этого обновления является дальнейшее обеспечение безопасности и эффективности сервисов SWIFT для наших клиентов в будущем. Оно будет применяться для продуктов Alliance Access, Alliance Entry, Alliance Gateway, Web Platform Server-Embedded и SWIFTNet Link.

Ваши контрагенты — предотвращение и обнаружение

Даже при наличии усиленных мер безопасности следует понимать, что злоумышленники могут действовать весьма изощренно, поэтому крайне важно управлять рисками безопасности при взаимоотношениях с контрагентами для того, чтобы свести к минимуму риски, связанные с потоками платежей. Необходимы действенные меры предотвращения и обнаружения наряду с основными положениями из передового опыта в области обеспечения безопасности в организации.

Существует ряд мер, которые пользователи SWIFT могут предпринять, и которые помогут им управлять рисками безопасности в отношениях с контрагентами, что поможет предотвратить и выявить случаи мошенничества.

♦ RMA: Сервис по управлению взаимоотношениями SWIFT (Relationship Management Application — RMA) поддерживает пользователей, позволяя им контролировать взаимоотношения с контрагентами через SWIFT, предоставляя предварительную проверку транзакций, ко-

Рисунок 2. Развитие CSP. Предъявляемые результаты в 2018 г.



Рисунок 3. Payment Controls Reports. Возможности

торая предотвращает их несанкционированное получение. SWIFT предлагает ряд продуктов и сервисов, помогающих финансовым учреждениям оптимизировать использование RMA и RMA Plus для лучшего понимания, управления и смягчения операционных рисков, а также рисков, связанных с несоблюдением требований и мошенническими действиями.

◆ **Daily Validation Reports** (Ежедневные отчеты по валидации): Этот сервис призван помочь учреждениям усилить существующие механизмы контроля мошенничества, предоставляя простые и независимые средства проверки обмена сообщениями. Ежедневные отчеты по валидации — это вторичные средства контроля мошенничества для проверки транзакционной активности и обеспечения целенаправленного наблюдения за большими, необычными и новыми потоками платежей. Отчеты доступны на следующий день.

◆ **Рыночная практика:** Рыночная практика играет важную роль в регулировании взаимоотношений между контрагентами. Информационный бюллетень SWIFT «Снижение риска мошенничества за счет усиления контроля операций по платежам», подготовленный в 2016 году, подчеркнул необходимость изучения подтверждений сообщений и выписок на конец дня, а также изложил передовой опыт по проверке расчетных инструкций и изменению платежных инструкций. Впоследствии в 2017 году Группа по анализу практики платежного рынка (Payments Market Practice

Group — PMPG) разработала Рекомендации по рыночной практике для осуществления отмены подозрительных мошеннических транзакций.

◆ **Payment Controls Reports** (Сервис контроля платежей): В 2018 году SWIFT запустит новый сервис контроля платежей для дополнения и усиления существующих у клиентов механизмов по контролю мошенничества. Новый сервис по предотвращению мошеннических действий и киберпреступлений позволит пользователям SWIFT отфильтровывать платежные сообщения в соответствии с выбранными параметрами, что даст им возможность незамедлительно обнаруживать любые необычные потоки сообщений прежде, чем они будут переданы. Изначально этот сервис предназначен для небольших учреждений, мелких дочерних предприятий крупных учреждений и центральных банков. Он будет запущен как общедоступное решение, доступ к которому пользователи SWIFT получат мгновенно и без установки оборудования, программного обеспечения или сопровождения.

Ваше сообщество — обмен информацией и готовность

Финансовая индустрия является глобальной, как и кибервызовы, с которыми она сталкивается. Кибератаку на одну организацию в одном месте, мошенники могут повторить где угодно в другом месте, поэтому важно заняться обеспечением безопасности в киберпространстве, объединив усилия глобального сообщества. SWIFT представил специализированную команду «Cus-

tomers Security Intelligence team», которая распространяет самую актуальную обезличенную информацию о показателях компрометации (Indicators of Compromise — IOCs) и подробно рассказывает о методах, используемых в известных атаках. Такое информирование уже внесло ощутимый вклад в борьбу с мошенничеством.

SWIFT представил «SWIFT ISAC» — Глобальный информационный портал для обмена подробными техническими разведывательными данными, чтобы дать финансовому сообществу возможность защитить себя, предпринять смягчающие меры и предотвратить дальнейшие атаки.

SWIFT регулярно информирует своих пользователей о соответствующих киберразведанных, новых рыночных практиках и рекомендациях. В частности, SWIFT построил сеть CISO и сотрудничает с сообществом CISO для расширения сотрудничества и обмена информацией.

Кроме того, SWIFT работает с партнерами — экспертами в области кибербезопасности для проведения исследований постоянно меняющихся киберугроз. Одним из таких примеров является совместный доклад SWIFT и BAE Systems, выпущенный в январе 2018 года, который содержит достоверную информацию, полученную в результате экспертных исследований кибератак на пользователей во всем мире, иллюстрирующий сложность и изощренность тактик и методов злоумышленников, а также подтверждающий положительное влияние Программы безопасности пользователей SWIFT. В докладе описывается, как за последние 18 месяцев произошла значительная эволюция киберугроз, стоящих перед глобальной финансовой индустрией, поскольку злоумышленники значительно продвинулись в своих знаниях.

ПРЕВОСХОДНАЯ РЕАКЦИЯ СООБЩЕСТВА

В конце 2017 года SWIFT сообщил, что 89% всех пользователей SWIFT подтвердили свой уровень соблюдения обязательных элементов контроля безопасности к обозначенному крайнему сроку — 31 декабря 2017 г. В совокупности эти учреждения обеспечивают более 99% всех сообщений FIN, отправляемых через сеть SWIFT.

Этот процент подтверждения в России еще выше благодаря поддержке со стороны локального сообщества, в частности РОССВИФТ и Центрального банка Российской Федерации, которые действовали максимально скоординировано с момента запуска программы CSP. С тех пор количество аттестаций продолжило увеличиваться, поскольку несколько сотен

организаций впоследствии подтвердили свои аттестации или находятся в процессе их подтверждения.

Такая превосходная реакция — по сегментам, рынкам и типам инфраструктуры — демонстрирует стремление финансовой индустрии к борьбе с постоянной угрозой кибератак.

Реакция сообщества на прохождение этого первого этапа процесса аттестации была чрезвычайно позитивной и позволила повысить уровень безопасности пользователей SWIFT, поскольку они теперь будут знать больше о своих контрагентах. Однако предстоит еще проделать значительную работу по дальнейшему совершенствованию системы безопасности и повышению прозрачности в финансовом сообществе. Например, в случае значительного качественного изменения, всем пользователям SWIFT необходимо будет повторно пройти аттестацию и подтвердить полное соблюдение обязательных элементов контроля безопасности до конца 2018 года. Начиная с 1 января 2019 года SWIFT вновь оставляет за собой право уведомлять местные надзорные органы о тех пользователях, которые не прошли переаттестацию или не подтвердили полное соблюдение обязательных элементов контроля в течение требуемого периода. После этого аттестацию необходимо будет проводить на ежегодной основе.

Пользователям SWIFT также предлагается начать включать данные аттестации своих контрагентов в процессы управления рисками и принятия бизнес-решений, наряду с другими факторами риска, такими как KYC, санкции и AML. Используя приложение по аттестации безопасности на базе платформы KYC Registry (KYC-SA), пользователи могут делиться своими аттестационными данными с контрагентами и запрашивать такие данные у других контрагентов. Это дает организации возможность быть прозрачной в отношении своего статуса аттестации, что должно повысить доверие и уверенность для контрагентов, ведущих бизнес друг с другом.

* * *

Прозрачность, которую обеспечивает эта система обмена данными с контрагентами, способствует прохождению аттестации и соблюдению элементов контроля, поскольку учреждения стремятся продемонстрировать уровень кибербезопасности своим контрагентам. SWIFT представит дополнительные меры для обеспечения постоянства качества и эффективности аттестаций безопасности пользователей в 2018 году.



Антон СВИНЦИЦКИЙ
директор по консалтингу
АО «ДиалогНаука»



Игорь ТАРВИ
ведущий архитектор систем безопасности
АСУ ТП АО «ДиалогНаука»

БанКИИ

ВСЕ БАНКИ ЯВЛЯЮТСЯ СУБЪЕКТАМИ КИИ
И ПОДПАДАЮТ ПОД ДЕЙСТВИЕ ФЕДЕРАЛЬНОГО
ЗАКОНА № 187-ФЗ

Летом прошлого года Государственная Дума приняла федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры» (КИИ), который вступил в действие первого января текущего года. В нем установлены требования по обеспечению безопасности значимых объектов КИИ (ЗОКИИ). Причем в определениях закона указывается двенадцать сфер деятельности, объекты которых могут быть отнесены к ЗОКИИ. Следует отметить, что финансовая сфера полностью и банки в частности подпадают под действие этого закона и являются субъектами КИИ.

КРИТИЧЕСКАЯ ИНФРАСТРУКТУРА

Закон № 187-ФЗ причисляет к критической информационной инфраструктуре все предприятия из указанных сфер деятельности. Относится или нет конкретное предприятие к одной из сфер определяется по ОКВЭД, который заполняется при регистрации предприятия, по полученным компанией лицензиям, а также по уставным документам. Однако обязательные требования к защите информации предъявляются только к ЗОКИИ, хотя владельцы незначимых объектов также должны исполнить ряд требований закона, например, в ча-

сти подготовки перечня объектов КИИ и выполнения процедуры их категорирования.

Также в законе устанавливаются два Федеральных органа исполнительной власти (ФОИВ): один отвечает за безопасность объектов КИИ, в том числе за определение требований по защите информации для объектов КИИ, а второй — за поддержание работоспособности государственной системы обнаружения и предотвращения компьютерных атак (ГосСОПКА) на объекты КИИ. В соответствии с подписанными в конце прошлого года указами первым ФОИВ стала ФСТЭК России, которая в результате получила полномочия устанавливать требования по информационной безопасности для объектов КИИ и осуществлять контроль, а вторым — ФСБ России.

Таким образом, в законе есть две ветки требований: обеспечения безопасности объектов КИИ, контролировать которую будет ФСТЭК России в рамках своих полномочий, и взаимодействия с ГосСОПКА с соблюдением всех регламентов. С точки зрения взаимодействия с ГосСОПКА для кредитно-финансовых организаций предполагается, что оно будет осуществляться через ФинЦЕРТ, который по факту будет являться ведомственным центром ГосСОПКА.

ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА № 127-ПП

В начале 2018 года было принято Постановление Правительства № 127-ПП, которое определяет процедуру проведения категорирования объектов КИИ. То есть описанные в нем правила позволяют определить, относится ли объект КИИ к ЗОКИИ или нет. Постановление описывает три категории значимости — от первой до третьей (первая наивысшая) — на основании которой и определяется базовый состав мер обеспечения информационной безопасности, необходимый к реализации субъектами КИИ. Категория значимости определяется по степени ущерба в пяти критериях значимости: социальной, политической, экономической, экологической и значимость для обеспечения обороны страны, безопасности государства и правопорядка. Таблица соотнесения показателей критериев значимости объектов КИИ и категории значимости находится в приложениях к постановлению.

Для проведения процедуры категорирования объектов КИИ нужно создать специальную комиссию, сформировать перечень объектов КИИ, определить процессы, происходящие на объектах, выявить информационные системы, которые поддерживают эти процессы и оценить ущерб, который может быть

нанесен в случае нарушения и (или) прекращения функционирования информационной системы. На процедуру категорирования отводится ровно год со дня формирования и утверждения субъектом перечня объектов КИИ. Результатами этой деятельности должны стать документы о присвоении категорий значимости объектам КИИ, которые необходимо направить во ФСТЭК для регистрации в реестре ЗОКИИ. Первая плановая государственная проверка соблюдения требований по информационной безопасности может быть проведена через 3 года после регистрации объекта в реестре. Впрочем, возможны внеплановые проверки после зафиксированных инцидентов.

Чтобы объект был признан не значимым, нужно провести полноценную процедуру категорирования, пройти по всем типам ущерба и показать, что ни по одному из них он (объект) не может соответствовать указанным в постановлении уровням ущерба. Эти документы также нужно будет подготовить для ФСТЭК России, которая может и не согласиться с выводами комиссии. Однако именно не значимые объекты КИИ освобождаются от соблюдения требований приказов ФСТЭК России № 235 и № 239 в соответствующих законах № 187-ФЗ сферах деятельности, но могут ими руководствоваться при определении требований к системе защиты информации и при построении такой системы защиты.

Процедура категорирования может проводиться банками самостоятельно, либо для этого могут привлекаться сторонние компании, имеющие необходимые лицензии ФСТЭК России.

ПРИКАЗЫ ФСТЭК РОССИИ

В рамках реализации требования закона № 187-ФЗ ФСТЭК России разработала пять приказов, которые определяют различные аспекты обеспечения защиты значимых объектов КИИ — от формы представления результатов в Службу до правил ведения реестра ЗОКИИ.

Ключевыми являются два приказа: № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Рос-

ПЕРВАЯ ПЛАНОВАЯ ГОСУДАРСТВЕННАЯ ПРОВЕРКА СОБЛЮДЕНИЯ ТРЕБОВАНИЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МОЖЕТ БЫТЬ ПРОВЕДЕНА ЧЕРЕЗ 3 ГОДА ПОСЛЕ РЕГИСТРАЦИИ ОБЪЕКТА В РЕЕСТРЕ

сийской Федерации и обеспечению их функционирования» и № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». Первый относится к субъектам, а второй — к объектам. Первый определяет обязанности владельцев ЗОКИИ по построению службы информационной безопасности, которая будет обеспечивать контроль ИБ всех критических объектов. Второй же устанавливает требования к самим системам защиты, которые обеспечивают безопасность объектов критической инфраструктуры от целенаправленных атак и управляются службами ИБ.

ФСТЭК России отмечает, что строить параллельную структуру для соответствия требованиям приказа № 235 не нужно. Важно только, чтобы служба ИБ занималась именно защитой, а не техническим сопровождением ИТ и другими не свойственными ей обязанностями. Впрочем, для защиты можно привлекать и сторонние организации, которые имеют соответствующие лицензии на предоставление услуг по защите информации.

Требования приказа № 239 определяют меры, которые необходимо будет выполнить для защиты объектов КИИ. При этом сертификация средств защиты в явном виде не требуется и может быть заменена процедурой оценки соответствия. Она необходима только при условии, что ИС является государственной (в соответствии с требованиями закона № 149-ФЗ). Однако же оценка эффективности средств защиты должна быть проведена в любом случае. В частности, ее можно провести в виде приемочных испытаний. Фактически этот приказ определяет минимально необходимый уровень безопасности для

всех предприятий России, и исполнение этих требований должно повысить уровень защищенности всего российского бизнеса.

ГОССОПКА И ФИНЦЕРТ

Вторая часть закона № 187-ФЗ относится к построению системы обнаружения вторжений и взаимодействию с распределенной системой ГосСОПКА. К счастью, банкам не нужно взаимодействовать с ГосСОПКА напрямую — взаимодействие может происходить через ведомственный центр, который получил наименование ФинЦЕРТ. Ранее он функционировал в рамках предписаний Центробанка, а теперь получает более высокий статус. Естественно, взаимодействие с ним будет обязательным как минимум для тех банков, которые будут признаны ЗОКИИ.

В настоящее время Центробанк ведет работу по значительному расширению возможностей по взаимодействию банков через ФинЦЕРТ как в части информирования об инцидентах, так и в части процессов расследования и реагирования на них.

На сегодняшний день важно отметить, что все банки являются субъектами КИИ и подпадают под действие Федерального закона № 187-ФЗ. В первую очередь банки должны составить перечень объектов КИИ и провести процедуру их категорирования в соответствии с требованиями Постановления Правительства № 127. Несмотря на то, что на эту процедуру формально отводится один год, с нашей точки зрения лучше уже сейчас начать планировать данные работы.

Андрей ФИЛАТОВ
генеральный директор
IBM в России
и странах СНГ

IBM ВЫСТРАИВАЕТ АЛЬЯНСЫ И РАЗВИВАЕТ
ЭКСПЕРТИЗУ В ОТДЕЛЬНЫХ РЕГИОНАХ



Переход к цифровой экономике предполагает накопление данных о клиентах, их предпочтениях и поведении, совершённых сделках и используемых продуктах. В современном бизнесе обладать наиболее полной информацией о потребителях и иметь к ним постоянный доступ — одно из ключевых конкурентных преимуществ. Компании, которые владеют такими данными, способны предложить клиенту оптимальные продукты и услуги. С другой стороны, всё больше организаций понимают важность обеспечения защиты информации.

Но так как с каждым годом характер угроз и атаки киберпреступников становятся все более изощренными и приобретают глобальный масштаб, предприятиям все сложнее в одиночку справиться с этой задачей.

Согласно исследованию IBM и Ponemon Institute, средний объем потерь компаний от утечки данных составляет \$3,62 млн на один инцидент. По мнению аналитиков, в течение следующих пяти лет количество инцидентов в системе защиты увеличится вдвое¹. При этом сложность кибератак также продолжает расти. Злоумышленники масштабируют наиболее успешные вредоносные программы и внедряют их на международном уровне.

Чтобы иметь эффективный арсенал средств информационной защиты, нужны огромные человеческие ресурсы для отслеживания стабильного функционирования системы информационной безопасности. Более того, быстро меняющийся ландшафт угроз в сфере ИБ требует от компаний постоянного экспертного анализа, а это в свою очередь требует подключения профессионалов. Поэтому компании все чаще обращаются в специализированные фирмы, которые предоставляют услуги в области кибербезопасности.

Такой подход продиктован реалиями цифровой среды, а вовсе не маркетинговыми ходами. По результатам другого исследования IBM, команды по обеспечению ИБ ежедневно отфильтровывают свыше 200 тыс. инцидентов в системе защиты. Более 20 тыс. часов в год уходит на обработку ложных угроз². В этих условиях особенно остро стоит необходимость внедрения средств искусственного интеллекта в системы информационной безопасности.

На рынке уже представлено множество услуг и продуктов для защиты с использованием технологий ИИ. У меня не вызывает никаких сомнений тот факт, что за этими технологиями будущее. Такие решения обречены на использование во всех отраслях экономики и сферах человеческой жизнедеятельности.

Главный вопрос в том, насколько быстро и качественно компании, которые занимаются кибертехнологиями, смогут довести ИИ до состояния, когда его

СЕГОДНЯ ТОЛЬКО 7% ПРОФЕССИОНАЛОВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИСПОЛЬЗУЮТ КОГНИТИВНЫЕ ИНСТРУМЕНТЫ. ОДНАКО, СОГЛАСНО ОЖИДАНИЯМ ЭКСПЕРТОВ, ЭТОТ ПОКАЗАТЕЛЬ УВЕЛИЧИТСЯ В ТРИ РАЗА ЧЕРЕЗ ДВА-ТРИ ГОДА

механизмы станут максимально эффективными. Кроме того, необходимо и развитие навыков самих ИТ-специалистов. В частности, в недавнем исследовании IBM отмечается, что сегодня только 7% профессионалов в сфере информационной безопасности используют когнитивные инструменты. Однако, согласно ожиданиям экспертов, этот показатель увеличится в три раза через два-три года³.

От тренда повсеместного внедрения ИИ не отстает и IBM. Корпорация — один из признанных мировых лидеров в области решений по информационной безопасности. Мы являемся не только глобальным разработчиком ИБ-продуктов, но и своего рода визионером в мире прорывных технологий.

У компании есть восемь круглосуточных центров кибербезопасности IBM X-Force Command Center, распределенных по всему земному шару. Мы провели мониторинг более одного трлн событий безопасности и ежедневно анализируем безопасность свыше 4,5 тыс. клиентов, которые пользуются управляемыми услугами защиты, предоставляемыми IBM. Мы обладаем свыше 3,5 тыс. патентов в области ИБ и широчайшей продуктовой линейкой для центров оперативного реагирования на инциденты ИБ, включая решения на базе искусственного интеллекта.

Год назад подразделение IBM Security представило решение Watson for Cyber Security, первую в отрасли технологию дополненного интеллекта, разработанную для управления когнитивными центрами информационной безопасности. Система способна помочь аналитикам информационной безопасности разобраться в тысячах отчетов, подготовленных на естественном языке, что ранее было невозможно при использовании обычных инструментов информационной защиты. Прикладным компонентом платформы является IBM QRadar Advisor with Watson. Новое приложение уже используют более 40 организаций по всему миру, в том числе и в России.

* * *

Угрозы ИБ глобальны и, если вы находитесь в России, то вас могут атаковать из любой страны мира. У киберпреступности нет географических границ. Поэтому IBM выстраивает альянсы, партнерства, развивает экспертизу в отдельных регионах и странах, чтобы обладать глобальной аналитикой и данными о передовых инструментах машинного обучения. Крайне важно уделять внимание тщательной и слаженной коллективной работе в партнерстве с компаниями, которые занимаются ИБ.

ЛИТЕРАТУРА

1. IBM & Ponemon Institute: Cost of a Data Breach Dropped 10 Percent Globally in 2017 Study <http://www-03.ibm.com/press/us/en/pressrelease/52643.wss>
2. Infographic: Watson for Cyber Security: Shining a light on Unstructured Data <https://securityintelligence.com/media/watson-for-cyber-security-infographic/>
3. IBM Institute of Business Value Study: Cybersecurity in the Cognitive Era <https://www-935.ibm.com/services/us/gbs/thoughtleadership/cyberimmunity/>



Михаил САВЕЛЬЕВ
директор
по развитию компании
«Информзащита»

СКОЛЬКО СТОИТ КИБЕР- РАЗВЕДКА?

ОТ 8 000 000 РУБЛЕЙ

Сегодня формируется мнение, что необходимым звеном в защите каждой компании является если не создание собственного подразделения киберразведки (Threat intelligence, TI), то как минимум приобретение результатов работы профессиональных команд в виде т.н. фидов — всевозможных списков подозрительных IP-адресов, хешей вредоносных, списков командных центров и т.п.

И действительно, TI дает много ценной информации. Порой даже возникает ощущение, что загрузи только волшебные «фиды» в свой SIEM и все само собой получится, но, к сожалению, это не так. Для получения результата необходимо научиться интегрировать результаты работы TI в процессы обеспечения безопасности. Не говоря уже о том, что эти процессы должны к моменту интеграции быть. Попробуем разобраться по порядку и определиться с задачами, которые можно поставить перед CTI командой, людьми, которым это можно поручить, и средствами, которые понадобятся для достижения успеха.

ЗАДАЧИ

На наш взгляд, киберразведка — комплекс процессов, мероприятий, технических средств и компетенций, нацеленный на две ключевые вещи.

Первое — проактивное управление угрозами ИБ еще на дальних подступах, до того момента, как произошел реальный инцидент на собственной инфраструктуре. Эту деятельность необходимо осуществлять через оперативный обмен информацией с киберсообществом: мировым, отраслевым,

вендорским (имеются в виду, в первую очередь, вендоры тех средств защиты, которые вы эксплуатируете). Цель обмена информацией — узнать о том, к чему нам надо подготовить инфраструктуру мониторинга и противодействия, механизмы реагирования и дежурные службы до момента проникновения «заразы» в периметр организации. Мы должны пытаться отслеживать информацию о массовых инцидентах, путях и способах их распространения. Необходимо заранее оценивать степень уязвимости инфраструктуры, понимать, сумеем ли мы закрыть уязвимости, или необходимо «трясти» своих вендоров на предмет выпуска сигнатур, правил обнаружения или, на худой конец, IoC (indicator of compromise), которые можем заложить в свои SIEM-системы для обнаружения признаков активности. На этом этапе важно расписать порядок действий для обнаружения инцидента в различных стадиях, оповестить и потребовать особой внимательности от персонала.

Второй глобальной задачей киберразведки должно стать противодействие целевым атакам. И тут сложность сильно возрастает: мы переходим в сферу «обнаружения необнаруживаемого». Тут от аналитиков требуется предположить, что злоумышленник уже контролирует часть вашей инфраструктуры и, базировавшись на знаниях о методах и тактике действий злоумышленников, пытаться строить и проверять гипотезы о том, как обнаружить следы присутствия непрошенных гостей.

Для проверки гипотез необходимо накапливать всю доступную киберразведчику информацию, формировать то, что называется SecBigData или

DataLake. Ведь заранее неизвестно, что именно потребуются для выявления злонамеренной активности. Именно тут, на этих массивах данных может сработать и т.н. поведенческий анализ, и появится возможность расширения контекста безопасности. Это сложная и интересная работа, в которой действует «обратный» принцип Парето: когда 95% усилий дают лишь 5% выявленных инцидентов. И то если повезет.

СИЛЫ

Собираетесь ли вы получать данные в виде подписки или хотите пойти по пути самостоятельного исследования OSINT (open source intelligence) источников — важно понимать, что все эти пути затратны. Даже на обработку бесплатных источников нужна пара высококвалифицированных специалистов. Их задачи — вычленять из общего потока крупинки релевантной по отношению к вашей организации информации и перепроверять её, чтобы не тратить время на «утки», подобные информации об атаке Skyfall, в которую после информации о Meltdown и Spectre поверила часть сообщества безопасности.

Обычно штат ИБ-специалистов невелик — 2–3 человека, у которых и без того много работы. Разбор «фидов» за утренним кофе не даст результата по причинам, описанным ниже.

СРЕДСТВА

Сразу определимся: ручная обработка информации обречена на провал. Из разных источников информация приходит в различных форматах, так что необходимо либо приобретать специализированную систему обработки



информации, либо усаживать своих специалистов за приведение информации к единому формату, продумывать процедуры ее хранения, обсуждения и дальнейшей обработки. Специализированные системы ТИ имеют необходимый функционал, но их недостаток — они стоят немалых денег.

И самое главное — куда загружать всю эту отфильтрованную и очищенную от «шума» информацию? Как минимум у вас должны быть системы и процессы по обнаружению и реагированию на выявленные угрозы, а точнее, процессы:

- ♦ выявления инцидентов по загружаемым фидам и IoC;
- ♦ корректировки создаваемых правил для уменьшения числа ложных срабатываний;
- ♦ реагирования на выявленные инциденты ИБ по заранее подготовленным планам.

Отсутствие любого из перечисленных звеньев сводит на нет всю ранее проделанную работу.

УПУЩЕННЫЙ МОМЕНТ — ОБЩЕНИЕ

К сожалению, когда речь заходит об инцидентах, мы, безопасники, становимся слушателями. Никто не хочет выносить сор из избы, сеять панику среди своих клиентов информацией об атаках. Но при этом мы готовы внимать любой информации об угрозах. Никому не приходит в голову мысль о том, а откуда же

берется релевантная информация, скажем, об атаках на финансовые организации, если они все молчат как партизаны и не делятся тем, что произошло у них? Выходом из этого тупика может стать обмен через третью доверенную сторону, обезличивающую поступающую информацию и раздающую ее остальным участникам обмена. Такой стороной может стать отраслевой или региональный CERT: благо, что инициатив о создании подобных сервисов много и на федеральном, и отраслевом, и частном уровнях.

Кроме того, не стоит недооценивать формат профессионального общения «без галстуков». Дружеские отношения с коллегами по отрасли, возможность переспросить что-то и получить неформальный совет может заменить дни и даже недели аналитической работы.

ВМЕСТО ВЫВОДОВ

В итоге возможны следующие альтернативные пути по организации/использованию ТИ:

- ♦ отказ от самой идеи упования на оперативность вендоров средств защиты;
- ♦ использование внешних платных/бесплатных сервисов, выделение специалиста для контроля и автоматизации процессов;
- ♦ создание собственной группы, которая будет использовать платные/бесплатные сервисы и автоматизировать процессы и процедуры выявления и реагирования.

При этом:

- ♦ Если у вас не решены задачи внедрения процедур выявления и реагирования на инциденты — говорить о киберразведке преждевременно.
- ♦ Нет одного выделенного человека на взаимодействие с подрядчиком — рано говорить о привлечении внешних поставщиков информации.
- ♦ Не можете позволить себе 3–4 «лишних» человека высокой квалификации — не стоит начинать строить собственную СТИ команду.
- ♦ Нет возможности организовать полноценный сбор информации с инфраструктуры — рано решать задачи по выявлению присутствия злоумышленников.

Постановка процесса взаимодействия команды/сервиса с исполнительским блоком занимает от 2 до 10 месяцев. Бюджет проекта (при собственной готовности и внешнем ТИ сервисе) — от 8 000 000 рублей с учетом одного выделенного сотрудника, услуг внешнего SOC, платной подписки на сервис ТИ и затрат на автоматизацию процессов. А в качестве обоснования бюджета перед руководством можно указать, что этот проект повышает показатели непрерывности бизнеса, доступности сервисов, обеспечивает снижение репутационных рисков.

ЦЕНТРАЛИЗОВАННЫЙ УДАЛЕННЫЙ ДОСТУП БЕЗ ПРОБЛЕМ

ИНТЕГРАЦИЯ CISCO ISE С РЕШЕНИЯМИ С-ТЕРРА ШЛЮЗ И С-ТЕРРА КЛИЕНТ



Алина СИДОРОВА
инженер отдела
технических решений
защиты информации
АМТ-ГРУП

В современном мире деятельность организаций становится более динамичной, и для повышения эффективности и гибкости работы сотрудников многие наши клиенты применяют технологии удаленного решения корпоративных задач. Традиционно удаленный доступ к корпоративной сети реализуется на основе решений, обеспечивающих построение VPN. Существует достаточно большое количество VPN-клиентов — каждый со своими плюсами и минусами.

Зачастую использовать произвольное решение по предоставлению удаленного доступа невозможно, так как при обработке в информационной системе информации, подлежащей обязательной защите в соответствии с законодательством (например, персональные данные), необходимо использовать сертифицированные средства защиты, прошедшие процедуру оценки соответствия регуляторами — ФСБ России и/или ФСТЭК России.

Также во многих организациях используются решения по контролю физических подключений к ЛВС, позволяющие реализовать функции идентификации и аутентификации пользователей по протоколу IEEE802.1x с помощью внутренней базы учетных записей или службы каталогов Microsoft Active Directory, при этом проблема состоит в том, что аутентификация при подключении по 802.1x и по VPN зачастую осуществляется независимо, что существенно снижает информативность журналов доступа и затрудняет расследование инцидентов и устранение неполадок.

В связи с этим у администраторов сети возникают вопросы о том, как одновременно обеспечить:

- ♦ выполнение требований российского законодательства по защите персональных данных при организации подключений удаленного доступа;
- ♦ централизованный контроль доступа к ресурсам сети удаленных пользователей;
- ♦ централизованный контроль физических подключений к ЛВС.

ТЕХНИЧЕСКИЕ РЕШЕНИЯ

Во многих организациях используется многофункциональное решение по реализации в корпоративной ИТ-инфраструктуре средств аутентификации и авторизации пользователей — система контроля доступа к сети Cisco Identity Services Engine (Cisco ISE).

В свою очередь, одним из решений, позволяющим реализовывать VPN-туннель, по которому передается зашифрованный с применением ГОСТ-алгоритмов трафик, являются ПАК С-Терра Шлюз и ПО С-Терра Клиент, традиционно используемые для соответствия требованиям законодательства РФ по защите персональных данных.

Решить задачу обеспечения удаленного доступа сотрудников с соблю-

дением всех вышеописанных требований позволяет интеграция С-Терра Шлюз и С-Терра Клиент версии 4.2, в которой появилась возможность аутентификации пользователей по доменному логину и паролю на RADIUS-сервере, с Cisco ISE версии 2.3, которые выступают в качестве данного сервера.

При этом использование доменной учетной записи при аутентификации позволяет организовать более строгую аутентификацию. Преимущество заключается в том, что даже если злоумышленник каким-либо образом получит доступ к компьютеру пользователя, то для входа в сеть ему необходимо ввести дополнительно аутентификационные данные. Также при утере устройства, с которого осуществлялся удаленный доступ, становится возможным не только отзыв сертификата пользователя, но и блокировка доменной УЗ.

Система контроля доступа Cisco ISE, которая выступает в качестве RADIUS-сервера, позволяет осуществлять интеграцию со службой каталогов Microsoft Active Directory, благодаря чему пользователь может использовать свою доменную учетную запись при подключении к сети.

**ОДНИМ ИЗ РЕШЕНИЙ, ПОЗВОЛЯЮЩИМ
РЕАЛИЗОВЫВАТЬ VPN-ТУННЕЛЬ,
ПО КОТОРОМУ ПЕРЕДАЕТСЯ
ЗАШИФРОВАННЫЙ С ПРИМЕНЕНИЕМ
ГОСТ-АЛГОРИТМОВ ТРАФИК, ЯВЛЯЮТСЯ
ПАК С-ТЕРРА ШЛЮЗ И ПО С-ТЕРРА КЛИЕНТ**

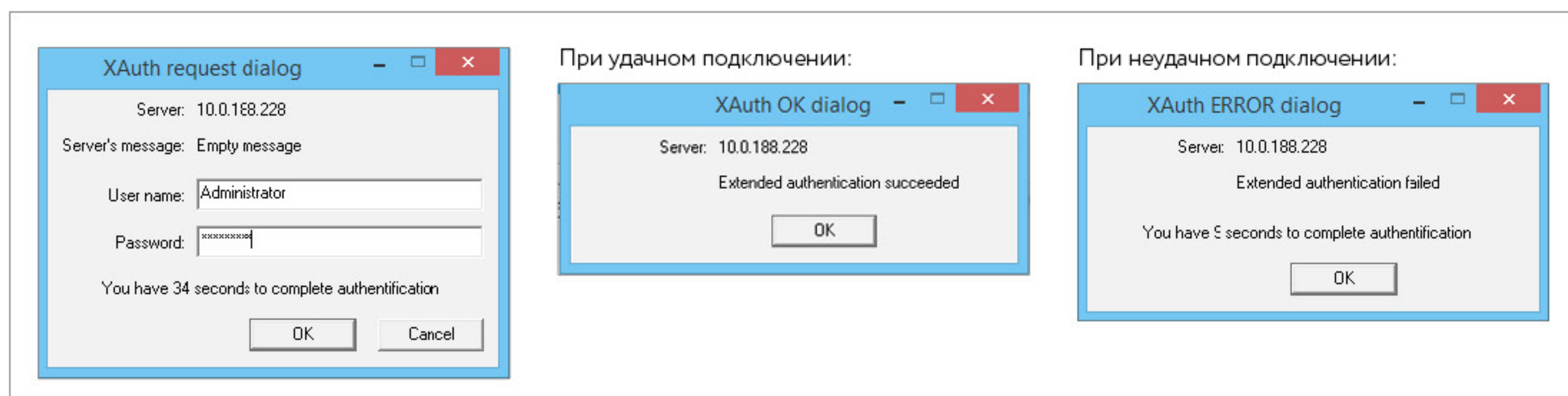


Рисунок 1. Окно запроса аутентификационных данных

ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ

Тестирование описанных выше решений проводилось в лаборатории АМТ-ГРУП. Для этого использовались С-Терра Шлюз и С-Терра Клиент версии 4.2, Cisco ISE версии 2.3 и служба каталогов Microsoft Active Directory.

Были произведены настройки по взаимодействию шлюза с RADIUS-сервером и использование XAuth. При построении IKE-сессии от клиента до шлюза на клиенте выводится окно «XAuth request dialog» (рис. 1). Введенные в окне данные передаются на RADIUS-сервер для аутентификации. При удачной аутентификации происходит построение IKE и IPsec туннелей между клиентом и шлюзом. При неудачной аутентификации будет выдаваться окно «XAuth ERROR dialog» с сообщением «Extended authentication failed», а также окно для повторной аутентификации.

Как только пользователь успешно проходит процедуры аутентификации и авторизации и получает доступ в сеть, на Cisco ISE появляется полная информация об этом пользователе, включающая IP-адрес пользователя и его учётную запись. В случае неудачной процедуры аутентификации и авторизации в журнале Cisco ISE появляется запись о неудачной попытке доступа к сети (рис. 2).

При просмотре детальной информации о подключении можно убедиться, что пользователь подключился к сети через С-Терра Шлюз, взаимодействие с которым настроено на сервере Cisco ISE (рис. 3).

Для выполнения данной задачи достаточно базовой лицензии Cisco ISE (Base).

При просмотре информации о подключении на С-Терра Шлюз дополни-

При удачном подключении пользователя:

Time	Status	Details	Repeat ...	Identity	Endpoint ID
Jan 25, 2018 04:22:44.825 PM	Auth Pass			Administrator	10.0.188.11

При неудачном подключении пользователя:

Time	Status	Details	Repeat ...	Identity	Endpoint ID
Jan 25, 2018 04:22:10.046 PM	Auth Fail			Administrator	10.0.188.11

Рисунок 2. Radius live log

Authentication Details

Source Timestamp	2018-01-25 16:22:44.738
Received Timestamp	2018-01-25 16:22:44.825
Policy Server	amtise
Event	5200 Authentication succeeded
Username	Administrator
Endpoint Id	10.0.188.11
Calling Station Id	10.0.188.11
Authentication Identity Store	amtise
Authentication Method	PAP_ASCII
Authentication Protocol	PAP_ASCII
Service Type	Framed
Network Device	S-Terra
Device Type	All Device Types#S-Terra

Рисунок 3. Детальный просмотр Radius live log


```

root@sterragate:~# sa_mgr show -detail '
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connection id: 7
cookies: 9710726B2A450753.D0DC273CCF7383A5
local peer (addr/port): 10.0.188.228/500
remote peer (addr/port): 10.0.188.11/500
IKECFG address: 10.0.1.1

local identity (DN): CN=Certificate of gate
remote identity (DN): CN=Certificate of client
IKERule name: IKERule:CMAP:1:DMAP:1
auth: gost signature + xauth (client as initiator)
mode: main

```

Рисунок 4. Информация о подключении на С-Терра Шлюз

Указание группы AD в условии применения профиля авторизации:

Conditions

AND

Device Type_S-Terra

amtise-memberOf CONTAINS Domain Guests

Radius live log при неудачном подключении пользователя, не состоящего в группе Domain Guest:

Status	Details	Repeat...	Identity	Endpoint ID	Authorization Profiles
Auth Failed	x		Administrator	10.0.188.11	DenyAccess

Атрибуты пользователя, не состоящего в группе Domain Guest:

memberOf	CN=Group Policy Creator Owners,CN=Users,DC=sblcise,DC=com
memberOf	CN=Domain Admins,
memberOf	CN=Enterprise Admins,
memberOf	CN=Schema Admins,
memberOf	CN=Administrators,CN=Builtin,

Рисунок 5

Radius live log при удачном подключении пользователя, состоящего в группе Domain Guest:

Status	Details	Repeat...	Identity	Endpoint ID	Authorization Profiles
Auth Pass	x		iiivanov	10.0.188.15	PermitAccess_S-Terra

Атрибуты пользователя, состоящего в группе Domain Guest:

memberOf	CN=Domain Guests,CN=Users,DC=sblcise,DC=com
RADIUS Username	iiivanov

Рисунок 6

тельно отображается метод аутентификации XAuth (рис. 4).

При этом при подключении удаленных пользователей к сети С-Терра Шлюз и С-Терра Клиент имеется возможность применения профилей авторизации на основе принадлежности к определенной группе в AD.

В данном случае используется проверка атрибута memberOf и указание условия принадлежности к выбранной группе в политики авторизации.

Например, при указании группы Domain Guest в политике авторизации (рис. 5), пользователь, не состоящий в данной группе, доступа к сети не получит, если для него не создана отдельная политика для подключения.

Пользователь, который состоит, в указанной группе, получит доступ к сети на основе указанного профиля авторизации (рис. 6).

Дополнительно возможно создание учетной записи на сервере Cisco ISE и применение профилей авторизации на основе группы пользователя, в которую помещена учетная запись, а также настройка таких атрибутов, как IP-адрес, выдаваемый по IKECFG, IP-адреса DNS-сервера и DNS-суффикса.

Для выдачи IP-адреса с помощью сервера Cisco ISE необходимо использовать атрибут Radius: Framed-IP-Address = <IP> (рис. 7), где IP- — адрес, выдаваемый удаленному пользователю. При этом на С-Терра Шлюз пул адресов в крипто-карте не указывается.

Для определения адреса DNS-сервера с помощью сервера Cisco ISE указывается дополнительный атрибут Cisco-avpair = «ipsec: dns-servers=<IP1>», где IP1 адрес DNS-сервера (рис. 8).

РАСШИРЕННЫЕ ВОЗМОЖНОСТИ ДЛЯ ПОВЫШЕНИЯ УРОВНЯ КОНТРОЛЯ

Вышесказанное демонстрирует, что интеграция решений по контролю доступа с решением по предоставлению удаленного доступа предоставляет возможность настройки параметров удаленных пользователей в зависимости от атрибутов, определяемых при аутентификации.

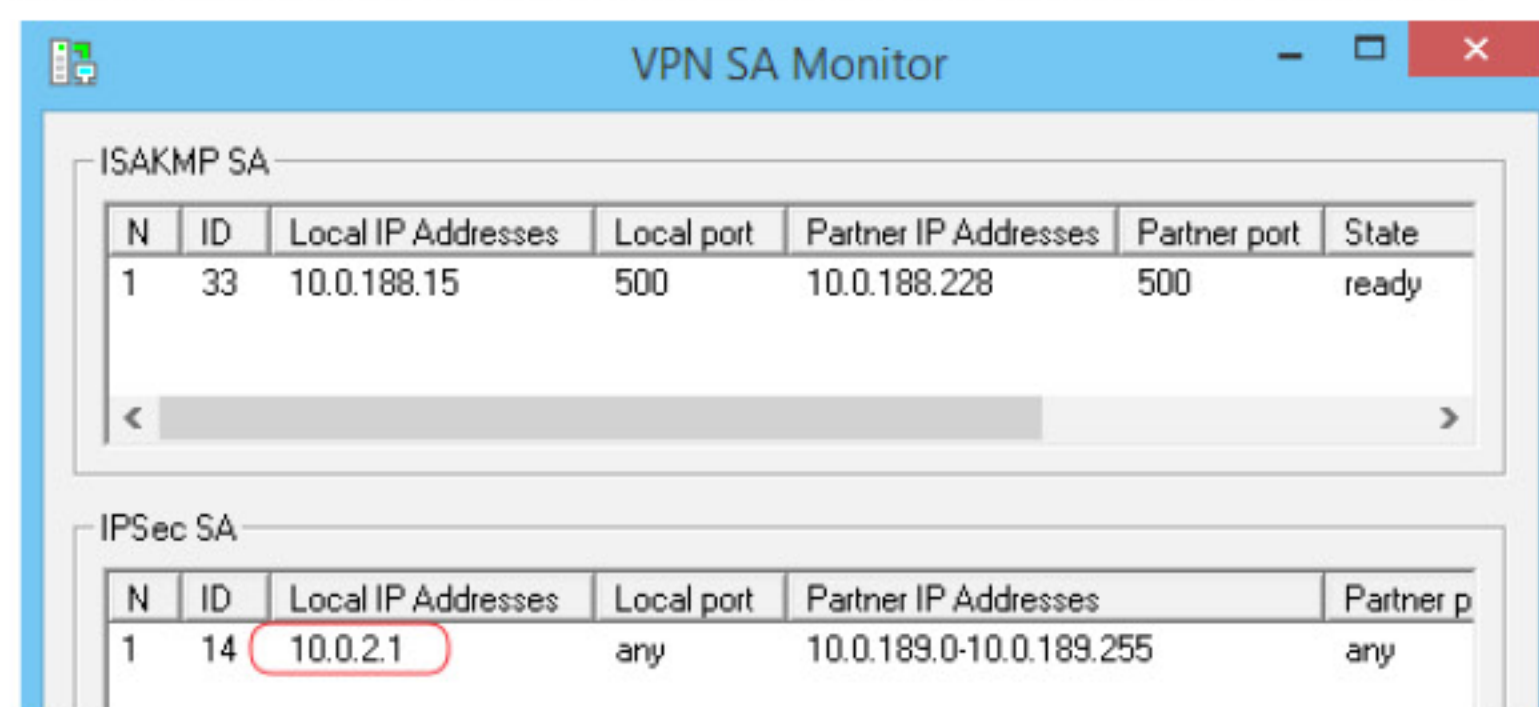
Становится возможным применение тонких настроек для конкретных пользователей и групп пользователей, под-

Атрибут, настроенный в профиле авторизации, для выдачи адреса по IKECFG:

▼ Attributes Details

Access Type = ACCESS ACCEPT
 cisco-av-pair = ipsec:dns-servers=10.0.189.204
 Framed-IP-Address = 10.0.2.1-10.0.2.10

Адрес, выданный пользователю, при подключении через C-Терра Клиент:



The screenshot shows the 'VPN SA Monitor' window. It contains two tables: 'ISAKMP SA' and 'IPsec SA'. In the 'IPsec SA' table, the 'Local IP Addresses' for the first entry is highlighted with a red circle.

N	ID	Local IP Addresses	Local port	Partner IP Addresses	Partner port	State
1	33	10.0.188.15	500	10.0.188.228	500	ready

N	ID	Local IP Addresses	Local port	Partner IP Addresses	Partner p
1	14	10.0.2.1	any	10.0.189.0-10.0.189.255	any

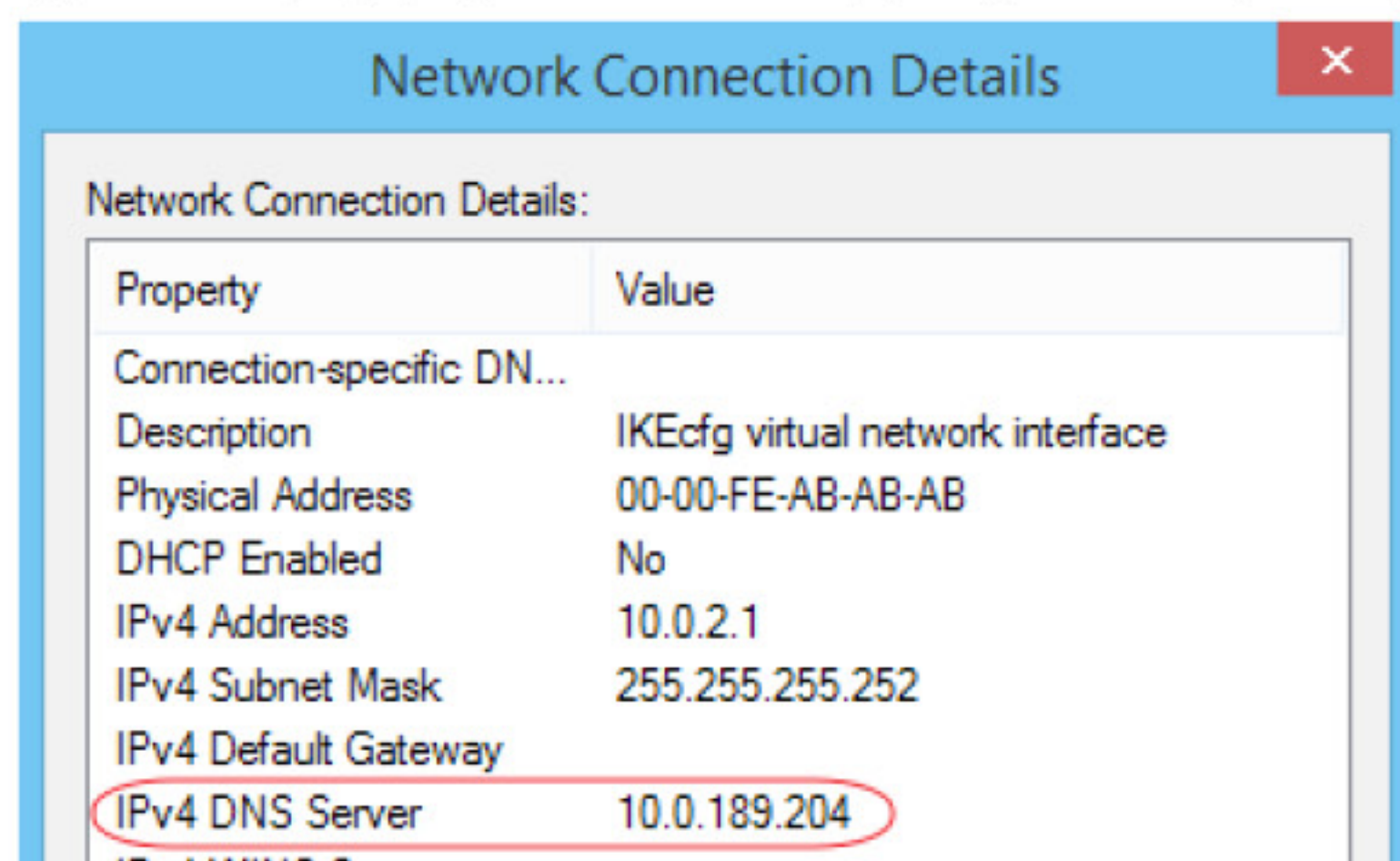
Рисунок 7

Атрибут, настроенный в профиле авторизации, для выдачи DNS-сервера:

▼ Attributes Details

Access Type = ACCESS ACCEPT
 cisco-av-pair = ipsec:dns-servers=10.0.189.204
 Framed-IP-Address = 10.0.2.1-10.0.2.10

Адрес DNS-сервера, выданный пользователю, при подключении через C-Терра Клиент:



The screenshot shows the 'Network Connection Details' window. It contains a table with network properties. The 'IPv4 DNS Server' property is highlighted with a red circle.

Property	Value
Connection-specific DN...	
Description	IKEcfg virtual network interface
Physical Address	00-00-FE-AB-AB-AB
DHCP Enabled	No
IPv4 Address	10.0.2.1
IPv4 Subnet Mask	255.255.255.252
IPv4 Default Gateway	
IPv4 DNS Server	10.0.189.204

Рисунок 8

ключаемых посредством C-Терра Шлюз и C-Терра Клиент, через централизованную консоль, а также решается задача по мониторингу состояния подключений к сети в реальном времени и ретроспективе.

Полученная при VPN-подключении пользователя к сети информация может быть использована в технологии Cisco Platform Exchange Grid (pxGrid), посредством которой осуществляется взаимодействие различных продук-

тов Cisco, а также связь решений Cisco с системами других вендоров. Данная технология предлагает общий язык взаимодействия для обмена информацией между различными системами, например, FirePOWER, ISE, WSA, Cyber Threat Defense (CTD) и т.д. Тем самым, появляется возможность использовать результаты профилирования Cisco ISE, например, в правилах доступа межсетевых экранов производства компаний Cisco, Check Point и др.

Помимо pxGrid Cisco ISE позволяет реализовать архитектуру Cisco TrustSec. Cisco TrustSec позволяет разграничивать доступ в сети по меткам, называемым Security Group Tags (SGT). Метка назначается как результат авторизации сессии оконечного подключающегося устройства, уникально его идентифицирует и переносится через всю сеть вместе с трафиком оконечного устройства. Тегирование дает возможность каждому устройству, поддерживающему работу с SGT, на пути следования пакета видеть, принимать решение по фильтрации и логировать события о прохождении данного трафика.

* * *

Таким образом, возможность совместного использования решений Cisco ISE и C-Терра Шлюз и C-Терра Клиент позволяет не только повысить уровень защиты сети при подключении удаленных пользователей к внутренним ресурсам и снизить риски связанные с безопасностью информации, но и соответствовать требованиям российского законодательства по защите персональных данных в части организации VPN для подключения к сети удаленных пользователей, снизить трудозатраты на инвентаризацию используемых конечных устройств, отправлять информацию о подключении удаленных пользователей в систему управления информацией и событиями о безопасности (SIEM), а также помогает отслеживать и расследовать инциденты информационной безопасности.



Андрей КОНУСОВ
генеральный директор
компании Аванпост



НА СМЕНУ SSO

WEB SSO — ОДНОКРАТНАЯ АУТЕНТИФИКАЦИЯ ДЛЯ ВСЕХ КАНАЛОВ ВЗАИМОДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЕЙ С ИНФОРМАЦИОННЫМИ СИСТЕМАМИ

Специалисты по информационной безопасности (ИБ) прекрасно знают, как упорно пользователи информационных систем (ИС) предприятий сопротивляются внедрению жестких политик безопасности в отношении аутентификации. Это и понятно: человек просто не в состоянии держать в голове стойкие, часто меняющиеся, пароли для каждой нужной ему программы или защищенного информационного ресурса. Стоит службе ИБ ослабить свои требования, пользователи тут же устанавливают одинаковые простейшие пароли и перестают их менять. Если же политики ИБ не смягчаются, пароли оказываются на бумажке, зачистую наклеенной прямо на монитор. Оба варианта позволяют злоумышленникам легко выдавать себя за других пользователей ИС, становиться невидимыми для сколь угодно навороченных средств ИБ. И спокойно

совершать компьютерные преступления, не оставляя следов.

Противоречие между удобством пользователей и безопасной аутентификацией снимается с помощью систем (Single Sign-On, или SSO), после однократной аутентификации открывающих пользователю все необходимые бизнес-приложения. Но радикальные изменения организаций и их ИС не вписываются в возможности классических систем SSO. На смену приходит новый класс ИБ-решений — Web SSO. Первое и пока единственное российское ПО этого класса выпустила компания Аванпост. Ниже мы кратко расскажем о технологии и трёх актуальных сферах применения этого инновационного ИТ-продукта.

БАНКОВСКИЙ СЕКТОР

Крупные банки, работающие с физическими лицами, стремятся максимально развить онлайн-бизнес и применить отработанный в ритейле комплекс технологий взаимодействия с клиентом. Для

этого крайне важно повышать разнообразие каналов электронных коммуникаций и через них предоставлять клиенту множество персонифицированных услуг. Естественно, доступ к ним нужно контролировать. С помощью Avanpost Web SSO банк может создать единую точку аутентификации для расширяющегося множества каналов коммуникации с клиентами (через Web-сайты, мобильные приложения, веб-сервисы и др.)

Второе требование — эффективная работа с большим и неконтролируемым числом внешних пользователей ИС, сохранение качества сервиса при пиковых нагрузках. Avanpost Web SSO поддерживает десятки миллионов пользователей, что подтверждено независимым тестированием и вполне достаточно для любого банка. При этом продукт Аванпост реализован в виде ПО (с лицензированием по ядрам), рассчитанного на работу в высоконагруженном режиме с уровнем надежности и готовности характерным для критиче-

ски важных элементов ИС. Это резко упрощает, ускоряет и удешевляет масштабирование Avanpost Web SSO по сравнению с аналогичными западными решениями, реализованными как программно-аппаратные комплексы.

КРУПНЫЕ ХОЛДИНГОВЫЕ СТРУКТУРЫ

Аутентификация в крупной организации холдингового типа имеет свои особенности и проблемы. Учесть и эффективно решить их без системы Web SSO практически невозможно.

В холдинговой структуре, объединяющей сотни разнопрофильных подразделений, происходит огромное число кадровых событий (прием на работу, увольнения, отпуска, включение сотрудников в различные проектные группы и др.). Но выстроить классическую схему аутентификации, где учетные данные корректируются в ответ на каждое кадровое событие, здесь совершенно нереально. С одной стороны, крайне сложно поддерживать в актуальном состоянии централизованную базу данных о сотрудниках всех подразделений холдинга, всех ролях, всех защищенных ресурсах. А без такой БД лица, администрирующие учетные данные, просто не имеют информации о пользователях на местах.

С другой стороны, такая централизованная БД, даже если бы ее удалось создать и поддерживать в актуальном состоянии, была бы неприемлемо избыточной. В подразделениях холдингов доля сотрудников, работающих с ИС, зачастую не превышает 2–3%. Причем до самого момента обращения к защищенному ресурсу совершенно неясно, кому и когда аутентификация потребуется. Обычную систему SSO это ставит в тупик. Но для Avanpost Web SSO это не проблема, т.к. система обрабатывает запросы на аутентификацию именно тогда, когда конкретный сотрудник определенного подразделения пытается начать работать с нужным ему приложением или ресурсом.

Именно поэтому уже сегодня Web SSO — это необходимый элемент ИБ-инфраструктуры холдингов.

КЛАСТЕРЫ И ДЕЛОВЫЕ СЕТИ

Чтобы система SSO не стала источником ограничений и рисков, ор-

AVANPOST WEB SSO ПОДДЕРЖИВАЕТ ДЕСЯТКИ МИЛЛИОНОВ ПОЛЬЗОВАТЕЛЕЙ, ЧТО ПОДТВЕРЖДЕНО НЕЗАВИСИМЫМ ТЕСТИРОВАНИЕМ И ВПОЛНЕ ДОСТАТОЧНО ДЛЯ ЛЮБОГО БАНКА

ганизация не должна думать лишь о технологических тенденциях и своем внутреннем мире. Меняются модели управления отраслями, крупными проектами федерального и регионального масштаба, самими предприятиями. И появляется все больше кластеров нескольких типов: корпоративных (складывающихся вокруг крупных организаций), отраслевых, территориальных (в пределах города, региона, особой экономической зоны) и проектных. В пределах кластеров выстраиваются производственные связи и цепочки поставок, осуществляется передача функций на аутсорсинг. И происходит интенсивное перекрестное использование информационных ресурсов и прикладного ПО (обычно в виде SaaS-сервисов или терминального доступа). Через эти каналы члены кластера открывают партнерам свои бизнес-функции и конфиденциальную информацию. При большом числе пользователей, работающих с «чужими» приложениями и ресурсами, оптимальным вариантом является т.н. федеративная аутентификация, «из коробки» поддерживает Avanpost Web SSO.

ТЕХНОЛОГИЯ

Avanpost Web SSO позволяет реализовать не только рассмотренные, но и другие сценарии использования, покрывающие как классические задачи внутрикорпоративной аутентификации, так и сценарии аутентификации во внешних по отношению к сети организации системах. Благодаря защищенности протоколов, для аутентификации можно использовать открытые каналы связи (интернет).

А поддержка многофакторной аутентификации позволяет лучше защитить внутренние ресурсы при обращении пользователей из внешнего периметра, а также сделать Web SSO фронтальной системой аутентификации для различ-

ных каналов взаимодействия с клиентами. Отметим: решения класса Web SSO могут определить, откуда идет обращение, и избирательно задействовать различные дополнительные факторы аутентификации: SMS, специальные мобильные приложения, электронную подпись и др.

Эти особенности открывают широчайшие возможности применения Avanpost Web SSO, такие как прозрачная аутентификация пользователей организации в информационных системах контрагентов, прозрачная и безопасная аутентификация пользователей в SaaS-сервисах, организация общей системы аутентификации для порталных решений, организация защищенного доступа через интернет к внутренним ресурсам предприятия.

ЗАКЛЮЧЕНИЕ

Сегодня актуальна еще одна особенность Avanpost Web SSO. Предпочтительная среда исполнения для данного ПО — это Linux. В то же время технологический стек, на котором построен продукт (язык программирования, дополнительные библиотеки и фреймворки) имеет эффективные реализации и для Windows. Полностью переносим между обеими платформами и исходный код продукта, созданный разработчиками Аванпост. Благодаря этому Avanpost Web SSO одинаково хорошо подходит и заказчикам, переходящим на импортонезависимые ИТ-решения, и коммерческим организациям, продолжающим ориентироваться на ИТ-инфраструктуру на основе Windows.

* * *

Отметим также простоту внедрения Avanpost Web SSO. И то, что этот продукт, как и другие разработки компании Аванпост, включен в Реестр российского ПО и баз данных.



Александр ПОГРЕБНОЙ
заместитель генерального директора
ООО «Газинформсервис»



Татьяна СТАНКЕВИЧ
менеджер по продукту
ООО «Газинформсервис»

ПЕРЕЛОМ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ МЕДИЦИНСКОЙ ОТРАСЛИ

28 июля 2017 года Правительством РФ было подписано Распоряжение № 1632-р, что ознаменовало начало претворения в жизнь программы «Цифровая экономика Российской Федерации» (далее — Программа). Для управления Программой были определены пять базовых и три прикладных направления развития. К базовым направлениям отнесены нормативное регулирование, кадры и образование, формирование исследовательских компетенций и технических заделов, информационная инфраструктура и информационная безопасность. К прикладным — государственное управление, «умный город» и здравоохранение. Таким образом, Программа предусматривает автоматизацию и цифровизацию одной из основных государственных отраслей, обеспечивающих удовлетворение физиологических потребностей людей, — здравоохранения.

ПРИМЕРЫ АВТОМАТИЗАЦИИ МЕДИЦИНЫ

Безусловно, автоматизация, цифровизация, роботизация любой отрасли связаны со значительными инвестициями, но при этом влияние их на повышение

эффективности производства (производительность труда, сокращение/исключение ошибок, связанных с человеческим фактором и прочие показатели) несоизмеримо выше. Передовые медицинские технологии получают все большее распространение среди российских клиник (рис. 1, 2).

Рассмотрим для примера робота da Vinci. Его особенность в том, что он не выполняет все свои действия самостоятельно, а лишь повторяет движения хирурга, то есть робот позволяет при значительной пространственной удаленности от врача, проводящего манипуляции, проводить операцию (например, врач находится в США, а пациент — в Индии, так называемая телехирургия). Робот осуществляет сложные хирургические действия, требующие высокой точности при манипуляциях.

Полноправным аналогом da Vinci стал робот под названием Raven II, который появился несколько позже своего собрата, и ни в чем ему не уступает. При этом важным конкурентным преимуществом Raven II является стоимость, которая значительно ниже стоимости da Vinci (\$250 тыс. против \$1,8 млн), что обусловлено функционированием его на операционной

системе и программном обеспечении, которые имеют открытый исходный код.

ПРОБЛЕМЫ ИБ МЕДИЦИНСКИХ ТЕХНОТРЕНДОВ

К сожалению, производители медицинских передовых технологий мало задумываются об их кибербезопасности. Так, например, все сигналы, посылаемые роботам (и da Vinci, и Raven II), передаются по открытым каналам, и могут быть легко перехвачены (уничтожены или модифицированы) злоумышленником. Тут возникает вопрос: «А как защитить от такой перспективы врача и пациента?» На сегодняшний день заказные убийства, основанные на незаконном вмешательстве в цифровые технологии, мало распространены, но в перспективе, при повышении зависимости жизнеобеспечения людей от данных технологий, это может стать реальной угрозой (рис. 3).

Подобная атака с успешным результатом была реализована специалистами Вашингтонского университета. На первом этапе эксперимента были перехвачены пакеты данных, адресованные роботу Raven II, что позволило изменить их последовательность при пере-



Рисунок 1. Помощник директора клиники МЧС России проверяет интеграцию роботизированного биохимического анализатора крови (робота) с лабораторной информационной системой

даче. Манипулятор робота начал производить хаотичные движения и перестал подчиняться управлению врачом. Вторым этапом экспериментальной атаки было изменение угла наклона рабочих инструментов робота и дистанции их перемещения. В итоге специалистам удалось получить полный контроль над действиями Raven II, при этом влияние на робота оказалось настолько серьезным, что робот-хирург даже не отреагировал на команду к перезагрузке системы и продолжал выполнять навязанные ему действия.

Проблема безопасности может стать одним из основных камней преткновения в развитии современной телехирургии. Своим экспериментом специалисты Вашингтонского университета доказали, что использование открытых каналов передачи данных для таких серьезных действий, как медицинские манипуляции, теоретически, может закончиться плачевно, если не прибегать к защите передаваемых данных. Не стоит забывать, что помимо проблемы отсутствия шифрования, канал передачи данных от хирурга к роботу может быть попросту подвержен DDoS-атаке.

Но все-таки роботизация медицины — весьма дорогое и далекое до массового внедрения «удовольствие». Давайте рассмотрим более актуальные проблемы и задачи ИБ в сфере здравоохранения.

НАСУЩНЫЕ ПРОБЛЕМЫ ИБ В МЕДИЦИНЕ

До сегодняшнего дня нам казалось, что медицинская сфера не может представлять для преступников особого интереса, поскольку в ней нет больших денег, секретных данных и другой значимой информации, ради которой нужно проводить дорогостоящие атаки. Но появление жизнеобеспечивающих систем и медицинского оборудования, подключенных к интернету и имеющих сетевые интерфейсы, открывает для злоумышленников новые, более дешевые способы воздействия.

Обратим внимание на автоматизированные линии производства лекарственных препаратов, которые тоже подключаются к сети Интернет. Представьте на минуту, насколько серьезны могут быть последствия изменения концентрации или состава производи-



Рисунок 2. Хирург проводит операцию при помощи робота da Vinci

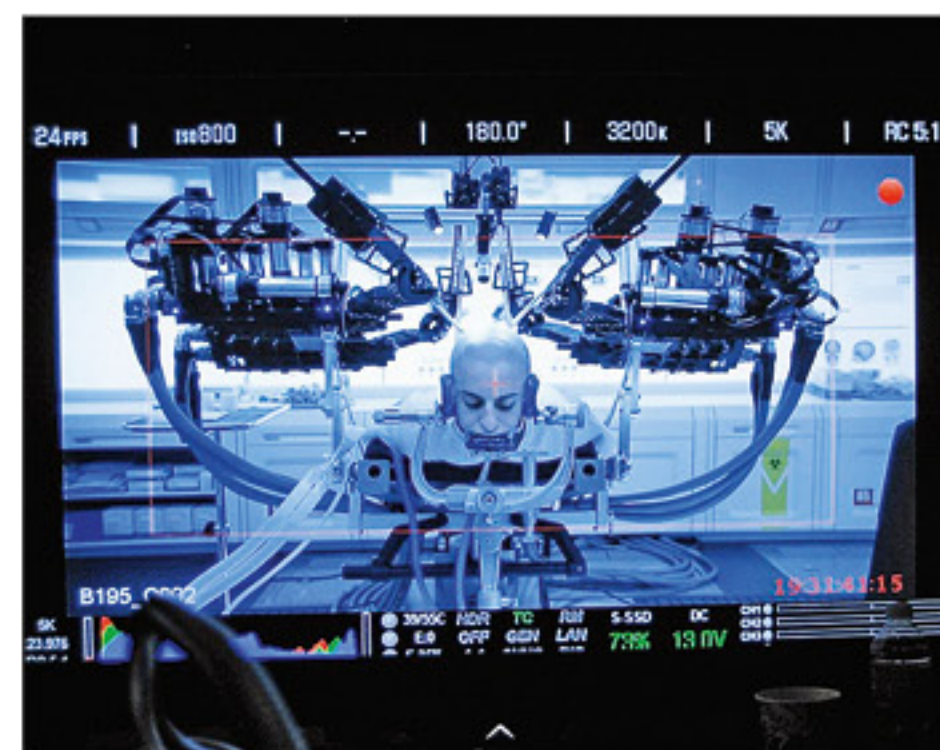


Рисунок 3. Робот-хирург Raven II делает операцию на мозге пациента

мых средств! Решением по защите таких систем являются продукты контроля их целостности: мы на каждом этапе штатного функционирования системы должны быть уверены в неизменности информационных потоков и конфигураций устройств, критичных для жизни и здоровья людей.

Системы помощи принятия решений при постановке диагноза, для анализа и прогноза состояния пациента на сегодняшний день имеются не во всех клиниках. Для решения этих задач врачи ежедневно посещают множество веб-сервисов, и здесь нашу клинику опять поджидают опасности: значительный ущерб могут нанести вирусы, поражающие Интернет-ресурсы. Снизить данные риски можно посредством выстраивания эшелонированной антивирусной защиты как на стороне владельцев веб-сервисов, так и на стороне медицинских организаций, являющихся потребителями соответствующей информации.

А задумывались ли вы об уязвимостях в специализированном программном обеспечении? Каждая ли компания-производитель медицинской

23% ВСЕХ ПРИБЫВАЮЩИХ В РОССИЮ ПАЦИЕНТОВ — ЭТО ГРАЖДАНЕ ЕС. И ЕСЛИ ВАША КЛИНИКА ПРЕДОСТАВЛЯЕТ УСЛУГИ ТАКИМ ПАЦИЕНТАМ, ТО ВОЗНИКАЕТ ВОПРОС ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ГРАЖДАН ЕВРОСОЮЗА

информационной системы проводит аудит своего продукта? Ответ однозначный — нет. По данным исследования, проведенного в США, в управляющих модулях кардиостимуляторов четырех производителей суммарно было обнаружено более 8 тысяч уязвимостей.

Рост доступности медицинских услуг через Интернет (так называемая телемедицина), приложения которой на текущий момент времени не обеспечивают должного уровня информационной безопасности обрабатываемых в нем данных, также являются одним из источников интереса для злоумышленников. Разработчикам таких решений стоит задуматься о реализации технологий электронной подписи в приложении (например, для формирования рецептов пациенту), а также шифрования результатов анализов, передаваемых от врача к пациенту.

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Одна из важнейших составляющих безопасной коммерческой деятельности любой медицинской организации — обработка персональных данных пациентов. Попадая в руки злоумышленников, информация о ваших клиентах, может повлечь судебные иски, мошенничество по отношению к пациентам, санкции регуляторов, удар по престижу клиники, нарушения штатного режима функционирования оборудования и жизнеобеспечивающих систем. Нужно предупредить возникновение подобных инцидентов.

Здесь же стоит обратить внимание и на возрастающий интерес к медицинскому туризму в Россию. На сегодняшний день такой тип получения медицинской помощи становится все более популярным, что связано не только с ценой оказываемых в России услуг, но и их качеством. Согласно исследованию компании Transparency Market

Research, мировой рынок медицинского туризма в ближайшие годы будет расти в среднем на 17,9% в год, и к 2019 году его объем достигнет \$32,5 млрд (в 2012 году это значение было \$10,5 млрд).

Относительно стоимости услуг приведем наглядный пример: коронарное шунтирование в России стоит примерно \$3200–\$3500, а в США — от \$55 тыс. до \$130 тыс., лазерная коррекция зрения — от \$340 до \$650 против \$4000–5000. При этом наиболее популярными направлениями для иностранцев являются: стоматология (имплантация, протезирование), урология, гинекология (экстракорпоральное оплодотворение), пластическая хирургия, ортопедия, травматология, сердечно-сосудистая хирургия, офтальмология.

По данным Forbes, 23% всех прибывающих в Россию пациентов — это граждане Евросоюза. И если Ваша клиника предоставляет услуги таким пациентам, то возникает вопрос защиты персональных данных граждан Евросоюза, что связано с выполнением новых требований ЕС — GDPR (General Data Protection Regulation).

Но, думая об иностранных клиентах, не стоит забывать и о защите персональных данных российских пациентов. В этом направлении основным регламентирующим документом является Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ. Таким образом, нужно учесть требования обоих документов, и при этом ничего не забыть во избежание штрафных санкций.

ЧТО ДЕЛАТЬ? КАК ЖИТЬ ДАЛЬШЕ?

Что же делать? Конечно, можно купить отдельные средства защиты информации, которые окажут благоприятное воздействие на ситуацию, но этого не-

достаточно. Не стоит забывать, что информационная безопасность — это в первую очередь совокупность соответствующих организационных процессов. Можно создать службу информационной безопасности, которая будет эксплуатировать эти средства и организовывать необходимые процессы, но задача проектирования, ввода в действие высокотехнологичных средств информационной безопасности и выстраивания защитных процедур является достаточно трудоемкой и требующей совместной работы многих высококомпетентных узконаправленных специалистов.

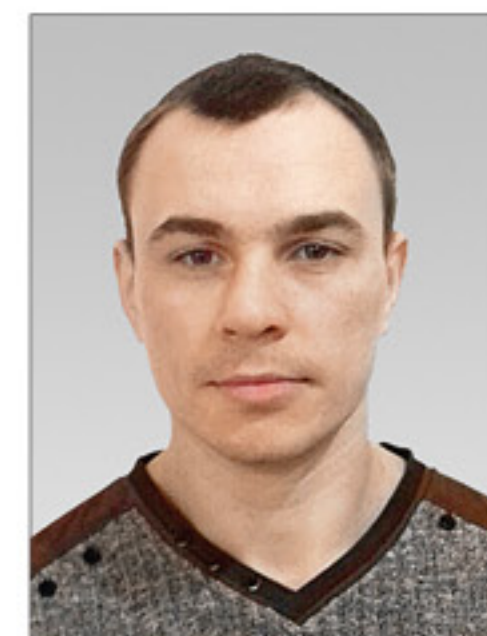
Для решения задачи обеспечения информационной безопасности на должном уровне лучшей практикой является привлечение соответствующих специализированных компаний, имеющих в штате требуемых экспертов каждого направления. Данные организации смогут провести аудит того, что есть; подготовят дизайн будущей системы; сделают так, как должно быть «под ключ», и в последующем будут обеспечивать ее сопровождение и модернизацию в соответствии с новыми требованиями регуляторов и актуальными проблемами информационной безопасности.

Хотелось также обратить внимание, что при решении задач информационной безопасности, зачастую, небольшие клиники обращаются к непроверенным подрядчикам, предоставляя им полный доступ к своим информационным ресурсам. Не поступайте так! Вспомните старую поговорку: «Скупой платит дважды», не экономьте там, где эта экономия может вылиться массой новых проблем.

Компания «Газинформсервис» является интегратором и разработчиком средств информационной безопасности. Мы трудимся на рынке уже на протяжении 14 лет, обеспечиваем спокойствие и безопасность целого ряда крупных предприятий, реализуем самые сложные и амбициозные проекты. С радостью поможем и Вам обеспечить безопасность на пути к успеху!

КРАСНЫЕ МЕТКИ В ЧЕРНЫХ СПИСКАХ

АНАЛИЗ ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ РЕПУТАЦИОННЫХ БАЗ ДЛЯ БОРЬБЫ С ФИШИНГОМ



Сергей СТОРЧАК
специалист
по защите информации
ПАО «Тэгмет»

СИТУАЦИЯ

Фишинг — это вид мошенничества, целью которого является незаконное получение конфиденциальных данных пользователя (логинов, паролей, реквизитов банковской карты) с помощью социальной инженерии или путем заражения вредоносным кодом устройств пользователя.

В третьем квартале 2017 года RiskIQ обнаружил 931 665 уникальных фишинговых URL-адресов, направленных против 279 брендов. TOP-10 брендов, против которых развернуты фишинговые кампании, возглавляют бренды финансовой категории (40%) [1].

По данным «Лаборатории Касперского» в 2017 году с помощью системы «Антифишинг» было предотвращено 246 231 645 попыток перехода пользователей на фишинговые страницы. Это на 91 273 748 больше, чем в 2016 году. Более половины (53,82%) срабатываний зафиксированы на страницах с упоминанием брендов финансовой категории, таких как «банки» (27%), «платежные системы» (15,87%) и «онлайн-магазины» (10,95%) (рис. 1) [2].

Из обоих отчетов видно, что основными целями фишинговых атак остаются компании в сфере финансовых услуг.

СПОСОБЫ РАСПРОСТРАНЕНИЯ

Основными векторами атак для распространения фишинга в банковской сфере являются:

- ♦ рассылка электронных писем банковским сотрудникам якобы от имени клиентов, компаний-партнеров, регуляторов и различных веб-сервисов (госуслуги, профессиональные сообщества и т.п.);

- ♦ рассылка личных сообщений через социальные сети и системы мгновенного обмена сообщениями (Skype, ICQ, WhatsApp и т.п.).

Наибольшее количество рассылок (58%) приходится на вредоносные программы типа Trojan.Downloader [3]: как правило, к почтовому сообщению прикреплено вложение с вредоносным кодом, которое впоследствии загружает и устанавливает на компьютер троянские программы. Через интернет мессенджеры часто распространяются ссылки, внешне схожие с настоящими. После того, как пользователь перейдет по такой ссылке, злоумышленники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои

чувствительные данные. Таким образом, злоумышленники получают доступ к учетным записям и банковским счетам пользователя.

МЕТОДЫ ОБНАРУЖЕНИЯ

Антифишинговые средства применяют следующие технологии для выявления поддельных сайтов:

- ♦ использование облачных репутационных баз или проверка по спискам запрещенных (blacklist) и достоверных (whitelist) сайтов;
- ♦ эвристический анализ.

Специально разработанные алгоритмы эвристического анализа предупреждают пользователя в случае, если посещаемый веб-ресурс соответствует опасным или подозрительным

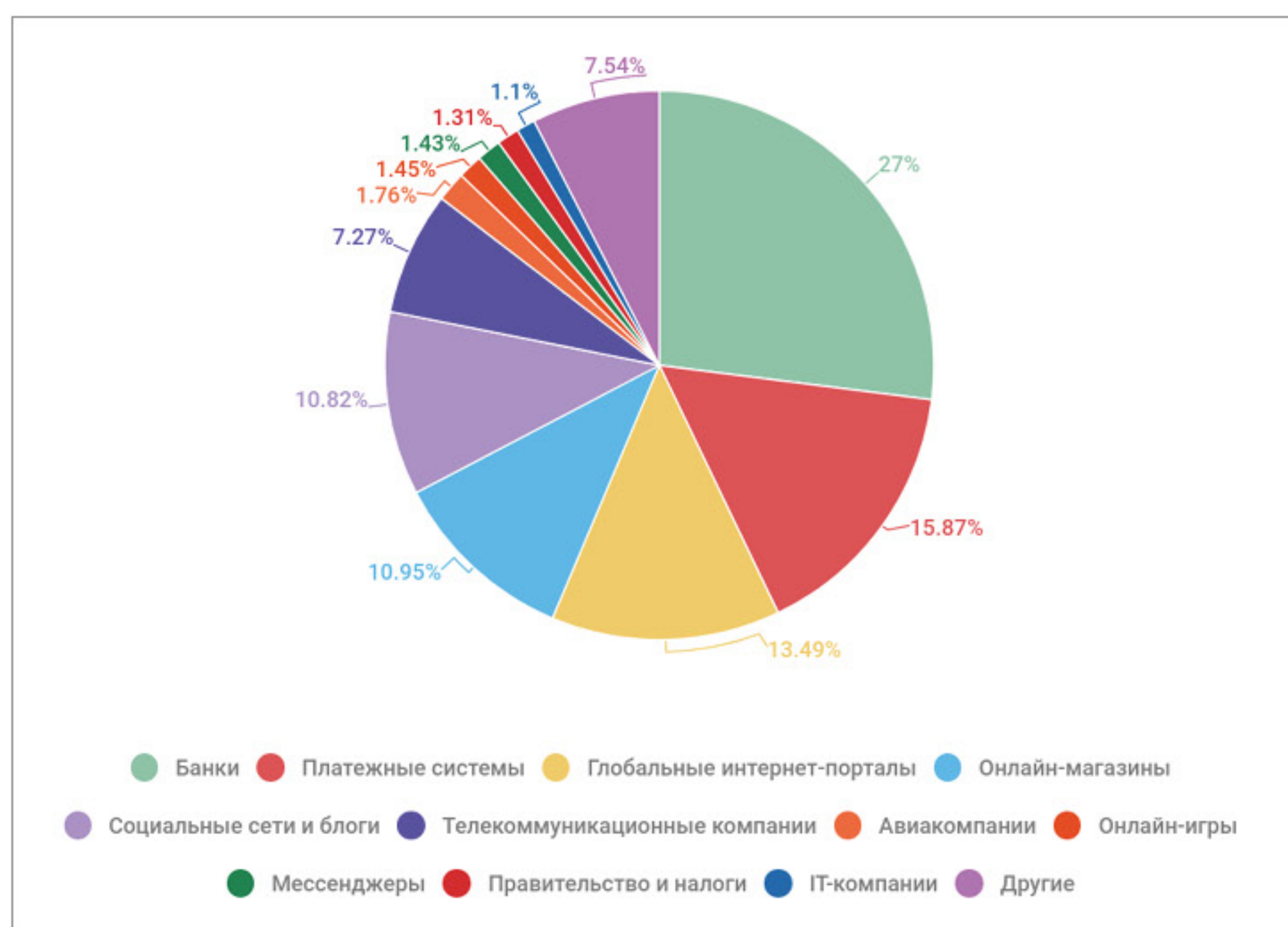


Рисунок 1. Распределение организаций, атакованных фишерами, по категориям, второй квартал 2017 г. Источник: Лаборатория Касперского

характеристикам. Данные алгоритмы могут быть построены на лексическом анализе контента или на анализе расположения веб-ресурса. Анализ расположения ресурса собирает информацию об ip-адресе, регистраторе домена, лице, зарегистрировавшем домен, и о доменном имени. Таким образом на основании полученных данных устанавливается степень опасности сайта [4].

Проверка фишинговых сайтов по репутационным базам является более точным методом, обеспечивающим минимальное количество ложных срабатываний, если мы имеем дело с известными угрозами [5].

В список доверенных сайтов заносятся заранее проверенные легитимные сайты. Например, список кредитных организаций формируется на основе сведений об адресах сайтов кредитных организаций Российской Федерации [6].

Blacklist пополняется за счет баз данных PhishTank [7], OpenPhish [8] и множества других подобных сервисов, а также за счет результатов эвристического и ручного анализа сайтов.

НЕДОСТАТКИ РЕПУТАЦИОННЫХ БАЗ

Существует несколько распространенных методов обхода списков доверенных сайтов. Во-первых, злоумышленники могут скупать домены, входящие в белый список, у которых недавно окончился срок регистрации. Во-вторых, владельцы сайтов добровольно могут установить код тизерных партнерских сетей или непроверенных рекламных блоков, которые будут скрыто выполнять перенаправление мобильных посетителей на вредоносную страницу с загрузкой шпионского ПО, майнить криптовалюту или оформлять платные подписки [9].

В-третьих, легитимный сайт может быть скомпрометирован. Известны случаи, когда проверка по базам доверенных сайтов проводилась без учета вредоносной активности на поддоменах, в результате чего происходило ложноотрицательное срабатывание (ошибка второго рода). В прошлом, когда средняя продолжительность жизни фишингового сайта составля-



Рисунок 2. Сайт банка «The First National Bank of Peterstown»

ла несколько недель или месяцев, для каждой фишинговой кампании регистрировалось новое доменное имя. В настоящее время такие сайты быстро вычисляются и блокируются. Поэтому злоумышленники используют легитимные домены для размещения на них фишинговых страниц. По данным Webroot почти 100% фишинговых URL-адресов расположены на легитимных сайтах [10].

В-четвертых, некоторые антивирусные и антифишинговые средства защиты формируют список доверенных веб-ресурсов на основе топ миллиона сайтов от Alexa или Cisco Umbrella.

В мае 2016 года сервис ReScan.pro провел исследование безопасности 50 тыс. сайтов рейтинга Alexa в зоне.ru. В результате около 2% сайтов среди проверенных имели те или иные проблемы безопасности [9]. В конце марта 2017 года разработчик NetworkMiner Эрик Хьелмвик (Erik Hjelmvik) проанализировал сайты, входящие в список Alexa и Umbrella, на наличие вредоносных. В итоге около 1% веб-ресурсов показали вредоносную активность [11].

Возможно, для таких средств защиты как IDS игнорирование 1–2% вредоносного трафика будет допустимо, но для антифишинговых средств защиты это неприемлемо, т.к. ежедневная аудитория некоторых зараженных сайтов составляет свыше 50 тыс. человек.

Черные списки тоже обладают рядом недостатков, ведь практически всегда найдутся способы их обхода,

не предусмотренные разработчиком. Так, например, злоумышленники могут использовать различные варианты представления ip-адреса или в самих средствах защиты может происходить некорректная логика работы проверки адреса [12]. Даже в черных списках PhishTank [7] иногда встречаются URL в виде ip-адресов, которые принадлежат легитимным сайтам. Например, адрес <http://213.159.214.86/> перенаправляет на amazon.com, а <http://66.55.107.122> — это тот же <http://www.fnbpeterstown.com/> — сайт банка «The First National Bank of Peterstown» (рис. 2).

Известны случаи, когда антивирус блокировал только главную страницу сайта, а загрузку с него файлов, в том числе вредоносных, — нет.

По данным Webroot [10] максимальная продолжительность жизни фишингового сайта составила 44 часа, а минимальная — 15 минут. Около 5% сайтов были заблокированы в течение часа, а 84% всех фишинговых сайтов просуществовали менее 24 часов. В среднем фишинговый сайт был доступен в сети менее 15 часов, т.е. большинство фишинговых сайтов закрывается в течение суток.

Поэтому злоумышленники всё чаще стараются использовать различные техники обхода, препятствующие обнаружению. Наиболее распространенные из них — это ограничение доступа к фишинговому сайту по HTTP-заголовкам «User-Agent» и/или «Referer», ip-адресу;

динамическая генерация URL. Так, например, на взломанных сайтах злоумышленники размещают специальный javascript, проверяющий источник перехода. Если пользователь перешел на взломанный сайт из поисковой системы, его перенаправят на фишинговый сайт. Если он зашел по прямой ссылке или на главную страницу взломанного веб-ресурса, перенаправление не произойдет.

Как правило, ограничение доступа к фишинговому сайту осуществляется через файл .htaccess или проверкой по блоклистам с помощью РНР-сценариев. В фишинговых кампаниях, нацеленных на конкретную страну или регион, иногда встречаются ограничения по белым спискам.

При динамической генерации URL-адресов для каждого посетителя задается уникальное имя каталога или параметров URL. На взломанном веб-сервере создается новый каталог, куда затем копируются все исходные компоненты фишингового сайта. В случае с URL-параметрами, они имеют легитимные названия, но уникальные случайные значения для каждого пользователя. Главное различие между генерацией URL для каталогов и URL-параметров заключается в том, что

в последнем случае на веб-сервере не создаются или не копируются новые файлы.

ЗАКЛЮЧЕНИЕ

Как было показано выше, репутационные базы имеют ряд недостатков, которые могут быть устранены следующими способами:

1. Факт попадания веб-ресурса в whitelist не означает, что он останется там навсегда, поскольку его репутация может измениться, например, в результате компрометации сайта либо окончания срока регистрации домена. Поэтому для поддержания белых списков в актуальном состоянии их нужно регулярно перепроверять на наличие вредоносной активности. То же самое касается и черных списков. Часты случаи, когда сайт был замечен в распространении фишинга, в связи с чем происходила его блокировка. После этого системные администраторы начинали подходить более ответственно к защите веб-ресурса.

2. Рекомендуется периодически удалять из белого списка «мертвые» веб-ресурсы. Это можно делать следующим образом. По умолчанию статус легитимного домена — «активный». Если он в данный момент не отвечает

(не доступен), его статус меняется на «временно недоступный». Когда не отвечает временно недоступный домен, он проверяется повторно через каждую одну минуту, затем две, четыре, восемь и т.д., пока этот период не станет большим, чем две недели. В этом случае статус домена меняется на «неактивный». Ровно через две недели домен опрашивается повторно. Если неактивный домен не отвечает и через две недели, он удаляется. Похожий подход использует IANA для поддержания в актуальном состоянии списка whois-серверов.

3. Для хранения в репутационных базах хешей веб-адресов рекомендуется использовать алгоритм SHA256 взамен или совместно с MD5 и SHA-1, т.к. последние могут приводить к коллизиям [13][14].

4. Для формирования и распространения черных списков требуется взаимодействие между различными источниками, предоставляющими информацию о подозрительных фишинговых сообщениях и URL-адресах (внешние источники данных об угрозах). К таким источникам могут относиться ловушки (honeypots), разработчики средств защиты, пользователи (APWG, PhishTank) и профессиональные сообщества типа ФинЦЕРТ Банка России [15].

ЛИТЕРАТУРА

1. RiskIQ's Q3 2017 Phishing Roundup: Phishing Down, Financial Services Still a Top Target. [Электронный ресурс] <https://www.riskiq.com/blog/external-threat-management/q3-2017-phishing-roundup/>
2. Лаборатория Касперского. Спам и фишинг в 2017 году. [Электронный ресурс] <https://securelist.ru/spam-and-phishing-in-2017/88630/>
3. ЦБ РФ. Отчет Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере главного управления безопасности и защиты информации Банка России, 1 июня 2016–1 сентября 2017 г. [Электронный ресурс] <http://www.cbr.ru/Press/event/?id=1361>
4. COMSS. Обнаружение вредоносных ссылок — Часть 1: Методы обнаружения [Электронный ресурс] <https://www.comss.ru/page.php?id=1259>
5. COMSS. Обнаружение вредоносных ссылок — Часть 2: Эвристическое обнаружение по расположению веб-ресурса [Электронный ресурс] <https://www.comss.ru/page.php?id=1260>
6. ЦБ РФ. Сведения об адресах Web-сайтов кредитных организаций Российской Федерации по состоянию на 30.09.2017 [Электронный ресурс] http://cbr.ru/credit/CO_SitesFull.asp
7. Официальный сайт PhishTank. [Электронный ресурс] <http://www.phishtank.com/>
8. Официальный сайт OpenPhish. [Электронный ресурс] <https://openphish.com/>
9. Rescan.pro. Исследование безопасности 50 тыс. сайтов рейтинга Alexa в зоне.ru. [Электронный ресурс] <https://goo.gl/9MYSwx>
10. Webroot. The 2017 Webroot Threat Report. [Электронный ресурс] https://www.webroot.com/download_file/view/946
11. Netresec. Domain Whitelist Benchmark: Alexa vs Umbrella. [Электронный ресурс] <https://goo.gl/VXcrQo>
12. Блог Антона Лопаницина. Способы обхода проверки домена и IP адреса. [Электронный ресурс] <https://bo0om.ru/domain-and-ip-checker-bypass>
13. Virus Bulletin. It's 2016. Can we stop using MD5 in malware analyses? [Электронный ресурс] <https://www.virusbulletin.com/blog/2016/07/its-2016-can-we-stop-using-md5-malware-analyses/>
14. M. Stevens, E. Bursztein, P. Karpman, A. Albertini, Y. Markov. The first collision for full SHA-1. [Электронный ресурс] <https://shattered.io/static/shattered.pdf>
15. ЦБ РФ. «ФинЦЕРТ» Банка России. [Электронный ресурс] http://www.cbr.ru/credit/Gubzi_docs/main.asp?Prtid=fincert



**Константин
ЧУМАЧЕНКО**
генеральный директор
провайдера облачных
сервисов NGENIX

DDOS-АТАКУ ОСТАНОВИТ ОБЛАКО

КАК ОБЛАЧНЫЕ СЕРВИСЫ ЗАЩИЩАЮТ БАНКИ ОТ ХАКЕРОВ

Голливудское клише — грабители проникают в хранилище банка и грузят пачки денег в мешки — давно неактуально. Сердце современного банка — это не хранилище с «кэшем» и золотыми слитками, а информационная система, так что современные преступники своей целью выбирают ИТ-инфраструктуру банка.

Банковский сектор можно назвать лидером по скорости и объему внедрения технологий — то, что еще недавно было конкурентным преимуществом отдельных «технологичных» банков, сегодня стало стандартом. Так произошло с публичными клиентскими сервисами — клиенты банков привыкли, что на сайте или в мобильном приложении можно управлять своими финансами в режиме 24×7 365 дней в году.

DDOS-АТАКА — НАСКОЛЬКО УГРОЗА РЕАЛЬНА?

Банковские веб-сервисы являются очевидной мишенью для злоумышленников. Самый распространенный тип воздействия — DDoS-атака, то есть вывод

из строя инфраструктуры или приложений банка с помощью большого объема нелегитимного трафика. Такие атаки преступники используют для нарушения онлайн-транзакций, срыва электронных торгов, отвлечения внимания от внедрения вредоносного кода. Причина популярности DDoS-атак — простота и низкая стоимость их организации.

Аналитическая компания Neustar заявляет, что в прошлом году хотя бы с одной DDoS-атакой столкнулись 84% компаний в мире. По данным исследования компании Nexusguard за 2016 г., Россия лидирует по количеству таких атак. По статистике «Ростелекома», в России наиболее подвержены нападениям коммерческие компании, игровые сервисы и финансовый сектор, причем на долю последнего в 2017 году пришлось 20% DDoS-атак.

Растет не только количество, но и мощность сетевых атак. Хакеры совершенствуют инструментарий DDoS: если раньше вредоносный трафик шел в основном с зараженных персональных компьютеров, то теперь в ботне-

ты оказываются вовлечены домашние маршрутизаторы и даже IoT-устройства. В феврале этого года уязвимость в ПО Memcached, используемом сотнями тысяч веб-серверов по всему миру, породила рекордную на данный момент атаку в 1,3 Тбит/с.

От атак не застрахованы даже гиганты финансовой отрасли. В прошлом году онлайн-банк крупнейшего розничного банка Великобритании Lloyds Banking Group был выведен из строя преступниками, требовавшими у банка выкуп в биткоинах. Особо критичны DDoS-атаки для «цифровых» банков, сфокусированных на дистанционном обслуживании. Например, немецкий «цифровой» банк Fidor в 2014 году стал объектом нескольких крупных DDoS-атак с целью вымогательства. Когда банк заблокировал нелегитимный трафик, хакеры стали угрожать повысить мощность атаки, если банк не заплатит им выкуп в биткоинах. Когда банк отказался, они увеличили объем атаки до 85 Гбит/с, с чем банк не смог справиться. Онлайн-сервисы были недоступны в течение 8 часов и банку пришлось выполнять запросы клиентов по телефону и в социальных сетях.

КАК ЗАЩИТИТЬСЯ?

Рынок предлагает широкий выбор устройств для защиты от DDoS-атак.

**АНАЛИТИЧЕСКАЯ КОМПАНИЯ NEUSTAR
ЗАЯВЛЯЕТ, ЧТО В ПРОШЛОМ ГОДУ
ХОТЯ БЫ С ОДНОЙ DDOS-АТАКОЙ
СТОЛКНУЛИСЬ 84% КОМПАНИЙ В МИРЕ**

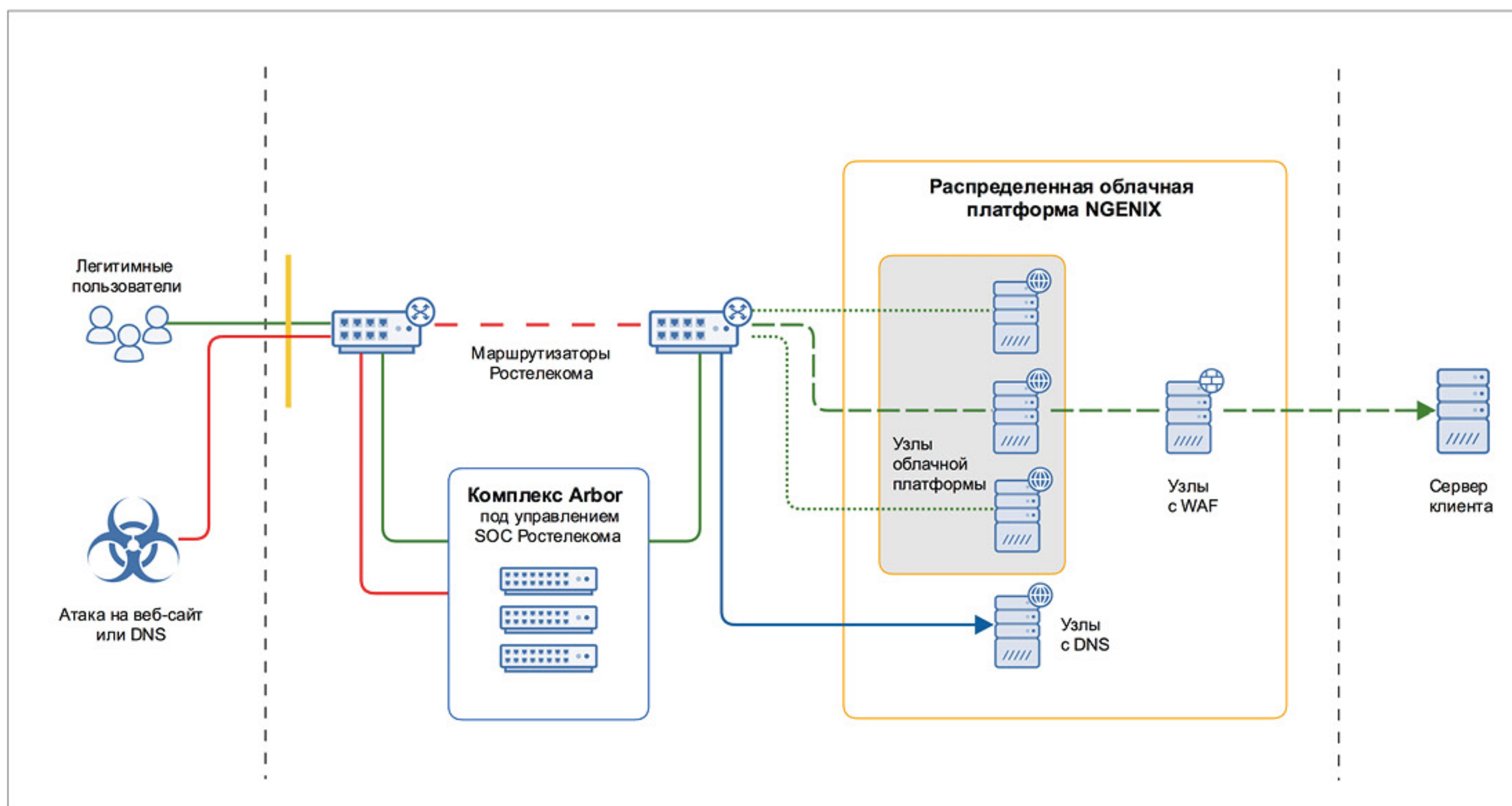


Рисунок 1. Облачная защита веб-ресурсов по сервисной модели

Однако собственная система не всегда способна справиться с атакой на сайт. Чтобы построить эффективное решение локально, нужны широкие каналы связи и высокопроизводительное сетевое оборудование, а также квалифицированный персонал. Такое решение никогда себя не окупит — атаки не происходят постоянно, а инфраструктура устаревает.

Еще один популярный вариант — заказ услуги защиты от DDoS-атак в дата-центре — тоже имеет подводные камни. Такая защита бесполезна, если мощность атаки превышает емкость каналов, ведущих в дата-центр. От действительно массовой атаки мож-

но защититься только если фильтровать вредоносный трафик на дальних подступах, например, на периметре сети крупного оператора связи. Чтобы обезопасить себя, крупнейшие компании используют одновременно несколько защитных систем. Это дорого и по силам только «тяжеловесам» бизнеса.

Оптимальным подходом является облачная защита веб-ресурсов по сервисной модели, что позволяет быстро получить высокий уровень безопасности без расходов на инфраструктуру. Такой комплекс защиты от DDoS-атак анализирует входящий на сайт трафик и, обнаружив подозрительную актив-

ность, перенаправляет аномальный трафик в систему очистки, не препятствуя доступу легитимных пользователей. В облачный сервис может входить защита от взлома с использованием межсетевых экранов уровня веб-приложений (WAF) (рис. 1). Такой сервис не требует сложной интеграции, а расходы на апгрейд инфраструктуры и развитие средств защиты берет на себя провайдер. Кроме того, современные облачные сервисы защиты от DDoS-атак можно использовать без раскрытия данных, составляющих банковскую тайну.

BIS-КОММЕНТАРИЙ

Илья Титов, управляющий директор «Модульбанка»:

У NGENIX мощное решение, которое фильтрует трафик и обеспечивает первый эшелон защиты наших публичных веб-сервисов.

Если строить подобный защитный комплекс самостоятельно, то потребуются широкие каналы связи и высокопроизводительное сетевое оборудование. Потребуются квалифицированные инженеры для настройки фильтрации трафика и дальнейшего обслуживания решения. Это долго, дорого, а с новым сервисом NGENIX — ещё и незачем.

Важнейшей частью защиты от DDoS-атак операторского класса является сопровождение квалифицированными инженерами, имеющими практический опыт борьбы с киберугрозами. Мгновенный доступ к их компетенциям может оказаться решающим фактором в предотвращении последствий DDoS-атаки. Можно ожидать, что услуги центров мониторинга ИБ в ближайшем будущем станут логическим продолжением сервисной модели.

В ЗАЩИТУ OPEN SOURCE КОМПОНЕНТОВ



Дарья ОРЕШКИНА
директор по развитию
бизнеса WEB Control

СНИЖАЕМ СТОИМОСТЬ РАЗРАБОТКИ И УСКОРЯЕМ ВЫПУСК

Сегодня сложно представить себе разработку программного обеспечения без Open Source. Компоненты с открытым исходным кодом дают существенные преимущества в скорости выпуска программных продуктов. Разработчики не пишут код с нуля, если он уже опубликован и проверен сообществом. Однако, неконтролируемое применение Open Source влечет за собой повышенные риски безопасности программных проектов, в том числе и юридического характера.

Применение компонентов с открытым кодом сегодня является типовой практикой. Зачем писать код с нуля, если можно найти нужный исходник или библиотеку в публичных репозиториях и зачастую бесплатно? Однако, не так-то просто выбрать подходящий компонент, а в одном программном проекте их десятки и сотни. Требуется, чтобы компоненты были качественными, в них не было известных уязвимостей и лицензионные требования были подходящими. Без автоматизированных средств такие проверки занимают много времени у специалистов по безопасности и качеству ПО, разработчиков и юридического отдела.

СКАНИРОВАНИЕ КОДА

Еще в 2002 году стартап Black Duck Software представил решение Protex, которое позволяло идентифицировать открытый исходный код в программных продуктах. Сканер кода показывал фрагменты исходного кода, совпадающие с Open Source в его базе данных. Со временем стало ясно, что при таком подходе получается слишком много ложных срабатываний — фрагменты проприетарного и коммерческого кода

идентифицировались как фрагменты открытого кода. В дополнение стали появляться сервисы, корректирующие результаты проверки в ручном режиме.

Вскоре свои решения стали предлагать и другие компании: Protecode (сейчас является частью Synopsys), Palamida (приобретена компанией Flexera Software) и Open Logic (приобретена компанией Rogue Wave).

НЕПРЕРЫВНОЕ УПРАВЛЕНИЕ КОДОМ

Со временем, доля Open Source в программных проектах увеличилась, безопасности компонентов стало уделяться больше внимания, практика копирования фрагментов кода утратила актуальность, а технологическая методика непрерывного развертывания получила широкое распространение.

Настоящую технологическую революцию совершила в 2011 году компания WhiteSource, представив свою разработку на основе agile-методологии. Решение получилось интуитивно понятным и доступным, встраивается на

всех стадиях жизненного цикла разработки ПО (SDLC) для оперативного обнаружения проблем. Благодаря WhiteSource появилась возможность блокировать неподходящие компоненты с открытым исходным кодом до добавления их в программный проект, что позволило существенно снизить стоимость разработки (рис. 1).

Open Source библиотеки и исходные коды выявляются по цифровым сигнатурам. Процесс управления компонентами с открытым кодом автоматизирован, начиная со стадии одобрения и заканчивая отслеживанием ошибок после развертывания.

При выборе подходящего инструмента для управления Open Source, нужно сосредоточиться на таких параметрах решения, как:

- ◆ Возможности по обнаружению компонентов
- ◆ Качество обнаружения уязвимостей
- ◆ Управление лицензионными рисками
- ◆ Возможности «Shift Left»
- ◆ Автоматизация и политики

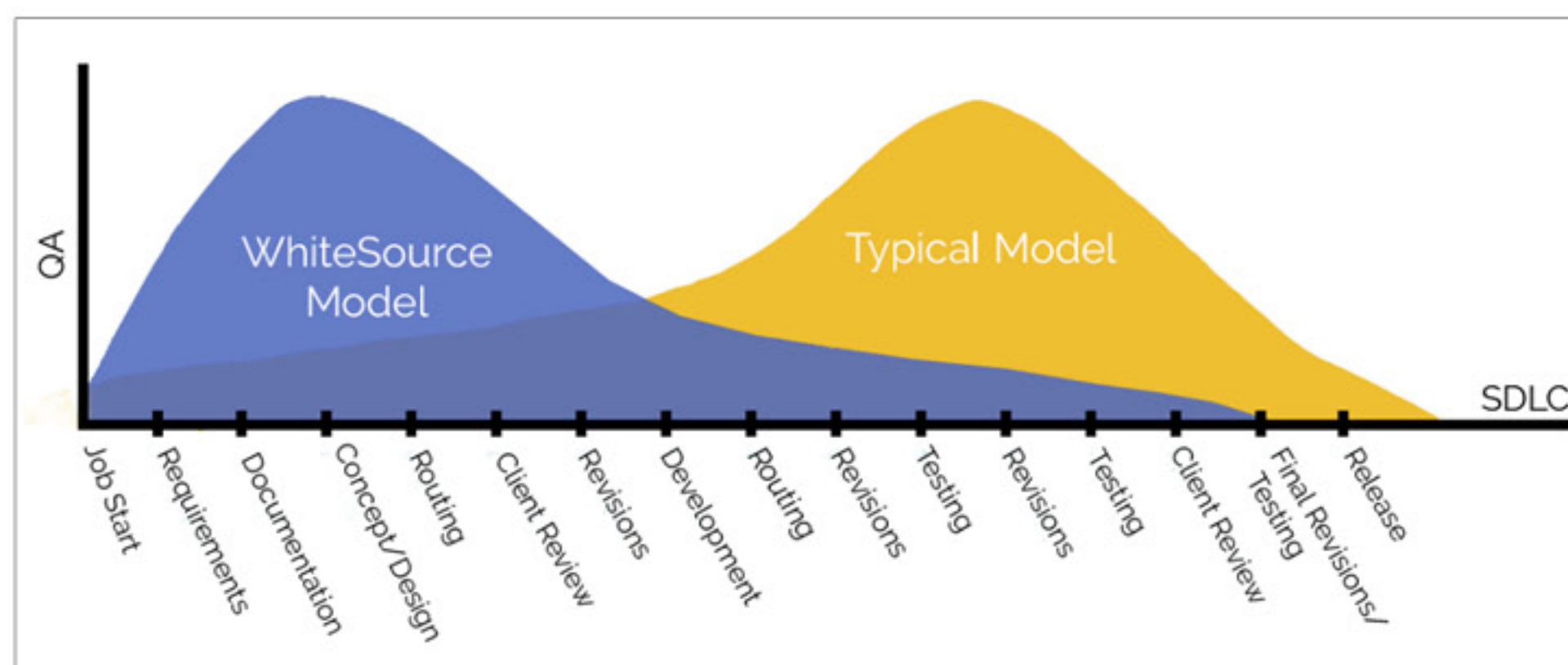


Рисунок 1. Стоимость исправления проблем безопасности и качества значительно возрастает по мере продвижения цикла разработки

1. ВОЗМОЖНОСТИ ПО ОБНАРУЖЕНИЮ КОМПОНЕНТОВ

Для обеспечения полного контроля за уязвимостями открытого кода и лицензионными соглашениями необходимо провести инвентаризацию в вашем программном продукте, которая позволит получить точный отчет об используемых компонентах, включая связанные объекты.

WhiteSource элементарно интегрируется с репозиториями и системами сборки для обнаружения всех компонентов открытого ПО, включая наследуемые связи, на основе действительного, а не заявленного использования.

Решение поддерживает свыше 20 языков программирования, включая исходный код. Содержит информацию о более, чем 3 млн компонентов открытого ПО и 70 млн файлов с открытым кодом. База данных о компонентах обновляется ежедневно.

WhiteSource может быть установлен на сервере компании, размещаться на виртуальном сервере в облаке или использоваться как SaaS-решение.

Сканеры кода находят фрагменты кода, совпадающие с фрагментами открытого кода, размещенными в их базах данных. Для исключения ложных срабатываний необходима ручная проверка, которая может занять довольно много времени. Любой компонент, добавленный в репозиторий между проверками, долго остается необнаруженным. Сама процедура сканирования проводится периодически, в основном перед релизом.

Системы управления артефактами. Обнаружение происходит в сборке на основе фактического применения. Некоторые инструменты способны находить компоненты в репозиториях. Большинство этих инструментов поддерживают только бинарный код. Большинство вендоров предлагают как локальное развертывание решения, так и хостинг (в облаке).

2. КАЧЕСТВО ОБНАРУЖЕНИЯ УЯЗВИМОСТЕЙ

Ежегодно становится известно о сотнях уязвимостей в компонентах Open Source. И хотя разработчикам в большинстве случаев удается их быстро



Рисунок 2. Принцип работы WhiteSource

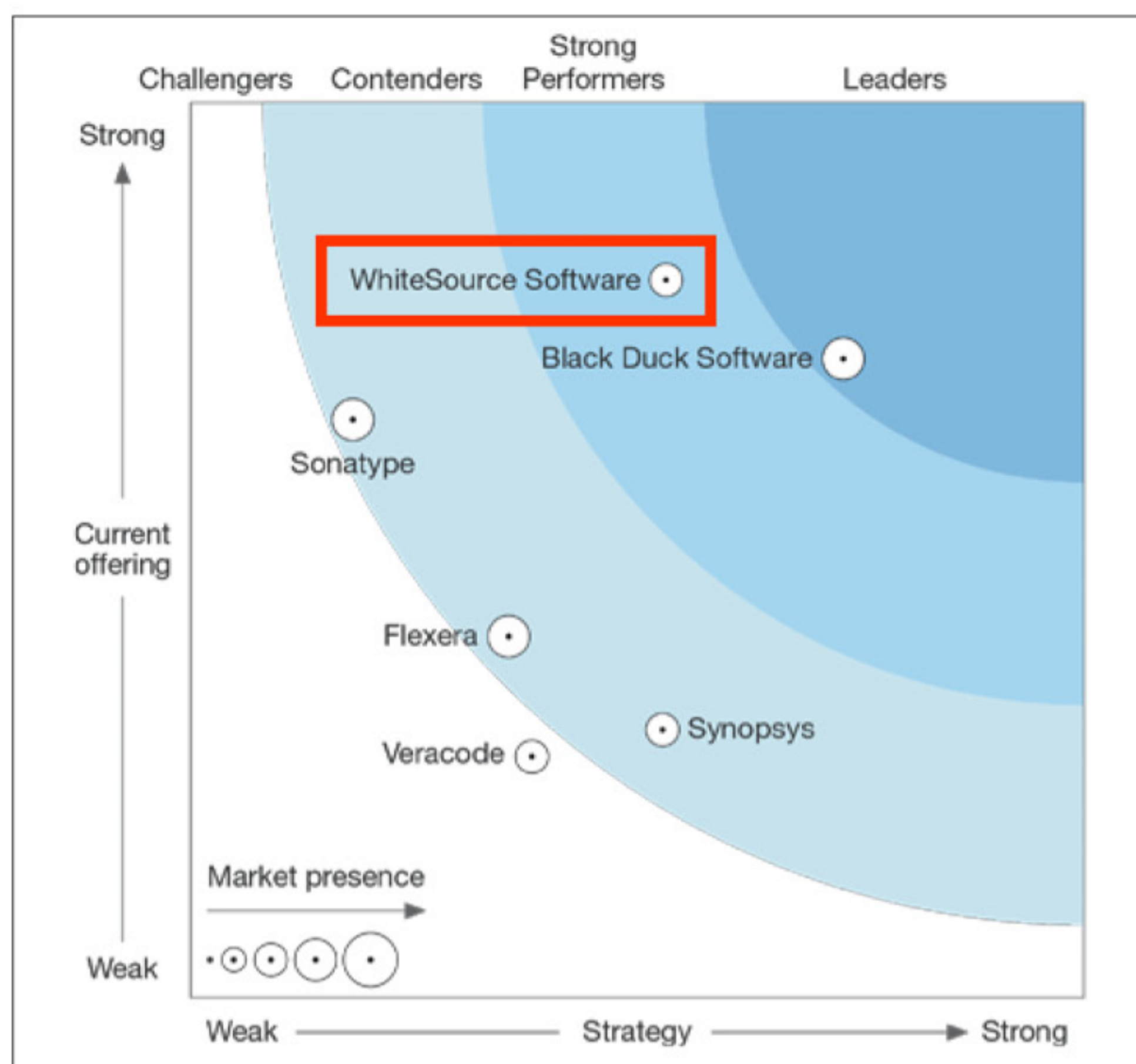


Рисунок 3. The Forrester Wave™: Software Composition Analysis (SCA) Q1 2017

устранять, при увеличении объема Open Source поиск уязвимостей становится все сложнее и важнее. Ни для кого не секрет, что уязвимость в одном Open Source компоненте помогает злоумышленникам скомпрометировать множество систем.

WhiteSource использует множество источников сведений об уязвимостях — NVD, бюллетени безопасности, треке-ры GitHub и других Open Source проектов. На сегодняшний день в базе насчитывается свыше 180 тыс. известных уязвимостей.

Уникальная технология WhiteSource гарантирует отсутствие ложных результатов, поскольку на наличие уязвимостей проверяется каждая в отдельности версия компонента. При этом система реагирует как непосредственно при попытке добавления уязвимого компонента в проект, так и при обнаружении уязвимости в будущем. Обратите внимание, что отслеживание компонентов продолжается даже после выпуска релиза для обнаружения проблем с безопасностью после финальной сборки.

Сканеры кода в большинстве своем отслеживают только NVD, поэтому их базы уязвимостей существенно меньше, и они не способны гарантировать высокую точность проверки. Безопасность обеспечивается только на момент сканирования.

Системы управления артефактами также зачастую отслеживают только лишь NVD и, соответственно, высокой точностью обнаружения уязвимостей не обладают.

НЕХИТРЫЕ РАСЧЕТЫ ПОКАЗЫВАЮТ, ЧТО ИСПРАВЛЕНИЕ УЯЗВИМОСТЕЙ И ОШИБОК НА РАННИХ СТАДИЯХ РАЗРАБОТКИ ОБХОДЯТСЯ ДО 90% ДЕШЕВЛЕ, НЕЖЕЛИ ПОСЛЕ ВЫПУСКА ИЛИ РАЗВЕРТЫВАНИЯ ПО

License Breakdown				
Name	Occurrences	Copyright	Patent	Royalty Free
Requires Review	20	-	-	-
Eclipse 1.0	9	78	80	conditional
GPL 2.0	4	78	60	no
GPL 3.0	2	78	20	yes
GPL 2.0 Classpath	1	78	60	no
LGPL 2.1	14	65	20	conditional
LGPL 3.0	1	65	20	yes
CDDL 1.0	1	65	60	conditional
MIT	151	39	20	yes
Apache 2.0	97	39	20	conditional
ISC	18	39	60	no
BSD 3	8	39	60	no
Mozilla 1.1	4	52	40	yes
BSD 2	1	39	60	no
Public Domain	1	13	60	no
Mozilla 2.0	1	52	40	yes

Рисунок 4. В помощь юристам

3. УПРАВЛЕНИЕ ЛИЦЕНЗИОННЫМИ РИСКАМИ

Оценка риска нарушения лицензионных соглашений постепенно становится регулярной процедурой перед выпуском ПО, поэтому юристам необходимо автоматизированное решение, чтобы идти в ногу с непрерывным развертыванием программных продуктов.

Увеличение видов лицензий открытого ПО, множественность версий лицензий в компонентах и объем кода, опубликованный без упоминания условий использования, весьма осложняют отслеживание лицензионного соответствия.

WhiteSource отображает лицензии всех Open Source компонентов и связанных объектов по всем проектам или по разрабатываемым программным продуктам в отдельности. Если обнаружено более одной лицензии в компоненте, то представляются все найденные лицензии. Инструменты анализа рисков по каждой лицензии

оптимизируют затраты юридического отдела. По каждой сборке ПО генерируются такие отчеты, как правовой анализ с перечнем лицензий, распределение лицензий по проектам и прочие.

Сканеры кода отображают лицензии всех компонентов, при этом отмечается высокий процент ложных срабатываний, поэтому необходим ручной анализ. Процесс генерации правовых отчетов автоматизирован частично, а результаты безошибочны только на момент последнего сканирования.

Системы управления артефактами в основном делают акцент на вопросах безопасности, а возможности управления лицензионными рисками ограничены.

4. ВОЗМОЖНОСТИ «SHIFT LEFT»

Раннее обнаружение (Shift Left) предполагает проведение тестирования на более ранних стадиях процесса разработки ПО, когда исправление проблем проще и дешевле. Нехитрые расчеты показывают, что исправление уязвимостей и ошибок на ранних стадиях разработки обходятся до 90% дешевле, нежели после выпуска или развертывания ПО.

Выявление проблемных компонентов перед добавлением в репозиторий или сборку позволяет улучшить качество программного проекта и повышает вероятность выпуска программного обеспечения в назначенный срок.

WhiteSource выполняет анализ рисков для каждой версии компонента при просмотре сетевых репозиторий (GitHub, Maven Central и т.д.), делает оценку качества и соответствия политикам компании.

Сканеры кода не интегрируются в CI/CD процесс, а могут только анализировать отдельную точку во времени — в момент последнего сканирования. Некоторые вендоры предлагают собственные каталоги Open Source, что усложняет интеграцию систем.

Системы управления артефактами имеют различные варианты интеграции, но нет решения, позволяющего разработчикам обнаруживать и блокировать проблемные компоненты на этапе выбора.

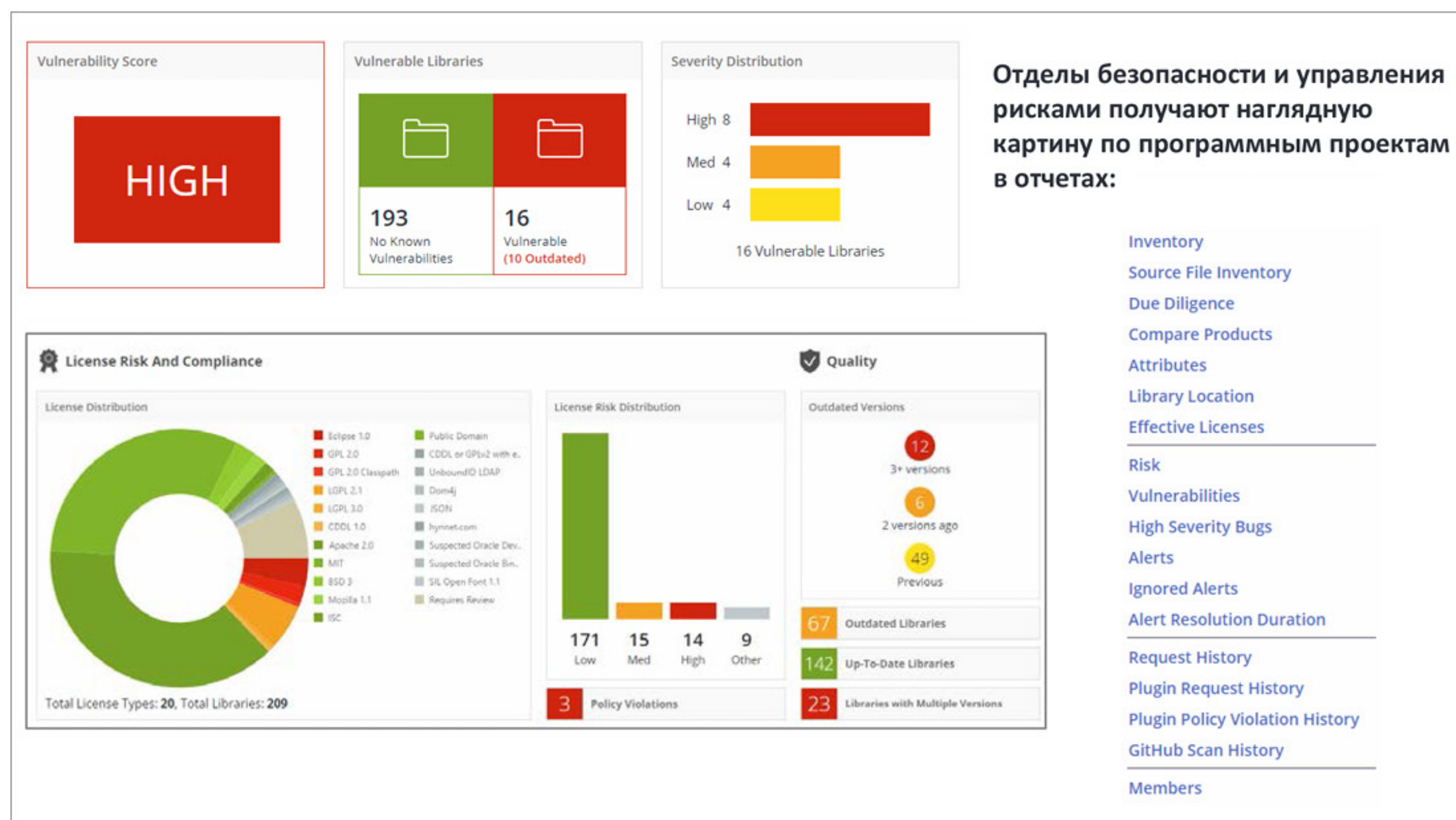


Рисунок 5. Анализ рисков по компонентам Open Source в проекте

5. АВТОМАТИЗАЦИЯ И ПОЛИТИКИ

Автоматизированная система управления открытым ПО является критически важной, она не только защищает от человеческих ошибок, но и ускоряет процесс разработки. Ручные процессы дорогостоящие и не позволяют обнаружить проблемы с безопасностью и качеством в режиме реального времени.

WhiteSource предлагает большое разнообразие плагинов с полной автоматизацией, включая соответствие сборки политикам компании. Политики могут быть основаны на любых сочетаниях параметров метаданных, таких как тип лицензии, уровень критичности уязвимости, оценки качества компонентов Open Source. Они могут автоматически устанавливаться на различных стадиях жизненного цикла создания продукта (SDLC). На основании установленной политики может создаваться заявка в баг-трекере. REST API обеспечивает гибкую интеграцию решения в инфраструктуру с учетом специфики компании.

Сканеры кода не интегрируются с CI/CD процессами, хотя в ручном

ПОЛИТИКИ МОГУТ БЫТЬ ОСНОВАНЫ НА ЛЮБЫХ СОЧЕТАНИЯХ ПАРАМЕТРОВ МЕТАДАННЫХ, ТАКИХ КАК ТИП ЛИЦЕНЗИИ, УРОВЕНЬ КРИТИЧНОСТИ УЯЗВИМОСТИ, ОЦЕНКИ КАЧЕСТВА КОМПОНЕНТОВ OPEN SOURCE

режиме некоторые могут отслеживать сборку после сканирования. Политики можно устанавливать для обнаружения проблемных компонентов после сканирования, но они не будут исполняться автоматически.

Системы управления артефактами предусматривают различные средства интеграции, но возможности автоматизации в части применения политик ограничены.

WhiteSource, будучи первым инструментом непрерывного обнаружения уязвимостей в программном обеспечении с открытым кодом, обладает самой наработанной базой данных.

Сегодня это, пожалуй, единственное решение, которое позволяет обеспечить защиту без ложных срабатываний.

Процесс защиты и управления компонентами происходит на всех стадиях жизненного цикла разработки ПО: от стадии выбора компонентов, в течение разработки и даже после развертывания ПО. Плагины WhiteSource интегрируются со всеми распространенными репозиториями, инструментами сборки и серверами CI/CD.

Специалисты по безопасности, тестировщики, разработчики и юристы гарантированно оценят должным образом наглядность, простоту и надежность решения WhiteSource.



Игорь ЛЕГЕЗИН
директор направления
информационной безопасности
компании «Диасофт»



БИЗНЕС-ПРОЦЕССЫ ПОД ПРИЦЕЛОМ

КАК ПОСТРОИТЬ ЭФФЕКТИВНУЮ СИСТЕМУ ЗАЩИТЫ
БАНКА ОТ СОВРЕМЕННЫХ ЦЕЛЕВЫХ АТАК

Самый безопасный банк — тот, который закрыт на ключ, а еще лучше — залит бетоном. Но вот незадача: любая активность подразумевает определенную свободу действий и, как следствие, приводит к возникновению уязвимостей. А с развитием дистанционного банкинга и расширением digital-каналов количество уязвимостей растет в геометрической прогрессии. Атаки сегодня нацелены в конкретную уязвимую точку бизнес-процесса. Как меняется вектор угроз, и что делать банку для защиты от новых видов мошенничества?

Случаев хищений в банках, совершенных внутренними злоумышленниками, по статистике, больше, чем при внешних проникновениях. Приведу пример из моей профессиональной практики. Сотрудник банка украл деньги. В ходе расследования, по заключению службы ИБ, выясняется, что аномальной активности в системе зафиксировано не было — «забор» (защита внешнего контура) цел. По словам сотрудников IT, все права доступа получены штатно, а представители службы охраны заверяют: человек прошел проверку. Но факт остается фактом — деньги украдены. Как же так? Перечень

возможных причин можно легко сократить до двух, наиболее вероятных: вор проник через «дырку в заборе», о которой еще не догадываются сотрудники службы ИБ, или воспользовался недостатками системы контроля выполняемого бизнес-процесса.

СОВРЕМЕННЫЕ АТАКИ ЕЩЕ НЕ ИЗУЧЕНЫ

Современные атаки прицельны, они направлены на конкретные точки бизнес-процессов и работают по еще не изученным мошенническим схемам. Конечно, без систем охраны периметра можно забыть о безопасности в прин-

ципе, но защита внешнего контура от типовых угроз сегодня уже не обеспечивает должную защищенность. В случае целевой атаки такая защита может не сработать вообще.

Банк — не монолитная система. Точками атак для злоумышленников становятся, как правило, стыки систем — часто это шлюзы для межбанковских операций и обмена платежами с Банком России, SWIFT и другими системами, например, карточного процессинга с АБС. Если для защиты бизнес-процессов внешнего взаимодействия использовать универсальные средства, не понимая самого процесса, прицельные атаки будут пропущены. При этом канал внешнего обмена может быть защищен, а вот перемещаемые между системами файлы — оставаться уязвимыми. Именно это, зачастую, становится причиной подмены их содержимого. Такие инциденты пытаются предотвращать средствами операционных систем, путем ограничения доступа. Но последние известные случаи атак во многом дискредитировали такой способ защиты. Первым действием злоумышленника было получение прав уровня системы, что делало все файлы доступными для чтения и модификации.

Укрепление защиты шлюза или содержимого файла обмена смещает направление вектора угроз на системы, его формирующие или принимающие.

ПРИНЦИПЫ ПОСТРОЕНИЯ СОВРЕМЕННОЙ ЗАЩИТЫ БАНКА

Если проанализировать успехи современных атак, становится очевидно: каждой из них предшествовала серьезная аналитическая работа. Грубо говоря, мошенники искали, куда «ударить». Исходя из этого, логично предположить, что максимальной эффективности вложений в обеспечение безопасности можно добиться при защите конкретных бизнес-процессов и наиболее критичных мест в них.

Разумнее всего начать с анализа бизнес-процессов банка, чтобы найти те «узкие места», которые могут быть атакованы. Вокруг этих условных точек для возможного вывода денег и нужно строить систему защиты. Порой достаточно внести лишь некоторые измене-

СОВРЕМЕННЫЕ АТАКИ ПРИЦЕЛЬНЫ, ОНИ НАПРАВЛЕННЫ НА КОНКРЕТНЫЕ ТОЧКИ БИЗНЕС-ПРОЦЕССОВ И РАБОТАЮТ ПО ЕЩЕ НЕ ИЗУЧЕННЫМ МОШЕННИЧЕСКИМ СХЕМАМ

ния в бизнес-процесс, чтобы устранить уязвимую часть или практически исключить возможность ее использования в деструктивных целях.

ОБРАТИТЕСЬ К РАЗРАБОТЧИКУ

Аудит бизнес-процессов целесообразнее проводить совместно с разработчиком АБС, который досконально знает систему и сможет проанализировать их быстрее и, главное, тщательнее. Найденные в процессах слабые места также эффективней устранять при участии вендора. Стороннее ПО, установленное вне системы, но имеющее неконтролируемый доступ к базе данных, создает условия для успешной атаки.

При подключении стороннего ПО банк всегда может обратиться к поставщику АБС, который предоставит адаптер для контролируемого и безопасного выполнения строго заявленных функций.

От взаимодействия с разработчиком банк получает и сопутствующий бизнес-эффект. Нередки случаи, когда после аудита бизнес-процессов обмена двух систем выясняется, что в нескольких местах, кроме недостатка в безопасности, производятся лишние действия, которые серьезно замедляют обработку. А это уже основание для оптимизации всего процесса.

СРЕДСТВА ДИАГНОСТИКИ И ЗАЩИТЫ УЯЗВИМЫХ ТОЧЕК БИЗНЕС-ПРОЦЕССОВ

Как мы выяснили, чтобы противостоять современным атакам, недостаточно использовать решения для защиты от универсальных угроз. Целесообразно применять продукты, которые защитят бизнес-процессы банка. Нет смысла долго искать партнера для создания системы ИБ, отвечающей современным реалиям и не предполагающей глобальной трансформации ИТ-системы. Мало кто сможет разобрать их на «мо-

лекулы» лучше, чем разработчик вашей АБС, не говоря уже об изменениях внутри системы.

Системы «Диасофт» работают во многих ведущих банках России и практически в каждом третьем из списка топ-100. С учетом опыта работы на банковском рынке, на фоне участвовавших изоощренных кибератак, в 2017 году мы создали центр компетенции по информационной безопасности. За год мы не только укрепили защиту использования продуктов компании, но и создали пул отдельных решений в сфере ИБ.

В портфолио продуктов «Диасофт» есть эффективные инструменты для защиты наиболее проблемных точек бизнес-процессов банка. Так, мы готовы защитить каналы вывода средств, обеспечив криптозащиту файлового обмена с внешними системами (АРМ КБР-Н и SWIFT), систем внутренних платежей, межсистемного обмена, внедрить усиленную аутентификацию и проверку действий сотрудников, участвующих в наиболее критичных бизнес-процессах.

Необходимо купировать возможную атаку уже при первых признаках нестандартной активности. Но что такое нестандартная активность? Если изменить в платеже какие-то данные, обычная система аналитики может этого не заметить. Сотрудник отправлял тысячи платежей, и этот не выбьется из статистики. Эффективно работающая система должна не только фиксировать факт внесения каких-то изменений, но и уметь распознавать потенциально опасные действия и операции.

РОБОТ В ПОМОЩЬ

Если через контролера ежечасно проходят сотни и тысячи платежей, и каждый он просматривает за доли секунд, становится ясно, что контроля нет. Мы даем ему в помощь робота — решение,

построенное по принципу фильтров, которые при настройке позволяют собирать потоки платежей, делить их на потенциально опасные и безопасные, направляя затем в зоны «красного и зеленого коридоров» соответственно. На проверку контролеру поступают только те операции, которые не соответствуют критериям «зеленой» зоны или попали в «красную». В зависимости от настроек, система может отправить критичные несоответствия на дополнительный контроль в службу ИБ либо остановить операцию. Критерии определяет сам банк, возможно, с нашей помощью, учитывая историю прошлых инцидентов и лучшие практики «Диасофт» в обеспечении защиты банковских систем. Робот служит как бы дополнительной «парой глаз» (кроме оператора и контролера) к прописанным нормативами Банка России «четырем глазам защиты». Так мы обеспечиваем защиту внутри системы банка.

MESSAGE GUARD, LAU, DATA BASE GUARD...

В июне прошлого года Межрегиональный центр обработки информации ЦБ РФ выпустил информационное письмо о разработке новой версии программного обеспечения комплекса АРМ КБР-Н для участников обмена электронными сообщениями при переводе денежных средств через платежную систему Банка России. Защитить канал внешнего взаимодействия с платежной системой ЦБ РФ позволит решение Message Guard «Защита электронных сообщений». Оно использует криптографическую защиту информации, передаваемой ИТ-системой на бесфайловом уровне, что исключает возможность подмены или изменений документа.

В обмене документами SWIFT угрозу подлога электронных сообщений можно предотвратить с помощью технологии LAU, реализованной в продуктах «Диасофт». Включение такой защиты в ПО SWIFT станет обязательным.

Следующий уровень безопасности — защита доступа в базы данных. Для этого «Диасофт» разработал Data Base Guard — средство контроля активно-

сти, сервер, который анализирует всю информацию при запросе или передаче ее в базу данных. Мы можем отслеживать не только изменения текста запросов, но и нетипичные суммы, номера счетов и т.д. При этом фиксируются не только изменения, но и сам факт доступа к данным конкретных клиентов и их счетам (VIP, «якорные» клиенты, «клиенты-локомотивы» и т.д.).

Большая проблема современной информационной безопасности связана с авторизацией пользователей паролями. Вычислительные средства становятся все мощнее, в итоге даже 12-значный пароль может быть подобран за полмесяца, типичный же пароль из 6–8 знаков взламывается за секунды. Функционал платформы Diasoft FA# Beans дополняет процесс осуществления доступа к системе банка еще одним этапом аутентификации — так называемым «вторым фактором», который позволяет исключить возможность действий от имени другого пользователя даже при условии знания данных для входа. Мы внедрили в систему алгоритм временных паролей (TOTP), которые действуют одну минуту. Они генерируются мобильным приложением или специальным токеном, не использующим для своей работы сетевой обмен и исключающим возможность перехвата. Целесообразно применять этот механизм, зная уязвимые точки бизнес-процесса и понимая, какие его звенья могут быть атакованы. Это может защитить банк даже от современных уязвимостей, например, от троянских программ «нулевого дня», которые проникают в машину пользователя незаметно, перехватывают его логин, пароль и передают их злоумышленнику для атаки от имени пользователя. Классический антивирус такую атаку часто пропускает, так как имеет дело с новым видом вредоносного ПО, который еще не фигурирует ни в антивирусной базе, ни в алгоритмах определения подозрительной активности.

ЗАЩИТА АБС — ЗАЛОГ БЕЗОПАСНОСТИ

Каждый банк старается чем-то отличаться от конкурентов, и это ведет к значительной доле кастомизации

в ИТ-системах. В итоге, где-то строгий контроль есть, а где-то — нет. Мы разработали инструмент, который контролирует выполняемый код АБС от «Диасофт». Как только он находит в коде системы, отчетах или иных доступных для изменения кода местах скорректированный или неподписанный элемент, тут же сигнализирует об этом в лог АБС, службу ИБ и ИТ банка. Как правило, случаи несанкционированного изменения кода приводят к инцидентам, при злонамеренном изменении кода в АБС даже правильные действия сотрудника будут отображаться некорректно. Поэтому любое изменение кода, инициированное без участия служб ИТ и ИБ, подлежит расследованию. Мы создали это решение в ответ на изменение вектора угроз в сторону АБС и ее СУБД. Функционал защиты кода предоставляется клиентам в рамках договора сопровождения. Ценно то, что такая мера предотвращает угрозы, от которых другой адекватной защиты сегодня не существует.

Следующий шаг в усилении защиты АБС — дополнительная криптозащита критичной информации. Разумеется, мы уже сейчас поддерживаем стадии ее жизненного цикла. В соответствии с требованиями закона № 152-ФЗ «О персональных данных», в продуктах «Диасофт» реализованы отзыв обработки, удаление и обезличивание персональных данных с контролем наличия действующих контрактов и сроков действия согласий на обработку. Для пользователей систем реализовано упорядочивание прав доступа в роли с возможностью гибкой адаптации набора прав при перемещении сотрудников или изменениях в бизнес-процессах с их участием.

* * *

Компания «Диасофт» разрабатывает решения так, чтобы они не влияли (или влияли минимально) на производительность систем и бизнес-процессы банка. В большинстве случаев, решения служат инструментом контроля и оповещения о подозрительной активности. Право предпринимать дальнейшие действия неизменно остается за банком.



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

#ИстиннаяБезопасность

© АО «Лаборатория Касперского», 2018. Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей

УРАЛЬСКИЙ ФОРУМ ЗА 15 МИНУТ



Алексей ЛУКАЦКИЙ
эксперт информационной безопасности

ЧЕМ БУДЕТ ЖИТЬ ОТРАСЛЬ
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ ФИНАНСОВОЙ
СФЕРЫ В БЛИЖАЙШИЕ ГОДЫ



12 –16 февраля в Башкирии прошел X Уральский форум «Информационная безопасность финансовой сферы». Организатором мероприятия стал Банк России при поддержке Аппарата Правительства РФ, Государственной думы РФ, Минкомсвязи России, МВД России, Роскомнадзора, ФСБ России, ФСТЭК России и Россвязи. Организационную поддержку форуму оказала Медиа Группа «Авангард».

Гуру отечественной ИБ Алексей Лукацкий в своем традиционном заключительном выступлении подвел основные итоги форума. Публикуется с сокращениями.

АКТИВНОЕ ТЕХНОЛОГИЧЕСКОЕ РАЗВИТИЕ БАНКА РОССИИ

Появление новых сервисов прибавит работы для финансовых организаций и служб информационной безопасности. Добавятся задачи, связанные с обеспечением безопасного и надежного подключения к новым платформам. Сервисы (финансовые маркетплейсы и технологии распределенных реестров), анонсированные Ольгой Скоробогатовой, потребуют особой защиты.

СТАНДАРТИЗАЦИЯ И НАПРАВЛЕНИЯ РЕГУЛИРОВАНИЯ ИБ

За всеми разработанными сервисами регулятора последуют новые положения, указания и стандарты ЦБ. На ближайшие 5 лет запланирована выработка 15 стандартов, в рамках ЦБ и ТК-122 разработана дорожная карта по развитию этих стандартов. Они разбиты на 6 ключевых направлений: киберриски, информационная безопасность, аутсорсинг, стандарты по управлению инцидентами, документы, связанные с непрерывностью, и мониторинг. Все стандарты придется выполнять.

МАЛЕНЬКИЙ СЕКРЕТ ПРО ВЫПОЛНЕНИЕ ГОСТОВ

Если ГОСТ вступает в силу с 1 января, это не значит, что нужно прямо сейчас его выполнять, к нему надо присматриваться, начинать выполнять для соответствия ему определенные мероприятия, но обязательным он станет только тогда, когда ссылку на него включат в специальное Положение Банка России.

УПРАВЛЕНИЕ КИБЕРРИСКАМИ

Еще одна идея, которая была озвучена больше года назад, связана с тем, чтобы «поднять» безопасность на уровень правлений банков или исполнительных органов других финансовых организаций, поскольку киберриски могут

**X УРАЛЬСКИЙ ФОРУМ
В ДВУХ СЛОВАХ:****Зампред Банка России
Дмитрий Скобелкин:**

♦ Банк России создаст Департамент информационной безопасности, куда войдет ФинЦЕРТ и ряд других подразделений регулятора. Кроме того, появится Центр компетенции по обеспечению киберустойчивости организаций кредитно-финансовой сферы.

♦ При установлении показателей значимости для организаций кредитно-финансовой сферы будут учитывать среднее количество операций, осуществляемых субъектом КИИ.

♦ С 1 июля 2018 года операторы по переводу денежных средств и операторы услуг платежной инфраструктуры будут уведомлять Банк России об инцидентах мошенничества при переводе денежных средств.

♦ Банк России намерен возвращать средства, похищенные у российских кредитных организаций и выведенные за рубеж, через Росфинмониторинг. Для этого будет использоваться система взаимодействия финразведок по всему миру.

♦ Планируется реализовывать программы переподготовки ИБ-специалистов, включающие не менее 500 учебных часов. Кроме того, будут разработаны методики и программы тестирования специалистов и руководителей ИБ-подразделений, а также профстандарты «Специалист по кибербезопасности».

♦ За 2017 год атакам Cobalt Strike подверглись 240 кредитных организаций, из них в 11 случаях атаки были успешными. Общая сумма хищений составила более 1 млрд 156 млн рублей.



За 4 дня деловой программы на форуме прозвучало более 70 докладов, прошло 13 тематических сессий, 5 дискуссий и 11 мастер-классов

нанести ущерб деятельности финансовой организации. Соответственно, если данный момент организация не учитывает, значит необходимо резервировать капитал, вести базу данных, оценивать риски по методике Банка России. Становится понятно, что, чем хуже управление рисками, тем больше денег резервируется, а значит, они не «работают», финансовые показатели организации становятся хуже.

**ИНЫЕ ПРОЕКТЫ
НОРМАТИВНО-
ПРАВОВЫХ АКТОВ**

Они готовятся самим регулятором либо при его участии. Во-первых, новая редакция 382-П, имеющая 2 версии: новую и перспективную. Изменения: деление контуров безопасности, пере-

ход от самооценки к внешнему аудиту и оперативность подачи информации об инцидентах в ФинЦЕРТ. Это заставит пересмотреть процедуры по управлению инцидентами.

Ключевое отличие перспективной редакции от новой — это ссылки на ГОСТ. С момента, когда ссылки на ГОСТ появятся в редакции 382-П, ГОСТ станет обязательным.

Кроме того, в январе прошел первое чтение законопроект о внесении изменений и дополнений в законодательные акты, где имеется ряд ключевых положений:

♦ введение глобальной национальной антифрод системы. Её регулированием и направлением индикаторов мошеннических операций займется Банк России;



Юбилейный форум собрал более 550 ИБ-специалистов из более чем 20 городов России

- ♦ возврат несанкционированно переведенных денежных средств;
- ♦ обмен информацией о компьютерных атаках с использованием сервиса ФинЦЕРТ;
- ♦ необходимость уведомлять регулятора о мошеннических операциях, а не только об инцидентах ИБ.

РАСШИРЕНИЕ ПОЛНОМОЧИЙ РЕГУЛЯТОРА НА ВСЕ ФИНАНСОВЫЕ ОРГАНИЗАЦИИ

Если сейчас Банк России может устанавливать требования по ИБ только для кредитных организаций и участников МПС, то с принятием этого закона («О внесении изменений в отдельные законодательные акты РФ») у него появится право устанавливать требования и для всех остальных организаций: страховых компаний, негосударственных пенсионных фондов, брокеров, микрофинансовых организаций и т.д.

ОТЧЕТНОСТЬ

Помимо существующей отчетности в рамках 552-П («О требованиях к защите информации в платежной системе Банка России») появится еще одна, более оперативная, по 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»).

Останется 203-я отчетность, в рамках которой нужно сообщать о суммах похищенных, готовящихся к хищению и возвращенных денежных средств раз в квартал или раз в полгода в зависимости от количества операций.

Планируется также отчетность о мошеннических операциях. Не стоит забывать и об отчетности ГосСОПКА, которая в перспективе будет осуществляться через ФинЦЕРТ, но пока отправляется напрямую.

ПРАВО БЛОКИРОВАТЬ САЙТЫ

Банк России получит право блокировать сайты, рекламирующие незаконные финансовые услуги. Проект закона, связанный с возможностью обмениваться информацией о мошенниках, о дропе без получения всяких согласий. Это — классическая тема, которая поднималась последние 6–7 лет, когда возникала тема с действиями антидроп-клуба, который обменивался информацией, но нарушал 152-ФЗ. Речь идет о необходимости просить у мошенника согласия для обмена информацией о нем. Разумеется, что мошенники согласий не дают. Сейчас этим законопроектом регулируется право обмениваться информацией без согласия субъекта, это будет делаться на основании ФЗ.

ХУРАЛЬСКИЙ ФОРУМ В ДВУХ СЛОВАХ:



Первый зампред Банка России Ольга Скоробогатова:

♦ В качестве основных внедряемых платформ Банк России рассматривает: финансовый маркетплейс, платформу для регистрации финансовых сделок, платформу быстрых платежей, перспективную платежную систему, Национальную систему платежных карт, систему передачи финансовых сообщений, единую систему идентификации и аутентификации (биометрическая платформа), сквозной идентификатор клиента, платформу облачных сервисов, платформу на основе технологии распределенных реестров.

♦ За 2017 год в 2,3 раза увеличилось число инцидентов информационной безопасности в финансовой сфере.

♦ В 2018 году мировые расходы на обеспечение информационной безопасности коммерческих организаций составят \$93 млрд0 (+8% по сравнению с 2017 г.).

♦ 40% российских компаний не имеют стратегии информационной безопасности (у банков эта цифра составляет менее 30%). К 2020 г. только 60% финорганизаций планируют инвестировать в ИБ.

♦ 89% банков относят деятельность по кибербезопасности и защите данных к приоритетной.

♦ К 2020 году потребуется 21 тыс. новых ИБ-специалистов.

♦ Банк России планирует полностью перейти на электронный документооборот с участниками финансового рынка в течение ближайших 3 лет.

**Х УРАЛЬСКИЙ ФОРУМ
В ДВУХ СЛОВАХ:****Зампред Банка России
Руслан Вестеровский:**

- ♦ Скорость изменения технологий составляет полгода, а образовательной программы — в среднем около двух лет. Если образовательная программа не отражает реальность, то специалист на рынке труда оказывается не востребованным.
- ♦ Для подготовки специалистов финансовой индустрии Банк России откроет базовые кафедры в 4–5 российских вузах.

**Начальник Управления
Департамента банковского
регулирования Банка России
Михаил Бухтин:**

- ♦ В 2018 году планируется установить требования к отдельной классификации событий киберриска в составе операционных рисков.
- ♦ С 2019 года банки будут обязаны предоставлять информацию по киберрискам в ДБР. А с 2020 г. данные риски должны учитываться при определении достаточности капитала банка.

**Руководитель SWIFT по России,
СНГ и Монголии Матвей Геринг:**

- ♦ Международная система банковских расчетов SWIFT совместно с ЦБ исследует систему приостановки подозрительных транзакций Payment control service. Это решение будет доступно начиная с июля-августа.

**Заместитель руководителя
Федерального агентства связи
Роман Шередин:**

- ♦ Классические банки никогда не будут предоставлять услуги связи.



Дискуссионная панель «ИБ как неотъемлемая часть цифровой экономики России»

**«О БЕЗОПАСНОСТИ
КРИТИЧЕСКОЙ
ИНФОРМАЦИОННОЙ
ИНФРАСТРУКТУРЫ»**

На основании этого Закона все финансово-кредитные организации являются субъектами, а информационные системы: АБС, процессинг, бухгалтерия, CRM — это объекты, однако не все из них являются значимыми объектами, на которые распространяются требования по информационной безопасности.

Тем не менее, независимо от наличия объектов, в качестве субъекта КИИ нужно осуществить 3 шага: категоризоваться, подключиться к ГосСОПКА, а затем выполнить требования по обеспечению безопасности.

С точки зрения категоризования, на Уральском форуме были показаны критерии, где только один пункт (десятый) касается кредитных организаций. На мой взгляд, важны три пункта в разделе «экономическая значимость», но не в полном объеме.

Я посчитал, на кого распространяется данный критерий:

- ♦ 31 финансовая организация с участием государства;
- ♦ один банк, который является стратегическим предприятием;

- ♦ 11 системно значимых кредитных организаций;

- ♦ 4 системно значимые инфраструктурные организации финансового рынка;

- ♦ 9 операторов услуг платежной инфраструктуры в системно и социально значимых платежных системах.

Собственно, есть несколько перечней организаций, которые подпадают под критерии. Но это не значит, что у этих организаций будут значимые объекты. Как минимум необходимо оценить себя, понять, есть ли у вас значимые объекты и какой они категории.

Кредитным организациям, которые не попадают в этот перечень, можно расслабиться с точки зрения выполнения требований по безопасности ФСТЭК, как для значимых объектов, но не стоит забывать о подключении к ГосСОПКА, поскольку этот закон распространяется на все субъекты без исключения.

Обратите внимание, что даже если у вас нет значимых объектов, вы все равно обязаны выполнять требования по безопасности, помимо требований ФСТЭК для объектов КИИ: 382-П, 21-й Приказ, PCI DDS, 552-П и т.д.



В демозоне форума были представлены 26 стендов ведущих ИБ- и ИТ-компаний, в том числе и стенд ФинЦЕРТ Банка России

УДАЛЕННАЯ ИДЕНТИФИКАЦИЯ

Доступ всех банков и Почты России к базе биометрических данных граждан Российской Федерации увеличивает риски хищения и подмены информации.

ДЕЯТЕЛЬНОСТЬ ФИНЦЕРТ

На базе ФинЦЕРТ будет создан центр компетенций финансовой сферы. Также я хочу обратить внимание на систему личных кабинетов, позволяющую более оперативно отдавать данные. И автоматизация вещей, связанных с рассылками.

ПОВЫШЕНИЕ КВАЛИФИКАЦИИ

Банк России взял под свое крыло тему повышения квалификации и разрабатывает ряд типовых программ как для рядовых сотрудников, так и для руководителей служб информационной безопасности в финансовой сфере. Но самое интересное — это создание системы

независимой аттестации и сертификации ИБ-специалистов. Эта тема будет разработана в перспективе трех лет, но к этому стоит готовиться.

ЦИФРОВАЯ ЭКОНОМИКА

Тема цифровой экономики, на мой взгляд, не проработана, примерно, как и документы по критической инфраструктуре. Я увидел несколько серьезных пунктов. Во-первых, разработка дорожной карты перехода всего российского интернета на российскую криптографию. Во-вторых, процедура обязательной оценки соответствия компонентов платежной инфраструктуры. В-третьих, тема работы с персональными данными. Вводится интересная норма — все операторы персональных данных обязаны либо иметь финансовую гарантию ответственности, либо страховать свои риски.

ЧТО НЕ УДАЛОСЬ УСЛЫШАТЬ?

Тему персональных данных и позицию ФСТЭК в отношении тематики КИИ.

Х УРАЛЬСКИЙ ФОРУМ В ДВУХ СЛОВАХ:



Заместитель начальника ГУБиЗИ Банка России
Артем Сычев:

♦ Банк России будет обмениваться с центральными банками стран ЕАЭС данными о рисках и угрозах информационной безопасности кредитно-финансовой сферы.

Глава Group-IB Илья Сачков:

♦ Уроки компьютерной безопасности в школах могут быть введены в 2022 году.

О чем еще не забыть?

♦ В 2019 году новый ГОСТ Р 57580.1 («Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер») станет обязательным.

♦ С 2019 по 2021 планируется выпустить серию национальных стандартов ГОСТ Р, которые будут регулировать процессы управления киберрисками и ситуационной осведомленностью.

♦ К 1 июля 2018 г. должна быть разработана новая редакция 382-П, которая будет включать контроль защищенности платежных приложений, обязательность внешнего аудита, оценку соответствия платежных приложений в части отсутствия недокументированных возможностей, необходимость оперативного уведомления об инцидентах (в течение дня), необходимость разделения контуров подготовки и подтверждения платежных поручений.

Материалы подготовила
Анна Воробьева

ИНФОФОРУМ 2018

О БЕЗОПАСНОСТИ ЦИФРОВОЙ РОССИИ:
НИКОГДА НЕ БЫЛО, И ВОТ СНОВА...

Достоинство площадки Инфофорума — сбор в одном месте представителей всех ведомств России, от которых зависит формирование и функционирование критической ИТ-инфраструктуры страны. Это позволяет в течение дня увидеть практически полную картину состояния ИБ в этой инфраструктуре, а за два дня — сделать выводы о том, что думает об этом состоянии профессиональное сообщество.

КАСТОМИЗАЦИЯ AB INITIO

Многие знания, приобретённые на форуме, порождают и многие печали. Лишь один высокопоставленный чиновник — заместитель начальника Центра ФСБ Н. Н. Мурашов, выйдя на трибуну, без обиняков заявил, что пришло время переходить от управления рисками в сфере ИБ к использованию безусловно безопасной ИТ-инфраструктуры. Похоже, что лицо этого человека организаторы форума оказались не готовы показать широкой публике (именно его фото не было представлено журналистам в завершающем пресс-пакете мероприятия), но его идеи заслуживают пересказа.

Путь к формированию безусловно безопасной информационной инфраструктуры — создание заказных (полностью кастомизированных) ИТ-систем, а не перелицовка коробочных решений под нужды конкретного заказчика.

Кастомизация ab initio (лат., с самого начала) позволит избежать появления в теле приложений избыточного кода, который часто и является причиной некорректной работы и лазейкой для сторонних проникновений, избежать существования в системе неиспользуемых интерфейсов — потенциальных «дыр» для партизанских атак хакеров и плановых боевых атак наших партнёров. Коренного пересмотра требует и практика аутсорсинга в сфере ИТ — сегодня он превратился в эффективный

инструмент для деловых злоупотреблений и источник проблем для ИБ.

Конечно, принцип кастомизации ab initio не должен доводиться до абсурда. И подобно тому, как при создании стратегической ракеты возможно частичное использование стандартных материалов (после их соответствующего анализа и испытаний), так и наличие документированного фонда программных компонентов и базового доверенного «железа» позволит снизить стоимость кастомизированных и безусловно безопасных ИТ-систем.

«ПРОСВЕЩЕНИЕ ВНЕДРЯТЬ С УМЕРЕННОСТЬЮ, ПО ВОЗМОЖНОСТИ ИЗБЕГАЯ КРОВОПРОЛИТИЯ»

Подавляющее же большинство докладчиков пленарного заседания исходили из того, что ИБ — это надёжный щит на вратах критической ИТ-инфраструктуры. И этот реактивный подход нельзя ставить им в упрек. Принцип единоточечности никто не отменял, и если даже банк-евангелист цифровой экономики содержит на своём балансе и увлечённо развивает «направление рисков кибербезопасности», то что делать ведомым структурам? Только ждать, когда мега-регулятор отдаст приказ «всем вдруг» повернуть на курс безусловной безопасности. Но пока такой команды не было.

Справедливости ради следует отметить, что в рамках парадигмы ИБ-щита «на воротах» ИТ-инфраструктуры доклады Минобороны, ДИТ Москвы, Банка России были профессиональны, интересны и каждый из них содержал свою изюминку.

ГУ развития информационных и телекоммуникационных технологий МО РФ уверенно доложило о готовности к появлению квантовых компьютеров и ответу на эту угрозу квантовой же криптографией.

ДИТ Москвы рассказал о практике внедрения и защиты элементов «Ин-

тернета вещей» в ИТ-инфраструктуре Smart City Москва.

В докладе Банка России была представлена детальная картина нынешней «оргструктуры» и нормативно-правового обеспечения ИБ в банковской сфере.

Управление Спецсвязи ФСО России проинформировало о развитии структуры ситуационных центров (СЦ) организаций России. Интересно было узнать, что движение по созданию СЦ спустилось уже на уровень вузовского управления. Но есть и трудности: эксплуатация развивающейся сети СЦ сталкивается, с одной стороны, с проблемой разнородности моделей данных в сотнях информационных баз страны и, с другой стороны, с нормативной необходимостью реализации «воздушных зазоров» безопасности между СЦ.

На секциях форума были представлены тематики «безопасного Интернета», комплексных решений по ИБ критической ИТ-инфраструктуры, безопасного использования ИТ на транспорте, модные темы «умного города» и «умного региона», неизбежно возникающие проблемы правового регулирования в сфере ИБ.

«КРУПНЫМИ БУКВАМИ ПЕЧАТАЛИСЬ СЛОВА СОВЕРШЕННО НЕСУЩЕСТВЕННЫЕ, А ВСЕ СУЩЕСТВЕННОЕ ИЗОБРАЖАЛОСЬ САМЫМ МЕЛКИМ ШРИФТОМ»

И на солнце есть пятна. Существенный минус организации форума проистекал, как и следовало ожидать, из главного достоинства мероприятия.

В решение задач и проблем ИБ были глубоко погружены не только спикеры форума. Многие гости обладали как экспертным уровнем знаний, так и актуальной информацией о ситуации в «поле». Казалось бы, сложилась идеальная ситуация для развития теории и практики ИБ в нашей стране,

однако недостаток времени в ряде случаев не только пресекал возможность публичных дискуссий и обсуждений, но и комкал запланированные доклады на секциях.

Тем не менее, работа демозоны «Зона позитивной безопасности» и секции «Информационная безопасность в кредитно-финансовой сфере» помогла выявить путем бурного обсуждения ряд свежих проблем.

«У НАС НЕТ СЕРЕДИНЫ: ЛИБО В РЫЛО, ЛИБО РУЧКУ ПОЖАЛУЙТЕ!»

Взгляд «из гугла» на ландшафт «интернета вещей» создаёт представление о нём, как об ухоженной лужайке, где тут и там произрастают полезные и нужные деревца, корни которых красиво укрыты дерном и недоступны для повреждения. Но оказывается, к этим корням есть и другой доступ, помимо того, что защищён в Google логином и паролем. Этот доступ подобен кровным норам, ведущим к камерам видеонаблюдения, уличным банкоматам и мобильному банкингу.

Переходя от садово-парковых аналогий, скажу, что специалисты компании Positive Technology, работавшие в демозоне «Зона позитивной безопасности», наглядно продемонстрировали, как средства, достаточно легко доступные в Интернете, позволяют заглянуть в разбросанные по миру веб-камеры, не заморачиваясь введением логина и пароля, и не совершая, по сути, противоправных действий, если забыть о нормах морали. А несложное тестирование с использованием социальной инженерии и содержания адресной книги в одной из критичных ИТ-инфраструктур, а затем имитация противоправных действий позволили продемонстрировать, как киберпреступник может «поселиться» на сервере аутсорсера, обслуживающего банковские терминалы. После чего многократно окупить свои небольшие затраты.

Ещё одним откровением стала демонстрация проникновения в рабочую сеть телекоммуникационной компании и перехват управления мобильным банковским приложением, призванным облегчить жизнь клиента банка, а на практике часто облегчающему его кошелек.



Выступление Виталия Лютикова, заместителя директора ФСТЭК России

«ВСЯКОМУ БЕЗОБРАЗИЮ СВОЁ ПРИЛИЧИЕ»

По оценке экспертов, банковская сфера выглядит наиболее защищённой от киберпреступлений по сравнению, например, с промышленной ИТ-инфраструктурой. Но оказывается, что внутри банковской «избы» достаёт «сора» в плане кибербезопасности.

Участники секции по информационной безопасности в кредитно-финансовой сфере обсудили много болевых точек. От набившей оскомину безответственности рядовых сотрудников, «кликающих» по любой почтовой ссылке, до оголённости штатов ИБ-подразделений и недобросовестности внешних соисполнителей, призванных выявлять прорехи в кибербезопасности банков второй и третьей линий. Была затронута и тема пресловутого искусственного интеллекта, причём разброс мнений по этой теме хорошо описывается выражением «кому щи пусты, а кому жемчуг мелок».

Бурную дискуссию обещал доклад ПАО Ростелеком о биометрической идентификации и дистанционной работе со счетами. Но, к сожалению, хайп был мягко пресечен ведущим секции со ссылкой на недостаток времени (уже упоминалось, что его дефицит стал ахиллесовой пятой форума).

Также большой потенциал для обсуждения имел доклад Positive Technology «Блокчейн на финансовых рынках: новые возможности и новые угрозы». На

мой взгляд, интерес в нем представлял не сам блокчейн, а указания на то, как появляются угрозы информационной безопасности в ИТ, казалось бы, безупречно отработанных академическим сообществом и вполне укладывающихся в достаточно широкое прокрустово ложе законодателей и регуляторов. Этот доклад с последующей дискуссией мог бы стать основой для развития методических основ отработки врожденного ИБ-иммунитета ИТ, но... времени для обсуждения не было, рамки форума поджимали.

Вместо полезной во всех отношениях дискуссии по практическим вопросам построения безусловно безопасных ИТ-систем, гости секции услышали просто приятное сообщение об опыте Сбербанка по управлению рисками кибербезопасности.

* * *

В целом Инфофорум 2018 представил весьма большой и сбалансированный набор докладов по важнейшим направлениям совершенствования ИБ. Слушатели форума продемонстрировали, сколь актуальна эта проблематика и сколь велик интерес к ней на местах. Остаётся надеяться, что через год мы услышим и о качественных прорывах в решении задач по укреплению информационной безопасности страны.

CYBER SECURITY FORUM 2018

БЕЗОПАСНЫЙ ИНТЕРНЕТ БУДУЩЕГО: РИТОРИКА БЕССИЛИЯ И ПОИСК НАДЕЖДЫ

«Безопасный Интернет Будущего» — именно так была задана тема Cyber Security Forum 2018 (SCF 2018), а сам Форум заявлен как российское мероприятие Международного Дня безопасного Интернета — праздника, изобретённого Еврокомиссией.

Русские-китайские-корейские хакеры, коварный бизнесмен Пригожин, вирусы Петя и ВаннаКрай, запрещённый контент для детей и взрослых, воровство денег со счетов в банках, рекламный спам и т.д. и т.п. — вот неполный перечень того, что сегодня называют «вызовами» для экономики и общества. На SCF 2018 Илья Сачков, основатель компании Group-IB, заявил: «Разрушение инфраструктуры является одним из основных трендов новых вирусов».

Сбои и фатальные крахи в работе АСУТП — это намного круче «Фауста» Гёте, особенно в нашей стране. Причина в том, что ИТ-инфраструктура нашей нищей промышленности опирается на оборудование и технологии, лишь косметически адаптированные под «условия эксплуатации», и недопустимо часто обслуживается сторонними организациями на аутсорсе. Их ценным специалистам «лениво» и экономиче-

ски неэффективно оторвать корму от офисного причала. В результате к локальным сетям АСУТП протягиваются «щупальца» Интернета. По этим каналам одинаково успешно доставляются как услуги аутсорсинга, так и вредоносное ПО.

ЗАВТРА БУДЕТ ХУЖЕ, ЧЕМ ВЧЕРА

Обсуждая Cyber Security Forum 2018, нельзя не отметить, что его тема «Безопасный Интернет Будущего» звучит символично и задаёт правильный настрой: как бы констатируется, что на нынешний момент «Безопасность» и «Интернет» — понятия, совместимые с большим трудом. Но возможно ли счастье в будущем?

Из системного анализа докладов спикеров следует, что ситуация может только ухудшиться. Уж слишком много противоречий между субъектами, населяющими Сеть.

Апологеты «Свободного Интернета» недовольны всевозможными притеснениями законодателей. Ибо, по их мнению, Интернет по своей сути — это свобода, воплощённая в ИТ. Уже как-то забылось, что корни Интернета — в глубоко внутреннем междусобойчике учё-

ных, возжелавших получить канал для келейных коммуникаций, и в поддержке этой инициативы военными, которым нужны были резервные линии связи на случай войны. Это уже потом по американской традиции всё ушло в частные руки...

Законодатели и известные защитники детства трогательно опасаются, что просторы Сети заполонит противоправный контент, унижающий человеческое достоинство, сеющий зёрна аморальности и агрессии. И встают грудью на защиту детей и бизнеса сетевых кинотеатров. Которые, заметим, с помощью Сети широким бреднем снимают «третий отжим» с подделок голливуда и болливуда, подрывая семейные устои и внедряя в сознание молодёжи представления о том, что лежащего человека можно раз пять ударить ногами, а он после этого встанет и продолжит драку с новыми силами.

Выступившие на CSF 2018 руководители компаний, входящих в «НОТ-list компаний-лидеров, представляющих услуги/товары кибербезопасности», не привели иных данных, кроме тех, что свидетельствуют о росте числа киберпреступников, изощрённости их атак и совершенстве технической оснащённости.

Как утверждает уже упомянутый Илья Сачков: «Цифровое оружие отличается от обычного тем, что чаще всего находится в открытом доступе, и каждый может его использовать. Проблема киберпреступлений в первую очередь в людях — киберпреступниках. Чаще всего их мотивация — деньги». Открыл Америку.

А вслед информации об алчности киберпреступников, уже в иных докладах сообщалось о том, что в компаниях существует и численно множится пятая колонна из сотрудников, крадущих данные из CRM-систем или безответственно кликающих на сомнительные ссылки в общедоступном Интернете, где они проводят больше половины рабо-



Илья Сачков, основатель компании Group-IB. Фото: runet-id.com/event/csf18



Открытие форума. Фото: runet-id.com/event/csf18

чего времени. И бороться с этим следует тотальной киберслежкой.

К слову сказать, в Германии такая слежка не приветствуется на официальном уровне, что, в частности, закрыло путь на рынок этой страны одной очень достойной отечественной компании.

КТО ВИНОВАТ?

На CSF 2018 многократно в разных вариациях утверждалось, что слабое звено в Сети — это пользователь. Но, похоже, это слабое звено не единственное. Общественный деятель и эксперт интернет-отрасли Сергей Плуготаренко заявил, что «цифровые технологии развиваются настолько стремительно, что разработчики не успевают внедрить эффективные меры по повышению уровня кибербезопасности».

Так кто же виноват? Пользователь? Или разработчики, которые не только «не успевают внедрить эффективные меры», но и зачастую не затрудняют себя созданием нормальной документации — по сути единственного объективного «набора знаний о современных ИТ-технологиях и возможностях их применения». О какой объективности при оценке рисков может идти речь?

И прав ли Сергей Плуготаренко, утверждая, что «в этой реальности можно жить и развиваться»? И только ли пользователи должны оценивать риски? А те, кто эти риски плодит, спеша монетизировать результаты ИТ-макетирования?

ДЕТИ — ТОЖЕ НАШЕ БУДУЩЕЕ

Интернет небезопасен для инфраструктуры предприятий и организаций и часто очень опасен для детей. Но, не отрицая последнего, нельзя согласиться со спорными тезисами уполномоченного при Президенте РФ по правам ребёнка Анны Кузнецовой:

«Детский контент играет важную роль в общем интернет-пространстве. Мы видим, как онлайн активность влияет на детскую активность вживую. Нам важно объединиться и посмотреть, какой интернет будет через 10 лет. Для этого необходимо сейчас понимать запрос детей к информационному пространству. Я абсолютно убеждена, что в основе запроса лежит культура выбора ребенка, которая напрямую зависит от воспитания. Нам необходимо формировать этот запрос. Многие зависят от того примера, который мы даем своим детям. Взрослым важно создавать навигаторы, которые помогут детям двигаться в информационном пространстве».

Что ни фраза, то недоумённый взгляд на говорящего.

«Мы видим, как онлайн активность влияет на детскую активность вживую».

Да, видим. Растёт число физически ослабленных детей, и виной этому не только качество питания, но и малоподвижная «жизнь в Интернете», отсутствие дворового пространства для детских активных игр, захваченного машинами и уплотненной застройкой.

«...необходимо понимать запрос детей к информационному пространству. Необходимо формировать этот запрос. ...Взрослым важно создавать навигаторы, которые помогут детям двигаться в информационном пространстве».

Не надо формировать запрос и создавать навигаторы. Надо создавать и формировать домашние библиотеки. Для этого у родителей должны быть средства и время: нормальная зарплата и работа не в другом городе. Но вместо этого на CSF 2018 презентуется новый проект Facebook, «созданный для обучения родителей основным навыкам работы с социальной сетью». Не лучше ли помочь родителям подобрать и проиллюстрировать аргументы, позволяющие объяснить детям преимущества здорового и безопасного образа жизни, живого (а не в чате) общения с друзьями, чтения книг, занятия физкультурой и спортом?

ЧТО ДЕЛАТЬ?

Возможно ли создание безопасного Интернета в будущем без пересмотра взглядов на технологии и методологию Сети? Вряд ли. Можно ли обеспечить безопасность на шоссе, на разных участках которого действуют разные правила? Можно ли обезопасить движение на изношенной магистрали, принцип эксплуатации которой не позволяет ни на мгновение остановить движение? Будет ли безопасным движение на дороге, по которой в едином потоке движутся велосипедисты, грузовики и стритрейсеры? Вопросы риторические.

В системах управления в числе важнейших принципов обеспечения надёжности и безопасности являются децентрализация и резервирование. Возможно, стоит подумать о создании в Сети региональных сегментов и специализированных магистралей для промышленности, финансово-кредитных организаций, военных и других пользователей-профессионалов. Не унификация технологий и законов, а их специализация — не это ли путь к безопасному Интернету будущего?



Фото: tbforum.ru

ТБ ФОРУМ 2018

ВСЕРОССИЙСКИЙ СМОТР ИМПОРТОЗАМЕЩЕНИЯ
В СФЕРЕ ИБ ПОРАДОВАЛ

Форум «Технологии безопасности» проводился компанией «Гротек» в 23-й раз. В этом году он принял формат Всероссийского смотра (решений и технологий для обеспечения безопасности граждан и объектов промышленной и городской инфраструктуры) и полностью этот формат оправдал.

ПРОТИВ ЛОМА. КОНЦЕПТУАЛЬНО

Футуристическая обыденность современных ИТ как-то затуманивает реальность тех покушений на безопасность, с которой ассоциируются слова «взлом», «ограбление» и «несанкционированное

проникновение». ТБ-2018 концептуально напомнил о возможности таких грубых, но по-своему технологичных, угроз, демонстрируя на самом видном месте выставки продукцию завода периметральных ограждений «ЕГОЗА». Фрагмент brutального забора, один вид которого способен остановить самого ражего американского «котика», уладил взор не одного зам. генерального по безопасности.

Но более подробное ознакомление с выставкой показало, что отечественные технологии безопасности — это не только забор завода «ЕГОЗА» и нелетальные средства самообороны компании «ОБЕРОН-АЛЬФА».

ХОРОШИЙ ПРИМЕР

Тут предлагается и то, что на языке консорциума «Интегра-С» называется интеллектом интегрированных систем безопасности. Мощнейшее приспособление, способное расплатать защитный «купол» из систем видеонаблюдения, контроля и управления доступом, пожарной сигнализации и т.д. Причем «купол» можно раскрыть как в интересах безопасности маленького отдельного офиса банка, так и огромной штаб-квартиры того же банка, а при необходимости и в интересах города и даже региона. А на транспортных магистралях ни один автомобильный номер, ни один элемент

маркировки ж/д вагона не укроется от учёта и контроля со стороны интеллекта систем видеонаблюдения консорциума.

Интересно, что в течение трёх дней выставки у стенда «Интегра-С» толпились заказчики из стран, для которых слово «Африка» — не виртуальные воспоминания о корнях, а естественная среда обитания, которую хочется защитить от порока и безобразий. Похоже, по коррупции и бардаку на транспортных магистралях африканских стран очень скоро будет нанесён чувствительный удар с помощью российских технологий. И хотя технологии эти нельзя назвать уникальными с точки зрения академических основ, отрадно видеть, что сегодня они «в тренде» и «на острие».

Также приятно осознавать, что для успешного бизнеса консорциума санкции североамериканских штатов и расколотого европейского сообщества совсем не помеха. Импортозамещение для «Интегра-С» не компанейщина, а давно сформировавшийся стиль жизни. Отечественные процессоры и производство электронных плат в подмосковном Зеленограде, операционные системы на основе Linux и российские интеграционные программно-аппаратные решения — всё это продукты российской мысли и сборки. А Oracle с её верноподданническими ограничениями в системах отечественной общественной и транспортной безопасности может идти туда, куда предприниматель Полонский отправлял гостей-миллионеров на своей на шумевшей вечеринке в Каннах.

ПОКУПАЙТЕ РОССИЙСКОЕ!

После панегирика уместно сказать, что инженерный high-tech и стиль бизнеса «Интегра-С» в среде участников ТБ-форума — явление довольно обычное. ТБ-2018 оказался действительно *все-российским* *смотром* новейших решений и технологий. А каталог выставки или список её участников на сайте мероприятия может служить отличным путеводителем для всех руководителей компаний и организаций, а также иных лиц, принимающих решения в сферах, ассоциирующихся со словом «безопасность».



Экспозиция ТБ Форум 2018. Фото: tbforum.ru

Для разогрева ассоциаций можно назвать области физической защиты и управления доступом, интеллектуальное видеонаблюдение и биометрию, защиту информации и каналов связи, средства для обнаружения подслушивающих устройств... Дальше фантазию можно не останавливать, всё, что душе «безопасника» широкого профиля, было представлено на выставке ТБ-2018. И это «всё» — на основе разработок отечественных инженеров и экспертов.

На платах, показательно отдельно выставленных рядом с коммутаторами, чётко выделяются действительно уникальные процессоры «Байкал-Т 1». В аккуратных углублениях транспортировочной тары лежат не менее уникальные средства нелинейной локализации компании «ЛОРНЕТ Экспорт», не оставляющие шансов электронным «закладкам» в помещениях для конфиденциальных переговоров. Также не оставляют шансов нашим «партнёрам» — в случае попытки грубого попользования на мирное небо российских граждан — и разработки РФЯЦ-ВНИИЭФ (полагаю, страну происхождения называть не надо).

Справедливости ради стоит отметить, что российский акцент ТБ-форума не помешал участию в нем компании Huawei и других зарубежных компаний, преимущественно из Японии и Германии.

СЛОВО И ДЕЛО

Полный формат ТБ Форума — конгрессно-выставочный. За три дня был проведён десяток конференций, а также выездное заседание Комитета Совета Федерации по обороне и безопасности. Руководители и сотрудники компаний встречались с представителями органов власти и регуляторами в конференц-залах, на выставочных стендах и в неформальной обстановке по всей территории Конгресс Холла.

Основные вопросы конференций — обеспечение безопасности на транспорте, на спортивных и массовых мероприятиях, безопасность городской среды, строительных объектов, предприятий нефтегазовой отрасли и энергетики, банковской сферы, вызовы безопасности в связи с реализацией программы «Цифровая экономика РФ», новое в нормативном регулировании безопасности КИИ.

Когда представители ФСТЭК детально рассказывали о путях реализации Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», в зале был полный аншлаг. Компетентные эксперты отвечали на десятки злободневных вопросов из зала. Эта встреча была тем более актуальна, что, в отличие от зарубежной практики, предоставляю-



Экспозиция ТБ Форум 2018. Фото: tbforum.ru

щей, как правило, двухгодичный переходный период для вхождения в новые условия регулирования КИИ, в России внедрение законодательных новаций будет реализовываться немедленно.

В то же время в другом зале слушатели знакомились с мнениями представителей власти о путях нахождения баланса между требованиями развития цифровой экономики и теми вызовами безопасности, что создаёт новая парадигма.

Обсуждение безопасности в городах при проведении массовых мероприятий и международного сотрудничества в этой сфере оказалось особенно актуальным в преддверии чемпионата мира по футболу. О практических шагах для создания атмосферы безопасности на стадионах и в городской среде рассказывали представители Москвы, Сочи, Екатеринбурга. Технические эксперты поделились опытом внедрения систем видеонаблюдения, биометрической идентификации, системы авто-

матизации выдачи гостевых билетов и пропусков.

Гвоздём третьего дня форума стала конференция по инновационному и во многом пока спорному подходу к проектированию в строительстве на основе методологии BIM (информационное моделирование) и сопровождению жизненного цикла возведенной промышленной инфраструктуры на основе BIM. Тут узловым стал доклад представителя Росатома о практических шагах по созданию информационных моделей АЭС, использование которых обеспечивает не только экономическую эффективность возведения и эксплуатации атомных энергоблоков, но и безопасность на этапах эксплуатации и вывода из эксплуатации.

Примечательно, что на одной из конференций ТБ-форума получил продолжение разговор о внедрении биометрической идентификации в банковской сфере, начатый две недели назад на Инфофоруме 2018. Но и на этот раз он не

был завершен. Похоже, эта тема, словно эстафетная палочка, обречена переходить от форума к форуму.

Выставка и десяток конференций в Крокус Конгресс Холле полностью оправдали заявленный формат Всероссийского смотра. Основные выводы о состоянии рынка технологий безопасности в России, которые можно сделать по итогам форума — это констатация следующих фактов: подавляющее доминирование отечественных компаний; владение ими полным спектром технологий безопасности на основе современной электроники, работающей в режимах локальной защиты, а при необходимости — в режиме IoT; своевременное выделение ресурсов на проработку перспективных технологий и аппаратуры...

В общем, неплохо.

INTERNATIONAL OPEN DATA DAY

КОГДА ИБ ВЫВОРАЧИВАЮТ НАИЗНАНКУ

В феврале российские миллениалы отметились в поддержке Международного Дня безопасного Интернета, а уже в марте вновь подставили плечо под брёвнышко пиара общественного блага международного масштаба. 3–4 марта состоялся International Open Data Day.

Подстрочник названия этой инициативы ясен, а вот содержание — не очень. Согласно энциклопедии, обслуживающей понятийный аппарат global digital infrastructure, открытые данные — это концепция, отражающая идею о том, что (цитирую) «определённые данные должны быть свободно доступны для машиночитаемого использования и дальнейшей републикации без ограничений авторского права, патентов и других механизмов контроля».

Как некогда идеи мирового анархизма и мирового же интернационала, Open Data сегодня призваны послужить общественному благу. Благу,

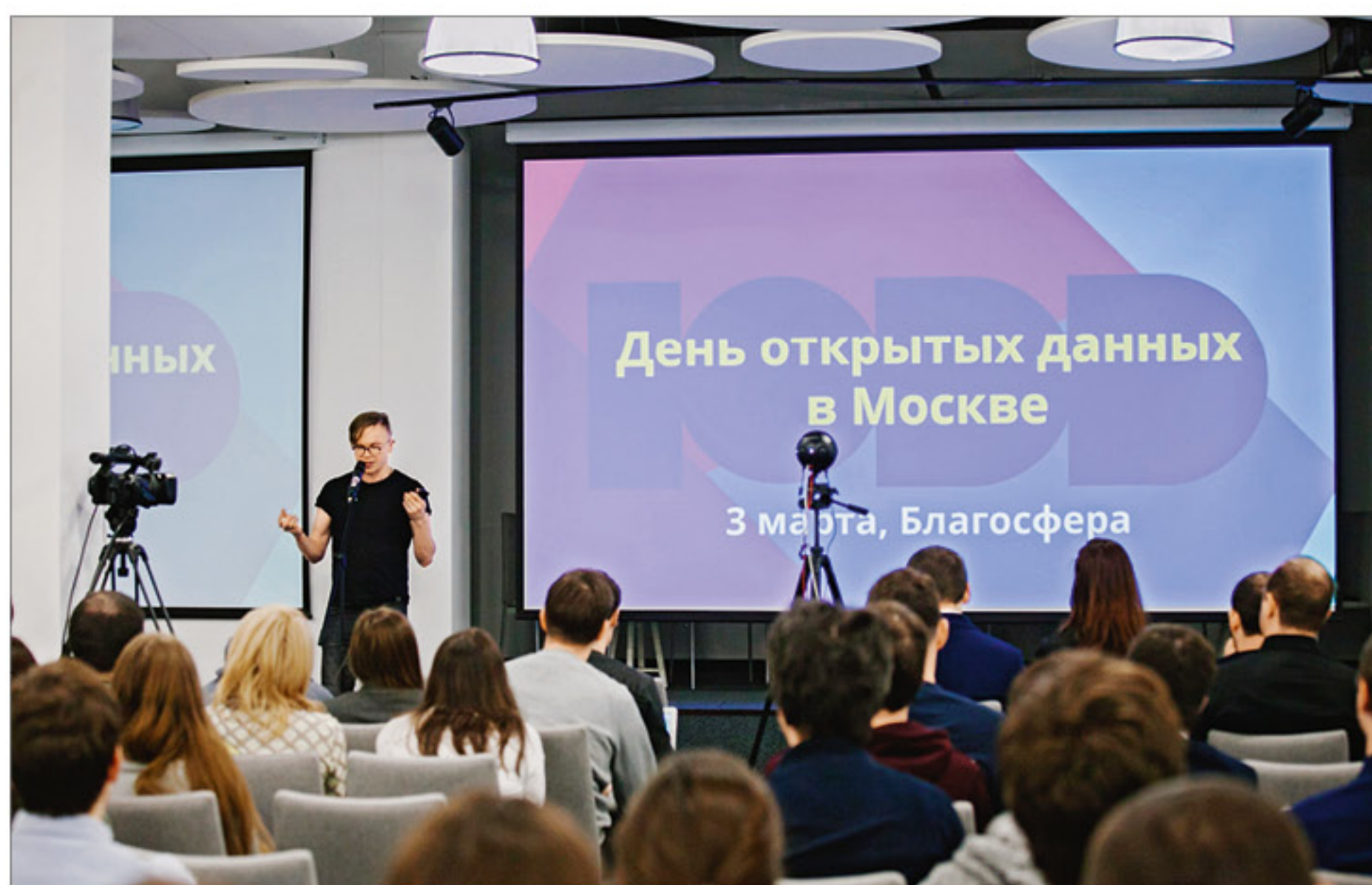
во-первых, в лице гражданского общества, которое с их помощью взнуздает жуликоватые правительства и вернёт госуправление в верную колею, и, во-вторых, благу в лице бизнеса, этого локомотива общественного прогресса, для которого открытые данные станут новым сырьем для получения added value. В частности, на сайте российского Федерального казначейства имеется прямое упоминание о возможности использования таких данных «для создания программ для ЭВМ и приложений».

НАСЫЩЕННОЕ МЕРОПРИЯТИЕ

Пленарное заседание продемонстрировало, что наши лидеры Open Data — люди образованные, эрудированные, обладающие острым гибким умом и отменной реакцией. Формальный, казалось бы, элемент открытия мероприятия — приветствие Министра РФ Михаила Абызова — был мгновенно обыгран и добротнo встроен в пленарную дискуссию.

Такой подход позволил узнать много интересного: о причинах заинтересованности чиновников в реализации идей Open Data (одна из них, например, — чиновничий КРП), о мнении бизнеса («Интерфакс двумя руками «за»», мнение культуры (Иван Засурский чрезвычайно высоко оценил помощь Дмитрия Медведева в части реализации проекта по созданию электронного хранилища произведений литературы и искусства, срок защиты интеллектуальных прав на которые истёк).

Вместе с тем, спикеры скептически «отнеслись» к чиновной готовности содействовать Open Data (препятствиями на этом пути были названы неясности с финансированием и беспорядок в закромах, где хранятся уже накопленные данные) и покритиковали законодательство «О забвении» (Иван Засурский вполне обоснованно обратил внимание на то, что Интернет ничего не забывает по своей технологической природе, а любые вновь появившиеся данные



сразу становятся общественным достоянием, и всякая попытка их уничтожить — это покушение на общественное богатство).

За два дня российские активисты Open Data представили и немало достижений: от методик создания машиночитаемых данных и практики инфографики, полезной для восприятия массивов Open Data, до ярких примеров широкого доступа к данным о жизни и географии городов, сведениям по истории и культуре. Ценные советы — как работать с открытыми данными — были даны журналистам, при этом широко использовался термин «дата-журналистика». ВШЭ даже анонсировала новый курс, в рамках которого журналистам новой формации будут прививать навыки программирования и работы с Big Data.

КТО? КОГДА? И ЗА КАКОЕ ВОЗНАГРАЖДЕНИЕ?

В связи с претензиями к качеству как самих данных, так и их выкладки («машиночитаемость») встаёт вопрос об ответственности (пока не в смысле наказания) за создание массивов открытых данных. Ведь если под открытостью не понимать (что вполне разумно) прямую механическую трансляцию всего, что фиксируют камеры видеонаблюдения ГИБДД, магазинов, учреждений и т.д., то *кто, когда и за какое вознаграждение* должен принимать решения и выполнять конкретную, весьма объёмную работу по созданию так называемых «дейтасетов»? При том, что их модели, например, для минкульта заметно отличаются от моделей для поселковой администрации, Сбербанка и т.д.

Рассмотрим эти проблемы на примере Министерства финансов России.

Руководство Минфина чётко осознаёт и указывает на своём сайте (www.minfin.ru/ru/opendata), что поиск перспективных идей по представлению информации в форме открытых данных и реализация этих идей могут оказываться сильно ресурсозатратными. Поэтому «поиск форматов, каналов и аудиторий потребителей, развитие идей, создание конкретных продуктов» в области открытых данных предлагает оставить за бизнесом и энтузиастами.

Но и государству Минфин отводит не простую задачу: подготавливать и раскрывать данные для использования, «подсказывать основные — корректные — возможности их применения». Это тоже затраты! Возможно Минфин полагает, что в нынешних условиях на пути к «цифровой экономике» удастся одним выстрелом убить двух зайцев — и в эту самую экономику перейти и данные подготовить и раскрыть?

В системе Министерства финансов России последовательно и системно решены вопросы управления процессами создания открытых данных. Для этого выпущены приказы:

- ♦ от 24.03.2014 № 76 «О назначении ответственного за обеспечение работы с открытыми данными в Минфине России»;

- ♦ от 31 декабря 2014 г. № 625 «Об утверждении регламента формирования, актуализации и принятия решения о прекращении актуализации наборов открытых данных Министерства финансов Российской Федерации».

С 2016 года Минфин ежегодно проводит конкурс «BudgetApps» (латиница — это, вероятно, дань «зарубежности» корней явления), для участия в котором приглашаются разработчики «интернет и мобильных приложений», журналисты, дизайнеры и историки.

Цели Конкурса заявлены вполне себе достойные, и на общее благо работающее, и Минфину помогающие:

- ♦ Популяризация использования сведений о государственных и муниципальных финансах, предоставленных в форме открытых данных среди разработчиков и журналистов, исследователей и других потенциальных потребителей открытых данных Минфина России.

- ♦ Повышение уровня информационной культуры среди разработчиков, журналистов и потребителей их продуктов.

- ♦ Формирование сообщества информационно образованных граждан, которые будут помогать продвижению идей и принципов открытых данных.

- ♦ Повышение прозрачности и доступности финансовой информации.

- ♦ Развитие проектов, нацеленных на создание общественных благ.

- ♦ Продвижение открытых данных Минфина России, включая исторические бюджетные данные.

- ♦ Повышение финансовой грамотности населения.

За все время существования конкурса в нём приняли участие почти 600 участников из 23 регионов Российской Федерации. Т.е. имеется практика ответа на вопросы *кто? когда? и за какое вознаграждение?* должен принимать решения и выполнять работу в области открытых данных. Минфин ещё даёт ответ и на вопрос *как?*

ПРО НАКАЗАНИЕ И ИБ

Следующий возникающий вопрос — вновь об ответственности за публикацию открытых данных, но уже в разрезе наказания за нарушение требований информационной безопасности.

На International Open Data Day прямое обсуждение вопросов информационной безопасности свелось к выступлению представителя компании Group-ID по общим проблемам защиты персональных данных персонами, эти данные не слишком тщательно хранящими. И косвенно в ряде выступлений затрагивались вопросы, связанные с такими метриками ИБ открытых данных, как целостность и доступность (пусть и в иной терминологии) в связи с промахами в машиночитаемости того, что подаётся под соусом Open Data.

Однако в сфере открытых данных вопросы защиты персональных данных и информационной безопасности интересов государства имеют свою специфику.

Не секрет, что в кредитно-финансовой сфере востребована информация, позволяющая проверить благонадежность физических и юридических лиц, которые претендуют на получение кредитов или могут стать деловыми партнёрами. Однако раскрытие подобных сведений может приводить к публикации персональных данных и сведений, составляющих банковскую (налоговую) тайну.

И даже когда Сбербанк готов предоставить всему миру в рамках инициативы Open Data обезличенную информацию, такую как:

- ♦ выручка юридических лиц в разрезе отраслей и регионов;



Фото в статье: vk.com/ioddmnsk

- ◆ уровень доходов населения — зарплаты, пенсии, стипендии, пособия;
- ◆ склонность к сбережениям и потреблению;
- ◆ уровень закрепитованности в разных регионах;
- ◆ мобильность населения внутри страны и за рубежом;
- ◆ доля расходов на еду, ЖКХ, транспорт и другие статьи;

возникает вопрос: а только ли для дата-журналистов и отечественной финансово-кредитной сферы ценна эта информация? Не упрощает ли свободный доступ к этой информации работу разного рода нуландам и соросам?

Открытость г-на Бакатина и претендентов на соросовские гранты в начале 90-х, предоставивших нашим партнёрам за малую толику денег пласты информации чернозёмных масштабов, получит, похоже, лишь моральную оценку.

Но заинтересованность в открытости данных, генерируемых в отечественных госучреждениях, не иссякает. Символично, что уже 4 марта г-н Станкевич предложил открыто поделиться с мировым сообществом тайнами российской ядерной энергетической установки «мегаваттного класса».

Интересы г-на Станкевича понятны в контексте истории его жизни и дружеских связей. Озабоченность вызывает легкомыслие некоторых лидеров отечественного движения Open Data, усмехающихся при упоминании о возможной не-

чистоплотности забугорных апологетов раскрытия информации. Которые требуют ни много ни мало, чтобы «данные должны быть доступны без последующих запросов на разрешение, хотя и способы повторного использования, такие как создание продуктов на базе данных, могут контролироваться лицензией». Факты об ушедшей на сторону в «открытые» 90-е документации по Як-141 и о манипуляциях с историческими архивами — это вполне себе открытые данные, но послужили ли они общественному благу, хотя бы в качестве уроков?

О том, что однозначного ответа на эти вопросы нет, указывает, например, ремарка на сайте Федерального казначейства в разделе об открытых данных: «пользователь обязан использовать открытые данные только в законных целях; не искажать открытые данные при их использовании; сохранять ссылку на источник информации при использовании открытых данных». Но и после упоминания об обязательности корректного использования Open Data «Федеральное казначейство не несет ответственности за использование открытых данных».

ДЛЯ ВНУТРЕННЕГО УПОТРЕБЛЕНИЯ

Формально вопросы ИБ и безопасности страны, в том числе и в ходе работ по открытым данным, рамочно регулируются законами «Об обеспечении доступа к информации о деятельности государственных органов и органов

местного самоуправления» и «Об информации, информационных технологиях и о защите информации».

Но сделают ли открытые данные лучше общество, в котором для обоснования вторжения в суверенное государство можно из ничего создать пробирку с белым веществом, а потом обеспечить забвение этого факта и безнаказанность создателей фейка? Сегодня на «международной арене» мы слишком часто видим, что открытость данных используется не для блага, а для разной степени хитроумности манипуляций.

В связи с этим есть необходимость совершенствования национальной законодательной и нормативной базы в области использования открытых данных для граждан и отечественного бизнеса. И возможно пока на основе запросов на разрешение. Особенно, если «способы повторного использования, такие как создание продуктов на базе данных, могут контролироваться лицензией».

* * *

А последовательное решение задач доверенного «цифрового документооборота» и цифровой трансформации институтов госуправления, финансово-кредитных организаций, сферы ЖКХ позволит естественным образом, без кампанейщины решить вопросы машиночитаемости и целостности открытых данных для внутреннего употребления.



КАДРЫ РЕШАЮТ ВСЕ

ЗАБОТА ОТРАСЛИ ИБ: ШКОЛЬНИКИ, СТУДЕНТЫ, МОЛОДЫЕ СПЕЦИАЛИСТЫ И Т. Д.

В рамках X Уральского форума состоялась сессия «Квалификационные требования к специалистам по информационной безопасности организаций кредитно-финансовой сферы РФ». В ней приняли участие представители регуляторов, университетов, учебных центров и банков, которые обсудили волнующий всех вопрос подготовки кадров и их соответствие современным требованиям в сфере ИБ. Роль модератора исполнил заместитель председателя Банка России Руслан Вестеровский.

Руслан Вестеровский: Мир становится все более волатильным, скорость изменений и внедрения инноваций

повышается с каждым годом. Футурологи утверждают, что через пять лет банков в классическом понимании практически не останется. Они уйдут в цифру, в онлайн-решения — и этот тренд уже сегодня набирает реальную силу. В этих условиях важно оценить угрозы, в том числе увеличение кибератак на индустрию в целом. По мнению экспертов, потери мировой экономики от киберпреступности составляют порядка \$1 трлн в год. И чтобы уберечь средства на счетах, компании совершенно справедливо повышают требования к специалистам по ИБ.

А достаточно ли у нас таких специалистов? Как оценивают работодатели

количество и качество выпускников вузов? Трудно ли найти хорошего специалиста? Если верить сайтам по трудоустройству, то вакансий на них много, но соискателей еще больше, при этом кадровый голод велик. Претенденты, как это ни парадоксально, не удовлетворяют потребности рынка, а часто они даже не востребованы рынком. Почему? Замечу, что Банк России активно занимается рекрутментом в сфере ИБ, и под наши запросы и требования трудно найти специалистов нужной квалификации.

Вопрос работодателю: приходят ли к вам на работу те, кто вам нужен, или приходится доучивать их под требования и стандарты банка?



Сергей Пазизин, начальник Управления по обеспечению ИБ Банка ВТБ



Руслан Вестеровский, заместитель председателя Банка России

МНЕНИЕ РАБОТОДАТЕЛЯ

Сергей Пазизин, начальник Управления по обеспечению ИБ, Банк ВТБ: Безусловно, мы сталкиваемся с дефицитом специалистов в области информационной безопасности. Он связан с увеличивающимся ростом спроса на кадры, и удовлетворить эту потребность в ближайшее время будет просто даже при значительном увеличении приема студентов на специальности, связанные с обеспечением ИБ.

Что касается качества подготовки, то у нас нет завышенных ожиданий. Мы не рассчитываем, что к нам придет полностью готовый к работе молодой специалист. Конечно, ему потребуется время адаптироваться к специфике отрасли. Необходимо изучить — нормативное регулирование, банковские и платёжные процессы. Человек, который будет заниматься безопасностью бизнес-процессов, использующих информационные технологии, внедрением безопасных банковских приложений, должен знать специфику банка. Как правило, этому в вузах, выпускающих специалистов по общим направлениям ИБ, не учат. Другой аспект — работа удостоверяющего центра, сетевая безопасность, разработка приложений — все эти направления требуют узкоспециальных знаний и, соответственно, дополнительной подготовки. Есть также специфика, связанная с работой в крупной организации со своей внутренней нормативной базой и требованиями, наработками, бэкграундом, корпоративной культурой. Человек, который приходит к нам, должен все это освоить, понять принципы работы

и влиться в команду. Поэтому, конечно, мы в первую очередь ищем перспективных талантливых людей, которые смогут у нас раскрыться и остаться надолго.

Руслан Вестеровский: Вы набираете выпускников или людей с опытом?

Сергей Пазизин: В подразделении безопасности мы отдаем предпочтение специалистам с опытом работы. Когда у человека есть опыт, то уже на собеседовании становится понятно, что он умеет, к чему стремится и как работает. Конечно, выпускникам мы тоже даем шанс. В ВТБ имеются все возможности для развития и обучения молодых специалистов. Также мы берём сотрудников без профильного образования, но с опытом работы в сферах, близких к ИБ, например, если они занимались разработкой и эксплуатацией автоматизированных систем или поддержкой сетевой инфраструктуры.

Учитывая мой опыт преподавания, я бы хотел отметить следующее. Необходимо, с одной стороны, достаточно глубоко изучать базовые дисциплины, получать фундаментальные знания по математике и информационным технологиям, а с другой обеспечивать гибкость при наполнении дисциплин на старших курсах.

Поскольку детально прописать требования к будущим выпускникам заранее невозможно, университетам важно иметь возможность формирования программ в части дисциплин по выбору и факультативов, чтобы на последних годах обучения они могли дать студентам набор знаний, который будет учитывать реальные кибе-

ругрозы, нововведения в нормативной базе и сможет обеспечить специализацию по актуальным направлениям. Тогда работодателям будет проще адаптировать выпускников на новом рабочем месте, и они будут быстрее вливаться в новые интересные проекты.

О ПРОФСТАНДАРТАХ

Руслан Вестеровский: По оценкам аналитиков, в 2022 г. в мире будут востребованы 1,8 млн специалистов по ИБ. По данным Минобрнауки, в России потребность в новых специалистах по ИБ до 2020 г. составит 21 тыс. человек в год притом, что отечественные вузы выпускают 5000 человек в год. Т.е. у нас выпускников в четыре раза меньше, чем требуется экономике в целом. Вузам необходимо ориентироваться на потребности рынка труда и увеличивать квоты и число мест на ИБ-направлениях.

В российских университетах специальность ИБ появилась 15 лет назад. В связи с развитием цифровых технологий, ее значимость и популярность среди абитуриентов растет, поскольку одновременно есть спрос у работодателей. И тут я бы хотел обратить внимание на кооперацию российских компаний и университетов, которые в партнерстве открывают базовые кафедры и получают на выходе из вуза уже готовых к работе выпускников. Это прямой заказ на подготовку выпускников, который позволяет удовлетворить спрос крупных игроков на хороших специалистов. Но таких случаев пока сравнительно немного.

Евгений Белов, заместитель председателя Совета ФУМО ВПО ИБ: Сегодня у нас есть линейка профессиональных стандартов. Семь профстандартов, которые задают основные требования к выпускникам высшей школы (ВПО), заведений среднего специального образования (СПО) и к дополнительному профессиональному образованию (ДПО). Стандарты прошли экспертизу у работодателей, утверждены и введены в действие. Это основа для работы системы образования, основная смычка между образованием и практикой, а также основа для оценки специалистов в области ИБ в ходе их профессионального роста.

Что есть в системе образования? В системе образования в области ИБ существует 10-я группа, которая включает три специальности СПО, бакалавриат и магистратуру высшего образования, семь специальностей высшего образования, аспирантуру и агентуру. Система достаточна по всем образовательным направлениям и закрывает потребности федеральных органов исполнительной власти и всего рынка в целом.

Последние три года образовательные программы по ИБ реализуют около 170 учебных заведений ВПО, порядка 89 СПО (многие из них имеют право, но им не пользуются) и 40 учебных центров. Вот официальные контрольные цифры приема Минобрнауки: в нача-

ле 2000 годов мы готовили 2000 специалистов в области ИБ, в 2019 г. — более 7000.

Образовательные стандарты закрывают всю индустрию ИБ, учитывая как государственные, так и коммерческие интересы, в т.ч. ОПК и кредитно-финансовую сферу. Именно по запросам банковского сообщества ФУМО разработало новые образовательные программы. Так по обновленному бакалавриату, где существует 6 профилей, выделен профиль «информационно-аналитические системы финансового мониторинга», который напрямую связан с кредитно-финансовой сферой, но в большей степени ориентирован на финансовый мониторинг. Есть и другие профили, более широкие. Учебные заведения вместе с заказчиком могут взять профиль, например, «Безопасность автоматизированных систем» и добавить слова «в кредитно-финансовой сфере», что допускается нормативами. В самом профиле бакалавриата, согласно новым актуализированным стандартам, существуют обязательные профессиональные компетенции, которые прописаны в программе и учитывают специфику направления.

Одновременно с актуализацией образовательного стандарта идет развитие базовых кафедр. Такую работу ведет Банк России в ряде ведущих университетов, возможно, будет создавать там свои кафедры и Сбербанк. Финансовый

университет, который имеет тесные связи с кредитно-финансовой сферой, разработал свои компетенции.

По направлению «Компьютерная безопасность» есть специализация по информационно-аналитической, технической экспертизе компьютерных систем. Она опосредованно применяется для подготовки специалистов для кредитно-финансовой сферы. Как и стандарт по специалитету ИБ АС. Вместе с Центробанком и с представителями Сбербанка России мы ввели новую специализацию в этом стандарте: «Безопасность автоматизированных систем в финансово-кредитной сфере». И мы благодарны экспертам Банка России, в первую очередь, Артему Сычеву и его сотрудникам, которые приняли активное участие в подготовке направления.

И в заключение хочу отметить специальность «Информационно-аналитические системы безопасности» с четырьмя специализациями, в т.ч. «Информационная безопасность финансово-экономических структур». Есть специальность «Безопасность информационных технологий в правоохранительной сфере», где направление компьютерной экспертизы и компьютерных инцидентов заинтересует кредитно-финансовую сферу.

Мы считаем, что любые вопросы и проблемы можно решить при сотрудничестве всех заинтересованных сторон. Спасибо.

ПОЗИЦИЯ ФСТЭК

Руслан Вестеровский: В 2016 г. президентом России утверждена «Доктрина информационной безопасности РФ», в 2017 г. — программа «Цифровая экономика РФ». Документы предусматривают создание правовых условий для развития отрасли ИБ. Банк России как мегарегулятор считает необходимым правовое оформление деятельности, обеспечивающей ИБ в кредитно-финансовой сфере. Это принципиально важно, потому что специфика деятельности сегмента, в котором строится ИБ, всегда должна учитываться.

В Центральном банке сейчас разработали проект программы повышения квалификации в области ИБ. Аналогичная типовая программа повышения квалификации разрабаты-



Евгений Белов, заместитель председателя Совета ФУМО ВПО ИБ



Анатолий Марченко, начальник отдела управления ФСТЭК России



Сергей Ерохин, ректор МТУСИ

вается для руководителей в сфере ИБ. К 2021 г. мы планируем разработать систему аттестации специалистов и руководителей подразделений по ИБ, прошедших обучение по программам ВПО и переподготовки. Мы хотели бы четко сформулировать, кто и как должен обеспечивать информационную безопасность в финансово-кредитном блоке, и создаем соответствующий аналог сертификации Банка России в области операций. Слово представителю регулятора в этом направлении.

Анатолий Марченко, начальник отдела управления ФСТЭК России: Федеральная служба по техническому и экспортному контролю (ФСТЭК) является федеральным органом исполнительной власти, который осуществляет госполитику по реализации таких вопросов, как противодействие иностранным техническим разведкам, техническая защита информации и обеспечение безопасной критической информационной инфраструктуры. И в рамках своих ограниченных полномочий в сфере образования мы занимаемся методическим руководством, подготовкой, переподготовкой и повышением квалификации специалистов в области защиты информации. Поэтому ФСТЭК имеет право утверждать квалификационные требования к специалистам по защите информации, разрабатывать и утверждать программы переподготовки и повышения квалификации. В том числе, в области кредитно-финансовой сферы.

Стоит напомнить, что по заказу ФСТЭК России разработаны и утверж-

дены квалификационные требования к специалистам по защите информации, которые вошли в Единый квалификационный справочник должностей руководителей, специалистов и служащих, утвержденный приказом № 205 Минздравсоцразвития.

Раздел «Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации» описывает характеристики 5 должностей, 3 руководителей и 7 специалистов по защите информации. Служба принимала большое участие в разработке профессиональных стандартов, о которых уже говорили коллеги. Мы принимали участие в разработке программ ДПО, которые велись при участии соответствующих образовательных организаций. Сегодня в рамках ДПО работают четыре программы переподготовки и восемь программ повышения квалификации. Есть и еще одна программа — программа повышения квалификации по обеспечению безопасности персональных данных, которая утверждена приказом Министерства труда. В настоящее время над своей программой работает Банк России.

Хочу отметить, что у нас не существует типовых программ. Заинтересованное ведомство может взять за основу примерные программы в области ДПО и ВПО для разработки собственной программы повышения квалификации. ФСТЭК России, в соответствии

с приказом Министерства образования, имеет право рассматривать программу профессиональной переподготовки, высказывать свое мнение и согласовывать ее в части своей компетенции, а именно: технической защиты информации.

Замечу, что качество образования зависит не только от ФГОСов, но и от профессионального сообщества — преподавателей, которые должны иметь базовое образование в области ИБ, от учебной материально-технической базы, используемой в образовательном процессе, и от самой организации образовательного процесса. То есть качество во многом зависит от того, как это все реализуется в образовательных организациях.

А КАК НА «ЗЕМЛЕ»?

Руслан Вестеровский: Слово Сергею Ерохину — ректору МТУСИ, одного из ключевых университетов в сфере подготовки специалистов по ИБ.

Сергей Ерохин, ректор Московского технического университета связи и информатики: Мы являемся отраслевым университетом, находимся в ведении Федерального агентства связи. В подчинении у Агентства четыре университета — в Москве, Санкт-Петербурге, Самаре и Новосибирске. Есть восемь филиалов от Архангельска до Ростова-на-Дону и от Хабаровска до Санкт-Петербурга. Они ведут подготовку по пяти из одиннадцати специальностей по ИБ. В этом году мы выпускаем 200 человек по всем направлениям подготовки по ИБ. Контрольные цифры приема на этот год — более 250 человек.



Андрей Ермаков, заместитель руководителя фонда «Талант и успех»



Юрий Малинин, ректор Академии информационных систем



Артем Сычев, заместитель начальника ГУБ иЗИ Банка России

В университетах мы готовим не только по классической программе по 10-му направлению ИБ, у нас есть профили по информационной безопасности в другом направлении ФГОС — «информатика и вычислительная техника». Это IT-специалисты с «окраской» ИБ. Есть профили по ИБ в инфокоммуникации. И на всех выпускников есть спрос.

Мне было грустно слышать выступление Сергея Пазизина, который с некоторым пессимизмом высказался о выпускниках, предпочитая им людей с опытом. Мы, как университеты, прежде всего, заинтересованы в том, чтобы готовить качественных специалистов, чтобы их не надо было доучивать на производстве. Как это сделать?

Текущее законодательство дает много механизмов, чтобы качество образования выпускников соответствовало ожиданиям работодателя. И если у предприятия есть постоянная потребность в сотрудниках по направлению ИБ, приходите к нам. Есть много способов оценить молодого специалиста. Это преддипломная практика, целевая под-

готовка, что особенно важно для регионов. Это базовые кафедры и образовательные центры. У нас есть успешный опыт сотрудничества с Лабораторией Касперского и компанией 1С.

Каждый год мы актуализируем образовательные программы, добавляем новые курсы. Например, в этом году у нас появились курсы по распределенному реестру и технологии блокчейна для магистров. Это веяние времени. Самое главное, мы можем готовить в два раза больше специалистов по ИБ, чем готовим сейчас.

Руслан Вестеровский: Спасибо. От себя добавлю, что Банк России тоже начал активно привлекать студентов старших курсов, организуя стажировки и практики. За 2017 г. больше 200 человек прошли через эту студенческую программу. Это очень хороший результат.

ПРОБЛЕМЫ ПРЕПОДАВАНИЯ

Артем Сычев, заместитель начальника ГУБ иЗИ Банка России: Человек физиологически меняется не так бы-

стро, как информационные технологии. Поэтому врачи выходят из мединститутов уже с опытом работы, а в нашей сфере выпускникам этот опыт только предстоит получить. В ФинЦЕРТ Банка России сегодня работают два выпускника, которые прошли стажировки и были интегрированы в структуру нашей организации. Это подтверждение того, что с вузами мы готовы работать и работаем.

Мы также готовы работать и как преподаватели, но тут есть проблемы. Первая: учебные мероприятия требуют гибкого подхода кафедр к загрузке привлеченного преподавателя, так как неизбежен отрыв от основной работы. Вторая и главная: объем документации, которую преподаватель должен заполнить, занимает 80% времени при подготовке к учебному курсу. Этот вопрос необходимо решать, поскольку часто именно эта проблема мешает привлечению в университеты квалифицированных специалистов. А приглашение опытного специалиста-практика — это единственная возможность подгото-

вить студента так, что на конкретном рабочем месте ему останется только войти в курс дела.

КАК РАБОТАТЬ С ТАЛАНТАМИ?

Руслан Вестеровский: Еще одно направление: поиск талантов. Недавно Банк России, Ассоциация Финтех и Образовательный центр «Сириус», который находится под управлением Образовательного Фонда «Талант и успех», подписали соглашение о сотрудничестве. Планируется большой спектр совместных проектов.

Андрей Ермаков, заместитель руководителя Образовательного фонда «Талант и успех», Образовательный центр «Сириус»: Мы работаем с теми самыми талантливыми школьниками, которые через несколько лет станут локомотивами отечественной экономики. У нас порядка 20 тыс. выпускников и ежемесячно их становится больше. 70% из них ориентируются на сферу IT. Не потому, что там большие зарплаты, главное для них — получить от работодателя сложную задачу. Эти ребята заметно отличаются от остальных, управлять ими трудно. Например, у них большая смычка между работой и личной жизнью, они часто асоциальны, но именно они могут совершить технологический прорыв, повернуть ход истории. О чем я говорю? О том, что, если не изменить подход и отношение к талантливым кадрам, их исход из профессии через какое-то время будет массовым.

Многие партнеры, с которыми работает «Сириус», создают департаменты по работе с талантливыми детьми. Эти структуры понимают, как надо работать с талантами, как ставить задачи, что получать в ответ. Это сложная комплексная работа и вести ее нужно со старших классов.

Сегодня скорость изменения технологий и появления новых вызовов такова, что за время между окончанием школы и выходом человека на работу меняется многое. Если за это время мы расслабляем студента, не даем ему интересных задач, не включаем в процесс развития, взаимодействия с отраслью, то любой, даже самый талантливый школьник, перегорает или находит своим талантам другое применение.

На базе «Сириуса» мы запускаем инновационный НТИЦ из трех лабораторий: когнитивное исследование в образовании, биотех и IT. Основная цель лабораторий — произвести смычку между работодателями и выпускниками «Сириуса». Один из партнеров по направлению ИБ — Центробанк.

Руслан Вестеровский: Действительно, сейчас перед компаниями стоят вопросы, как работать с разными поколениями: что предлагать, как интегрировать? В Центробанке мы стараемся, чтобы система мотивации была ориентирована на разные возрастные группы с учетом их интересов.

ОБУЧЕНИЕ ВЗРОСЛЫХ

Руслан Вестеровский: И еще одна тема нашей дискуссии — это дополнительное профессиональное образование, — важнейший компонент обучения людей со стажем работы.

Юрий Малинин, ректор Академии информационных систем: Главное достоинство центров, аналогичных нашему, — мы мобильны, потому что жесткие требования Минобрнауки направлены напрямую в сторону вузов и мало затрагивают нас. За счёт этого мы можем оперативно менять программу. На подготовку программы переподготовки продолжительностью от 360 ч. мы затрачиваем полгода, проходим согласования, и запускаем. Это не касается краткосрочных программ, а в сфере ИБ повышение квалификации начинается от 40 ч. (а не от 16 ч., как для других отраслей). Это было заложено изначально, с учетом мнений регуляторов и экспертного сообщества. На переподготовку специалистов в области ИБ необходимо не менее 360 ч. Опыт показал, что программы профессиональной переподготовки в ИБ занимают в среднем 500 ч. и выше. И эти программы востребованы среди работодателей и слушателей.

Сегодня много говорили о создании более тесной связки производства с работодателями, с вузами. Эта связка есть, она развивается, движется, создаются учебные лаборатории совместно с работодателями, учебные лаборатории совместно с вузами. Именно у университетов есть фундаментальная материальная база за счёт государственного и целевого финансирования, хотя это-

го бывает и недостаточно. Есть академии Cisco, Huawei, учебные центры крупных компаний — это все результат взаимодействия. Есть ещё формы сетевого взаимодействия, которые появились относительно недавно, но активно используются. Идея заключается в создании сильной лаборатории на базе одного крупного и успешного вуза в регионе, и использования этой дорогостоящей лаборатории другими вузами и учебными центрами.

Многим интересен портрет того, кто приходит на переподготовку по направлению ИБ. Мы провели анализ и получили слушателя 32 лет, мужчину (89%) с высшим образованием (93%). Люди повышают квалификацию и проходят переподготовку, имея базовое образование, хотят карьерного роста и понимают всю необходимость переподготовки.

И о развитии онлайн-образования, спрос на которое будет повышаться, в ближайшие три года ожидается прирост до 10% в год. Минобрнауки, регуляторы отметили активность в продвижении дистанционного онлайн-образования, и тут необходим федеральный закон об электронном обучении. Я думаю, когда закон примут, продвижение этой формы обучения станет еще более активным.

УЧЕНАЯ СТЕПЕНЬ

Евгений Белов: Мы забыли еще один аспект — вопрос научной специальности и наличия ученой степени в этой области. Сегодня базовое образование по группе ИБ или ученую степень по научной специальности, связанной с вопросами защиты информации, имеют не более 30% специалистов. И в ближайшей перспективе вопрос научной степени встанет остро. Поэтому требования по переподготовке надо вводить в профстандарты как в области защиты информации, так и в смежных отраслях.

* * *

В завершение сессии Руслан Вестеровский поблагодарил коллег и подчеркнул, что состоявшийся разговор имеет исключительно важное значение для развития кадрового потенциала отрасли ИБ в целом и ИБ кредитно-финансовой сферы в частности.



Александр БОДРИК
заместитель генерального директора
по развитию бизнеса ANGARA
Professional Assistance, CISA, ITIL Expert



Фарит МУЗИПОВ
руководитель проекта
ИБ АО «РЭЦ», CISA,
CISM, CRISC

НА ПЕРЕПУТЬЕ

ИСТОРИЯ ОДНОГО ПОИСКА РАБОТЫ

В один солнечный день в банк топ-100 была введена временная администрация, и перед отделом ИБ и его руководителем (всего 3 человека) встала задача поиска нового работодателя. Поиск осложнялся тем, что CISO работал в банке третий год и не имел намерения его покидать — руководство и процессы были достойного уровня. То есть путей отступления он заранее не подготовил.

Первым делом CISO навел справки у коллег и разослал письма: кто мог бы забрать сотрудников отдела ИБ? Каждый из бойцов обладал значимыми компетенциями, и обоих довольно быстро подобрали ИТ-компании. К настоящему времени оба вполне успешны на своих должностях.

CISO И ПОИСК РАБОТЫ

А вот работа для самого CISO нашлась не сразу. Нужно отдать должное, банк выполнил свои обязательства по выплате выходного пособия, что несколько ослабило давление материальных обстоятельств.

Основные встречи и переговоры CISO вел с крупными банками и ин-

теграторами, предлагали ему, как правило, позицию консультанта. Позиция вполне удовлетворительная, но для нашего CISO все же недостаточная. Тем более, что сам по себе активный поиск, частые переговоры, доброжелательный отклик коллег предоставляли на тот момент главное — ощущение востребованности и эмоциональную поддержку. CISO видел, что рынку специалисты его уровня нужны, и понимал, вернее, ощущал, что достойная работа рано или поздно появится.

В конце концов, примерно через полгода он получил оффер от крупного банка и готов был его принять, но неожиданно пришел еще один оффер — от небольшого государственного банка, где нужно было трансформировать и со временем возглавить функцию ИБ.

Перед CISO встала дилемма. В крупном банке светила перспектива стать «винтиком» корпоративной машины. Но несколько друзей CISO уже были поглощены аналогичными машинами и благополучно «потонули» в корпоративной рутине, оставив в ней как мечты о развитии и творчестве, так и, похоже, свои перспективы.

В небольшом банке ключевым и, собственно, и определившим выбор преимуществом была возможность самостоятельно закрывать широкий и разнообразный спектр задач по ИБ.

ИСПЫТАТЕЛЬНЫЙ СРОК

Важный момент: испытательный срок оказался действительно испытанием, вступительным экзаменом. Перейдя в новый для себя вид банка (государственный банк), CISO столкнулся и с новыми вызовами («Мозги первое время просто кипели»). Однако ранее накопленный опыт и набор личностных качеств помог и «выплыть», и преуспеть.

Аллегорически ситуацию можно представить так. В любой организации есть некая система управления ИБ. Даже если нет подразделения или офицера по ИБ, то обязательно есть или грамотный администратор, у которого «болит душа» (с «пристрастием» настраивает FW, AV), или ответственные бизнес-руководители, отчетливо понимающие, что информация — такой же актив, как и финансовые средства, и аккуратность в обращении с ней является обязательным условием непрерывности бизнес-процессов и реализации стратегий.

В конце концов, всегда есть тот самый спонсор (драйвер) функции ИБ, который и инициировал либо активно поддержал создание подразделения/должности лидера ИБ, и готов тему ИБ обсуждать и продвигать.

CISO ВИДЕЛ, ЧТО РЫНКУ СПЕЦИАЛИСТЫ ЕГО УРОВНЯ НУЖНЫ, И ПОНИМАЛ, ВЕРНЕЕ, ОЩУЩАЛ, ЧТО ДОСТОЙНАЯ РАБОТА РАНО ИЛИ ПОЗДНО ПОЯВИТСЯ



Совокупно спонсор и текущие участники системы ИБ составляют потенциальный пул для поиска и привлечения союзников, без которых новому лидеру ИБ будет проблематично не то, что проводить какие-то преобразования, но даже пройти испытательный срок.

Мораль простая. Лидер по ИБ обязан быть гибким. Навязывая в зубах ситуация «Ребята, вы все делаете неправильно!» чаще всего приводит к печальному исходу, потому что невозможно добиться реальных изменений в организации без конструктивного общения со смежниками, спонсором и ключевыми участниками системы управления ИБ. Тут альтернативы нет: договаривайся или проиграй!

Наш CISO сумел договориться.

РАБОТА НА УПРЕЖДЕНИЕ

Какой опыт можно извлечь из этой истории?

Урок первый. Потеря работы — как гром среди ясного неба. Поэтому к поиску новой работы нужно быть готовым заранее, то есть всегда.

Урок второй. При поиске работы нужно отчетливо понимать, какие проблемы («головняк») мы должны решить для нанимающей нас организации и непосредственно ее руководителя. В идеале нужно проактивно моде-

лировать разные ситуации и развивать соответствующие компетенции «на всякий случай».

Урок третий. Как писал известный юморист Роберт Асприн: «Доблесть неизвестная не лучше неизвестной трусости». В реальной жизни ни один руководитель не пригласит на собеседование (если речь идет о достаточно высокой должности) человека, которого не знает, никогда не слышал о нем и не имеет на него рекомендаций. Неизвестный рынку специалист не попадет в шорт-лист, будь он хоть трижды подходящий.

Урок четвертый. Теория «Сила слабых связей» — это сила! Основной выигрыш при поиске работы дают именно «слабые связи» (люди, с которыми видишься всего несколько раз в год). Для развития сети «слабых связей» возможно участвовать в волонтерских движениях, профессиональных ассоциациях (например, ISACA), комитетах АРБ и ТК, конференциях, социальных сетях и т.д. В профессиональных и волонтерских организациях всегда есть определенный фронт работ («поляна» для деятельности), в том числе и для молодых специалистов без большого опыта и редких навыков. Такая активность позволяет получить нужные контакты и в принципе понять, как мыслят корпоративные безопасности.

Урок пятый. Слова кандидата о самом себе в ходе собеседования (интервью) подвергаются большему сомнению, чем его репутация — когда он получает независимые рекомендации с рынка от внешних людей. Также очевидно, что рекомендации от участников профессиональных сообществ намного ценнее иных вариантов («брат», «сват» и т.п.).

Урок шестой. Испытательный срок — это еще не работа, а вступительный экзамен, составляющая процесса поиска работы. Тут главное — способность интегрироваться в новую систему взаимоотношений, а значит, умение договариваться. Голой конфронтацией надежной ИБ не построить. В одной из организаций директор по ИТ как-то воскликнул: «Наконец-то пришел безопасник, с которым можно работать (в смысле договариваться — авт.)».

Главный вывод. Информационная безопасность — это гораздо больше о людях, чем о технике. Технику создают, выбирают, внедряют и эксплуатируют люди. Поэтому технические знания, образование, опыт — это необходимое, но далеко не достаточное условие при приеме вас (нас) на новую хорошую работу.

КАК ПОВЫСИТЬ?

ГЛАВА 4. КАК ПРАВИЛЬНО НАЧАТЬ, ЧТОБЫ ПРАВИЛЬНО ЗАКОНЧИТЬ

(Продолжение. Начало
в № 3,4/2017, №1/2018)

Этой статьей мы продолжаем серию публикаций о практических аспектах повышения осведомлённости в области информационной безопасности. В последних двух статьях мы рассмотрели вопросы получения поддержки руководства организации для реализации корпоративной программы повышения осведомлённости, а также возможности повышения осведомлённости собственными силами, без привлечения внешних консультантов.

И вот, руководство, наконец-то, поддерживает вас в стремлении реализовать программу повышения осведомлённости, а выбор, делать ли проект собственными силами или привлекать внешних соисполнителей, сделан. Теперь надо двигаться дальше — начинать проект разработки и реализации этой самой программы повышения осведомлённости. При этом, когда впервые начинаешь какое-либо ответственное предприятие, всегда полезно заранее подумать о том, как правильно его начать, чтобы потом правильно закончить.

ЦЕЛИ — ОБОСНОВАННЫЕ, ПОНЯТНЫЕ, ДОСТИЖИМЫЕ

Здесь мы не имеем ввиду формальные цели программы повышения осведомлённости, которые обычно прописывают в концепциях и аналогичных декла-

ративных документах — мы говорим о фактических практических целях, которые вы ставите перед собой и командой и за достижение которых несёте ответственность.

Обоснованные. Цели должны быть обусловлены именно вашими условиями, прогнозами развития и практическими нуждами организации. То есть программа повышения должна быть направлена на снижение наиболее вероятных рисков, наносящих бизнесу наибольший возможный ущерб. Иными словами, программа повышения осведомлённости должна иметь максимальный ROI при минимальном сроке окупаемости.

Понятные. Цели не должны быть абстрактными, при этом они должны быть понятны 1) вам, 2) руководству, 3) коллегам-соратникам, с которыми вы вместе запускаете программу повышения. Кроме того, каждому должно быть понятно, какие выгоды в результате реализации программы получит лично он, ибо личная выгода есть мотив искренности отношений.

Достижимые. Не следует ставить сверхцелей, которых вы заведомо не сможете достигнуть, или которых, хуже того, просто не нужно достигать. В условиях сильно ограниченных ресурсов их трата на неверно поставленные цели быстро обречёт на провал всю инициативу. Поэтому нужно иметь стратегическое видение, но действовать тактически грамотно.

Например, по итогам реализации программы можно ожидать усвоение

пользователями 3–5 основных (то есть, по результатам анализа статистики ИБ-инцидентов за последний год, «закрывающих» 80–90% инцидентов) правил обеспечения информационной безопасности с формированием устойчивых навыков правильного поведения «в случае если» (получил подозрительное email-сообщение — распознал фишинг, не открывая, удалил). Как следствие, целью в этом случае может являться сокращение количества ИБ-инцидентов, связанных с персоналом, скажем, на 70%.

Не лучшим вариантом цели, по нашему мнению, является формулировка вроде «создание корпоративной культуры обеспечения персоналом информационной безопасности». Вне сомнений, это стратегическая цель любых организованных усилий по повышению осведомлённости персонала. Однако, с тактической точки зрения, ресурсы на программу повышения вы тратите сейчас, а вышеупомянутую корпоративную культуру вам удастся создать лишь по прошествии нескольких «волн» реализации программы (срок от года до нескольких лет), поэтому неизбежно встанет вопрос обоснования эффективности расходования ресурсов. Ещё один отдельный и сложный вопрос — выработка и согласование критериев, по которым можно с уверенностью судить, создана ли корпоративная культура или ещё нет.

БЕЗ ДРУЗЕЙ МЕНЯ ЧУТЬ-ЧУТЬ, А С ДРУЗЬЯМИ — МНОГО!

Проекты повышения осведомлённости с точки зрения проектного управления являются проектами повышенной сложности: большая организационная значимость проекта (а значит и сильное организационное сопротивление ему), наличие нескольких заинтересованных сторон (часто с взаимно про-

КАЖДОМУ ДОЛЖНО БЫТЬ ПОНЯТНО, КАКИЕ ВЫГОДЫ В РЕЗУЛЬТАТЕ РЕАЛИЗАЦИИ ПРОГРАММЫ ПОЛУЧИТ ЛИЧНО ОН, ИБО ЛИЧНАЯ ВЫГОДА ЕСТЬ МОТИВ ИСКРЕННОСТИ ОТНОШЕНИЙ

тивоположными интересами) и люди как «целевая аудитория» для результатов — всё это порождает множество рисков, управлять которыми в одиночку довольно сложно.

Вы существенно повысите шансы на успех, если привлечёте к реализации проекта (будем конкретнее — включите в команду проекта) авторитетных представителей других заинтересованных подразделений (например, кадровиков и/или юристов). И в дальнейшем обязательно будете поддерживать на высоком уровне их вовлечённость в проект. Так вы не только превратите многих противников в союзников (или хотя бы в немешающих), но и действительно поспособствуете объективному улучшению результатов программы повышения.

ТОЧНОЕ ОПРЕДЕЛЕНИЕ КРИТЕРИЕВ УСПЕШНОСТИ

Вопрос эффективности повышения осведомлённости (в том числе экономической) как метода обеспечения информационной безопасности актуален для многих. Вы должны быть готовы к тому, что с вас спросят за каждый потраченный на реализацию программы повышения рубль и человеко-час. Поэтому по итогам реализации программы необходимо иметь недвусмысленные свидетельства того, что после программы стало заметно лучше, чем было до неё. Ключевое слово здесь — «заметно»: эффект должен быть существенно положительным (а значит чётко идентифицируемым и измеримым) и являться следствием именно реализации программы повышения.

До начала программы необходимо договориться со всеми заинтересованными сторонами об ожидаемых каждой стороной результатах, а также о том, по каким критериям будет приниматься решение об успешности программы в целом. Требование измеримости эффекта влечёт необходимость определения метрик, характеризующих обеспечение персоналом информационной безопасности до и после реализации программы. Выбор таких метрик и разработка методики интерпретации их значений — весьма важная в политическом и техническом смыслах задача.

ВЫ СУЩЕСТВЕННО ПОВЫСИТЕ ШАНСЫ НА УСПЕХ, ЕСЛИ ВКЛЮЧИТЕ В КОМАНДУ ПРОЕКТА АВТОРИТЕТНЫХ ПРЕДСТАВИТЕЛЕЙ ДРУГИХ ЗАИНТЕРЕСОВАННЫХ ПОДРАЗДЕЛЕНИЙ

ТЩАТЕЛЬНОЕ ПЛАНИРОВАНИЕ

Прописная истина проектного управления: правильное планирование — 50% успеха проекта. Конечно, это справедливо и для проектов реализации программ повышения осведомлённости. Однако, заострим внимание на другом — на степени детализации планирования программ повышения осведомлённости. Чем детальнее будет разработанный и согласованный с другими участниками план реализации программы повышения, тем больше вероятность общего успеха. Детальный план подразумевает определение:

- ◆ целей, задач и результатов программы с привязкой к стратегии развития и нуждам организации;
- ◆ системы метрик, характеризующих ход реализации, охват и эффективность программы;
- ◆ состава команды проекта, ролей её членов и их зон ответственности;
- ◆ ресурсных потребностей, объёма и графика выделения ресурсов для реализации программы;
- ◆ целевых аудиторий (высшее руководство, ИТ/ИБ-персонал, линейные руководители, рядовые сотрудники, аудитории, выделяемые по иным критериям);
- ◆ перечня тем для повышения осведомлённости в разрезе целевых аудиторий;
- ◆ методов и средств повышения осведомлённости в разрезе тем и целевых аудиторий;
- ◆ требований к материалам для повышения осведомлённости (к контенту, графическому оформлению, технические требования и другие);
- ◆ состава работ по разработке материалов для повышения осведомлённости;
- ◆ состава работ по обучению персонала с использованием разработанных материалов;

◆ методов и средств сбора обратной связи;

◆ процедур пересмотра и модернизации программы повышения.

Конечно, то, насколько детально удастся разработать план напрямую зависит от глубины (степени зрелости) имеющегося видения командой проекта процесса повышения осведомлённости (основные черты которого мы описали в нашей первой статье, см. № 3 2017 г.). Именно поэтому до начала разработки программы важно иметь собственное чёткое представление о предстоящей программе, ключевых этапах её реализации, а также, главное, о том, какой эффект она должна оказать на обеспечение безопасности деятельности организации.

* * *

Подведём итоги — на что стоит обратить внимание на этапе подготовки и планирования программы повышения осведомлённости:

1. Выработка и согласование фактических целей программы — важный этап. Цели должны быть обоснованы «жизнью» и согласованы со всеми участниками, должны быть конкретными и достижимыми;
2. В команду проекта должны входить представители других заинтересованных в результатах подразделений. Необходимо поддерживать их вовлечённость в проект на протяжении всей программы;
3. Метрики, характеризующие ход реализации программы, и критерии оценки её успешности должны быть разработаны и согласованы до начала реализации;
4. Степень детализации плана программы повышения должна быть максимальной с учётом необходимости его согласования со всеми участниками.

ЛОВЛЯ БЛОХ ЗА ДЕНЬГИ

ПРОГРАММЫ BUG BOUNTY В РОССИИ И ЗА РУБЕЖОМ



Марина БРОДСКАЯ
обозреватель
BIS Journal

Заработать на поиске уязвимостей становится проще. К многочисленным международным и отечественным IT-компаниям, которые регулярно выплачивают премии исследователям программного обеспечения, присоединяется Российская Федерация. Согласно плану мероприятий по информационной безопасности программы «Цифровая экономика Российской Федерации», который был утвержден в конце декабря 2017 г. правительством страны, поиск «черных ходов» в ПО начинается в апреле текущего года. Работы по отечественной программе bug bounty будут вестись до конца 2020 г., исследователи получают премии и призы 500 млн руб. бюджетных и 300 млн руб. внебюджетных средств. За реализацию проекта отвечают Минкомсвязи, ФСБ и ФСТЭК, исполнителем назначен Центр компетенций по импортозамещению в сфере информационно-коммуникационных технологий.

КАК ЭТО БУДЕТ

Протестировать программное обеспечение отечественных и зарубежных производителей смогут как физические, так и юридические лица. Программа bug bounty предполагает две модели тестирования. В первом случае исследователям будет известен заказчик пентеста, который даст доступ к системе и предложит свою схему тестирования. Во втором случае тестирование будет производиться без ведома разработчика программного продукта.

Как рассказал в интервью газете «Ведомости» руководитель Центра компетенций по импортозамещению в сфере ИКТ Илья Массух, тесты пройдут

рыночные IT-платформы, операционные системы, системы управления базами данных. Средства между этими двумя моделями будут распределяться в пропорции примерно 75 на 25. Системы массового потребления будут тестироваться всеми желающими. Часть работ по программе bug bounty будет доступна лишь для компаний, поскольку тестирование может потребовать доступа к инфраструктуре систем. Информация о найденных уязвимостях будет раскрываться после выхода патчей или оставаться доступной только разработчику и вендору системы. В случае отказа разработчика устранить найденную уязвимость возможен запрет использования такого ПО. По мнению опрошенных «Ведомостями» специалистов в области ИБ, сведения о найденных уязвимостях могут стать ценной информацией в руках заинтересованных ведомств. Внятных ответов от представителей Минкомсвязи и Сбербанка изданию не получило.

По данным самого Плана мероприятия по направлению ИБ (программы «Цифровая экономика РФ»), поиск и исправление уязвимостей предполагается в разработанном отечественном программном и программно-аппаратном обеспечении в рамках повыше-

ния его надежности. Исследователи будут получать вознаграждения (гранты) за найденные уязвимости. Финансирование разработок будет осуществляться венчурными фондами, созданными для стимулирования разработки отечественного ПО и увеличения его доли в условиях цифровой экономики.

Выделение средств на поиск уязвимостей будет проводиться из расчета 100 млн (внебюджетное финансирование) в 2018 г., 200 млн (бюджет) и 100 млн (вне бюджета) в 2019 г. и по 200 млн из бюджетных и внебюджетных средств в 2020 г. Выдача денежных премий (призов) за найденные уязвимости в программном и программно-аппаратном обеспечении будет проводиться с апреля 2018 г. до 31 декабря 2020 г. Ответственные: Минкомсвязь, ФСБ, ФСТЭК, АНО «Центр компетенций по импортозамещению в сфере ИКТ» и АНО «Цифровая экономика».

Информации о том, кто из юридических лиц будет допущен к работе по программе и на каких условиях, найти не удалось. Сведений о том, сколько будет получать один тестер в случае обнаружения уязвимости, пока так же нет.

Дополнительно, с марта по июнь 2018 г. Фондом «Сколково» при участии

**КАК РАССКАЗАЛ РУКОВОДИТЕЛЬ
ЦЕНТРА КОМПЕТЕНЦИЙ ПО
ИМПОРТОЗАМЕЩЕНИЮ В СФЕРЕ
ИКТ ИЛЬЯ МАССУХ, ТЕСТЫ ПРОЙДУТ
РЫНОЧНЫЕ IT-ПЛАТФОРМЫ,
ОПЕРАЦИОННЫЕ СИСТЕМЫ, СИСТЕМЫ
УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ**

Минкомсвязи, ФСТЭК и ФСБ России должен быть проведен «Комплексный анализ и оценка потенциальных уязвимостей, угроз и рисков информационной безопасности, характерных для систем, реализованных на технологиях облачных, туманных, квантовых, виртуальных, искусственного интеллекта и дополненной реальности, а также сравнительная оценка экономического эффекта от внедрения облачных, туманных, квантовых технологий, систем виртуальной и дополненной реальности и технологий искусственного интеллекта» и соответственно утвержден отчет. На эти цели из бюджета будет потрачено дополнительно 59 млн руб. Еще 50 млн уйдут на «проведение исследований по оценке уязвимости web-приложений, размещенных в российском сегменте сети «Интернет» (цитата по документу).

ИСТОКИ И РАЗВИТИЕ

История поиска уязвимостей в программном обеспечении началась примерно в 1995 г., когда выяснилось, что разработчики ПО компании Netscape Communications Corporation (США) самостоятельно ищут и исправляют ошибки в браузере Mosaic / Netscape / Mozilla. Тогда же, с подачи инженера Джарретта Ридлингера появился термин «bug bounty». На программу Netscape Bug Bounty Program было выделено \$50 тыс., что некоторые руководители компании посчитали бесполезной тратой средств и времени. Однако программа полностью оправдала себя.

Сегодня программы bug bounty запущены во многих компаниях, среди них Mozilla, Facebook, Yahoo!, Google, Reddit, Square, и Microsoft, Yandex, Одноклассники, ВКонтакте, Mail.Ru и пр.

Поиск уязвимостей поставлен на промышленную основу, существуют сообщества экспертов-исследователей, которые специализируются на тестах и выявлении брешей и ошибок разработчиков. Компании Facebook, Microsoft, Ford Foundation, Hackerone и GitHub выступили спонсорами bug bounty сообщества (internetbugbounty.org) и оплачивают найденные уязвимости в продуктах с открытым кодом и программном обеспечении, если его вендор не проводит собственную программу по поиску уяз-

Компания	Минимальная выплата	Максимальная выплата
Intel	\$500	\$30 000
Yahoo	—	\$15 000
Snapchat	\$2000	\$15 000
Cisco	\$100	\$2500
Dropbox	\$12 167	\$32 768
Apple	—	\$200 000
Facebook	\$500	нет предела
Google	\$300	\$31 337
Quora	\$100	\$7000
Mozilla	\$500	\$5000
Microsoft	\$15 000	\$250 000
OpenSSL	\$500	\$5000
Vimeo	\$500	\$5000
Apache	\$500	\$3000
Twitter	\$140	\$15 000
Paypal	\$50	\$10 000
GitHub	\$200	\$10 000
Uber	—	\$10 000
Perl	\$500	\$1500
PHP	\$500	\$1500
Starbucks	\$100	\$4000
AT&T	\$500	нет предела
Word Press	\$150	нет предела

Таблица 1. Лучшие программы по поиску уязвимостей 2018 г.

вимостей. По некоторым данным, доход эксперта по поиску уязвимостей, работающего на постоянной основе, может составить до \$25 тыс. в месяц.

Например, в 2017 г. компания Google выплатила \$2,9 млн 274 специалистам, сумевшим найти различные уязвимости в её программах. Финансирование происходит в рамках Google Vulnerability Reward Program (VRP). Так, \$112,5 тыс. получил исследователь Гуан Гум, который выявил цепочку эксплойтов в смартфонах Pixel. На поиск брешей в ОС Android было потрачено \$1,1 млн, из этой суммы \$125 тыс. было выделено на тендеры, гранты получили 50 че-

ловек. \$50 тыс. получили специалисты, занимающиеся регулярным обновлением системы. Всего за годы работы VRP компания Google потратила \$12 млн. По словам представителей компании, эти затраты окупаются. Согласно приведенным на сайте VRP расценкам, цена одной найденной уязвимости составляет от \$100 до \$31 337 в зависимости от значимости ошибки.

С 2011 г. занимается поисками уязвимостей безопасности компания Facebook. Исследователи могут искать ошибки в множестве сервисов и приложений, использовать тестовые аккаунты, минимальная сумма вознаграж-

НАСТОЯЩИЕ ИССЛЕДОВАТЕЛИ НЕ ОСТАНАВЛИВАЮТСЯ НА ПОВЕРХНОСТНОМ ИЗУЧЕНИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, А ИДУТ ГЛУБЖЕ, БЕЗ ИСПОЛЬЗОВАНИЯ СТАНДАРТНЫХ ПРОГРАММ ПО ПОИСКУ УЯЗВИМОСТЕЙ

дения — \$500. За 2017 г. компания потратила на программу Facebook's 2017 Bug Bounty более \$880 тыс., вознаграждения получили более 100 исследователей. Всего за 6 лет на программу потрачено \$6,3 млн. Получено 12 тыс. заявлений. Более 400 из них сделано исследователями из Индии, США, Тринидада и Тобаго. По сравнению с 2016 г. средняя выплата составила \$1900 против \$1675. 32% исследователей приняли участие в программе впервые.

Программа Яндекса по устранению уязвимостей называется «Конкурс «Охота за ошибками». Она стартовала осенью 2012 г., участникам предлагается искать ошибки в браузере поисковика, в сервисах Яндекса в различных доменах и в мобильных предложениях. Минимальная ставка 5500 руб., максимальная — 170 тыс. руб. При работе с Яндекс.Браузером ставка за нахождение критически важной уязвимости вырастает до 250 тыс.

ИССЛЕДОВАТЕЛЬ ИЛИ УГОЛОВНИК?

Хакерство наказуемо, соответствующие статьи прописаны в уголовных кодексах большинства стран мира. И если в России можно отделаться условным наказанием или незначительным сроком, то в США хакеру грозят десятки лет тюремного заключения.

Чтобы потом не доказывать правоохранительным органам, что исследователь — всего лишь искатель потенциальных брешей с намерениями заработать деньги честным путем, большинство IT-компаний прописывает правила, которые следует соблюдать в ходе работ: зарегистрироваться, работать под своим именем, использовать тестовые аккаунты и входы. Также необходимо соблюдать политику лояль-

ности компании и не разглашать сведения о найденных уязвимостях в течение определенного срока. Нередки случаи, когда не дождавшийся закрытия уязвимости исследователь публиковал сведения об ошибках разработчиков и попадал за решетку.

Нередки и случаи, когда найденные уязвимости реализуются на «черном рынке», поскольку разработчики программного продукта не проявили интереса к обнаруженной «дыре», в отличие от хакеров, которые готовы предложить за нее хорошую цену. Вопросы этики «белых хакеров» в данном случае не рассматриваются.

Как правило, участвовать в программах и конкурсах могут все желающие, однако некоторые компании (например, Facebook) указывают, что получение вознаграждения может быть невозможно по политическим мотивам.

В России отношения исследователя и компании, объявившей о программе поиска уязвимостей, подпадают под действие Гражданского кодекса РФ, а в случае разногласий о правомерности доступа к компьютерной информации — под Кодекс об административных правонарушениях и Уголовный кодекс РФ, где компьютерным преступлениям посвящена глава 28.

Отдельный вопрос — ответственность пентестеров как представителей юридического лица. Часто компании, которые специализируются на компьютерной безопасности, выступают аудиторами компьютерных систем крупных организаций. И подписывая акт о соответствии систем всем требованиям ИБ, они гарантируют отсутствие известных уязвимостей на момент проверки систем. Однако это не дает никакой гарантии, что завтра система не будет взломана через вновь открытую уязвимость, упущенную пентестерами.

ЧТО И КАК ИСКАТЬ?

Большинство любителей поискать огрехи в чужом коде работают по верхам и просматривают сервисы на стандартные уязвимости и ошибки. Чаще всего проверка ведется с помощью программ тестирования. Обычно ищут уязвимости xss, sql-injection, php-инклюдинг, crlf-injection, просматривают хакерские запросы по базам поисковых систем, методы обхода каталога, общедоступные резервные копии сценариев, незакрытые порты и пр. Однако тут берет первым, остальные переходят к следующему проекту в надежде заработать хоть каких-то денег.

Настоящие исследователи не останавливаются на поверхностном изучении программного обеспечения, а идут глубже, без использования стандартных программ по поиску уязвимостей, а следуя своим проверенным методам. Потому и цена за выявленную критическую ошибку, а то и не одну, составляет десятки тысяч рублей, долларов или евро, в зависимости от страны-производителя ПО.

В случае с отечественным ПО потребуется повышение квалификации не только искателей уязвимостей, но и самих программистов, которые грешат тем, что пишут экраны программного кода, не всегда удовлетворяющие минимальным требованиям ИБ. Поиск и исправление ошибок в собственном творении вызывает порой большие затруднения у создателей программ.

* * *

Подводить итоги еще не стартовавшей программы по поиску уязвимостей в еще не созданном ПО — дело неблагоприятное. Однако есть опыт зарубежных коллег. Так, Министерство обороны США выявило более ста потенциальных брешей в рамках программы поиска уязвимостей Hack the Pentagon в 2016 г. В проекте Defense Digital Service приняли участие свыше 1400 исследователей. Организаторов поразило не столько число найденных уязвимостей, сколько количество потенциальных хакеров, которые зарегистрировались для участия в программе и поработали на благо государства.



Дмитрий ЛАРИН
кандидат технических наук,
ЗАО «Лаборатория „СКАТ“»

ПЕРИОДИЗАЦИЯ КРИПТОГРАФИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ В РОССИИ

Этой статьей мы начинаем цикл публикаций, посвященный периодизации криптографической деятельности в России.

Под криптографической деятельностью понимается не только шифрование и дешифрование, но и организация каналов передачи сообщений (системы связи), использование различных методов защиты информации (криптография, стеганография, физическая защита линий связи и т.д.), организация перехвата шифрованной информации противника. Дешифрование без перехвата невозможно. Разумеется, сюда входят меры по добычанию информации, облегчающей дешифрование (добывание ключей, описания шифрсистем и т.д.). С другой стороны, при разработке методов и средств защиты информации необходимо учитывать возможные аналогичные действия противника и предпринимать соответствующие меры для их пресечения. Если действия по добычанию информации связаны с разведывательными операциями, то при защите главную роль играют контрразведывательные мероприятия. Поэтому криптографические службы работают в тесном контакте с разведкой и контрразведкой.

Вообще криптографическая деятельность является составной частью информационного противоборства, которое включает в себя организацию

пропаганды и информационного воздействия на потенциального и реального противника и своего населения (поддержка патриотического духа, разъяснение политики государства и т.д.), ведение контрпропаганды, проведение операций по дезинформации противника. В случае проведения операций по информационному воздействию на противника нередко используется криптография. С одной стороны, узнав о дешифровании своих секретных сообщений, можно не усиливать защиту, а продолжать использовать тот же шифр, передавая дезинформацию, которую противная сторона будет принимать за истинную информацию. Такая ситуация называется дезинформацией «под шифром». В этом случае для передачи настоящей информации следует использовать новые шифры и каналы связи. С другой стороны, тайно захватив шифры и ключи противника (или вскрыв их аналитическим путем), можно попытаться от имени истинного отправителя передать противнику дезинформацию. [Гольев, 2008].

Фактически, как только где-то на Земле происходило становление того или иного государства, тут же начиналась криптографическая деятельность, с развитием государственных институтов учреждались специальные криптографические службы. Известный американский историк Дэвид Кан считает, что признаками великой державы яв-

ляются наличие у страны ядерного оружия, успехов в освоении космоса и достижений в области криптографии [Кан, 2004].

Разумеется, не стала исключением и наша страна, история криптографической деятельности в России насчитывает не одно столетие. По словам Д. Кана, «русские вознесли достижения своей страны в сфере криптологии¹ до высоты полета космических спутников» [Кан, 2004, с. 261].

* * *

Данная работа является первым шагом автора в этом направлении, периодизация проведена, исходя из использования тех или иных криптографических идей, под влиянием которых находилась отечественная криптография в определенные временные этапы. В некоторой степени учтены организационные изменения, происходившие в криптографических службах нашей страны. Безусловно необходимо продолжать работу в данном направлении.

¹ На Западе часто употребляется этот термин для обозначения науки о криптографических методах защиты информации. Криптология разделяется на криптографию (науку о создании шифров) и криптоанализ, изучающий методы их взлома. У нас в стране для обозначения данной сферы человеческой деятельности принят термин криптография.



IX ВЕК — 1549 ГОД

СТАНОВЛЕНИЕ СИСТЕМЫ СВЯЗИ В ДРЕВНЕРУССКОМ ГОСУДАРСТВЕ

Для обеспечения секретности передаваемой информации использовались различные методы, в том числе криптографические, однако время регулярных служб по защите информации еще не пришло. Мероприятия по защите информации проводились по мере необходимости и занимался этим сам князь или его доверенные люди. Не существовало каких-либо универсальных подходов к выбору методов и средств, все зависело от ситуации, и в схожих случаях могли приниматься совершенно различные решения.

1549



1549 ГОД — КОНЕЦ XVII ВЕКА

В ПОСОЛЬСКОМ ПРИКАЗЕ СФОРМИРОВАНА

ПЕРВАЯ В НАШЕМ ОТЕЧЕСТВЕ РЕГУЛЯРНАЯ ШИФРОВАЛЬНАЯ СЛУЖБА

Активное использование шифров для защиты русской дипломатической переписки. Для усовершенствования системы связи был учрежден Ямской приказ, организованы международные линии почтовой связи. Первый опыт организации перехвата иностранных сообщений.

КОНЕЦ XVII ВЕКА — 1725 ГОД

ПЕТРОВСКАЯ ЭПОХА

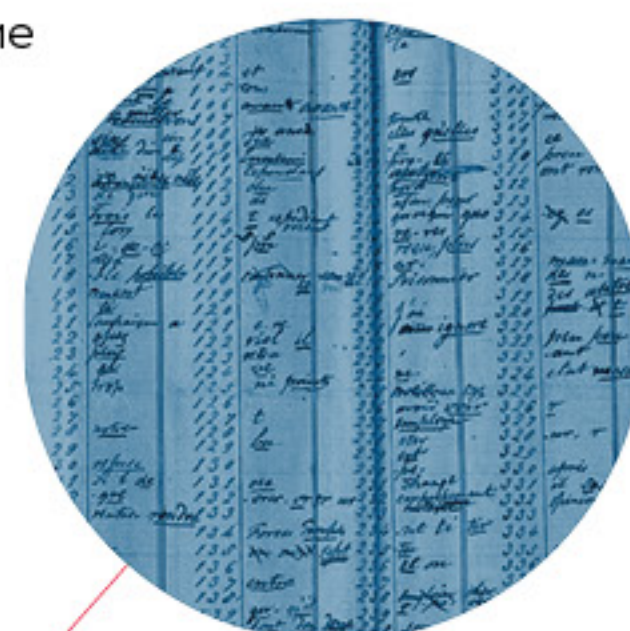
Появление шифров разнозначной и пропорциональной замены, простейших номенклаторов (номенклатор — шифрсистема, объединяющая кодовую книгу и шифр замены), первое упоминание о криптоанализе, реформа криптографической службы. Активное использование криптографических методов защиты информации для защиты не только дипломатической, но и военной и внутриаппаратной информации.



1725 ГОД — 30-Е ГОДЫ XIX ВЕКА

РАЗВИТИЕ СИСТЕМ МНОГОАЛФАВИТНОЙ ЗАМЕНЫ

Широкое применение кодов и сложных номенклаторов. Введение «генеральной цифири». Появление «черного кабинета» — дешифровальной службы. Активное чтение иностранной шифрпереписки. Вскрытие шифров Наполеона и его генералов во время Отечественной войны 1812 года.



1700

1725

1830

30-Е ГОДЫ XIX ВЕКА — 1917 ГОД

ПОЯВЛЕНИЕ НОВЫХ СРЕДСТВ СВЯЗИ

Появление профессии шифровальщика, разработка новых шифров, массовое использование шифровальных приборов, внедрение новых способов перехвата. Образование шифровальных служб в МВД и военном ведомстве. Активная криптографическая деятельность революционеров и борьба с ними правоохранительных органов, появление дешифровальной службы в МВД.





КОНЕЦ 1920-Х ГГ. — 1941 ГОД

НАЧАЛО ЭПОХИ «МАШИННОГО ШИФРОВАНИЯ»

Боевое крещение советских дешифровальщиков в Испании, работа в Китае, Монголии (Халхин-Гол), во время советско-финской войны.



1989 ГОД — НАСТОЯЩЕЕ ВРЕМЯ КРИПТОГРАФИЧЕСКАЯ ДЕЯТЕЛЬНОСТЬ ПЕРЕСТАЕТ БЫТЬ МОНОПОЛИЕЙ ГОСУДАРСТВА

В 1989 году впервые в СССР открыто опубликован криптографический алгоритм — государственный стандарт ГОСТ 28147-89. В 1994 году принимаются еще два криптографических стандарта: алгоритм цифровой подписи ГОСТ Р 34.10-94 (в 2001 году вместо него появляется новый алгоритм цифровой подписи ГОСТ Р 34.10-2001) и хэш-функция ГОСТ Р 34.11-94. Криптографическая деятельность перестает быть монополией государства, с начала 1990-х годов на территории России ее начинают осуществлять коммерческие структуры, финансовые организации и частные лица. Появляются частные фирмы-производители шифровального оборудования, других средств защиты информации, а также специализирующиеся на оказании услуг в области защиты информации. Для регламентации криптографической деятельности, а также введения определенных ограничений на отдельные ее виды для негосударственных организаций принимается ряд законодательных и других нормативных актов (например, Закон РФ «Об информации, информатизации и защите информации»). Нормативно-правовая база в области защиты информации продолжает совершенствоваться и в настоящее время.



1917

1930

1941

1945

1989

2018

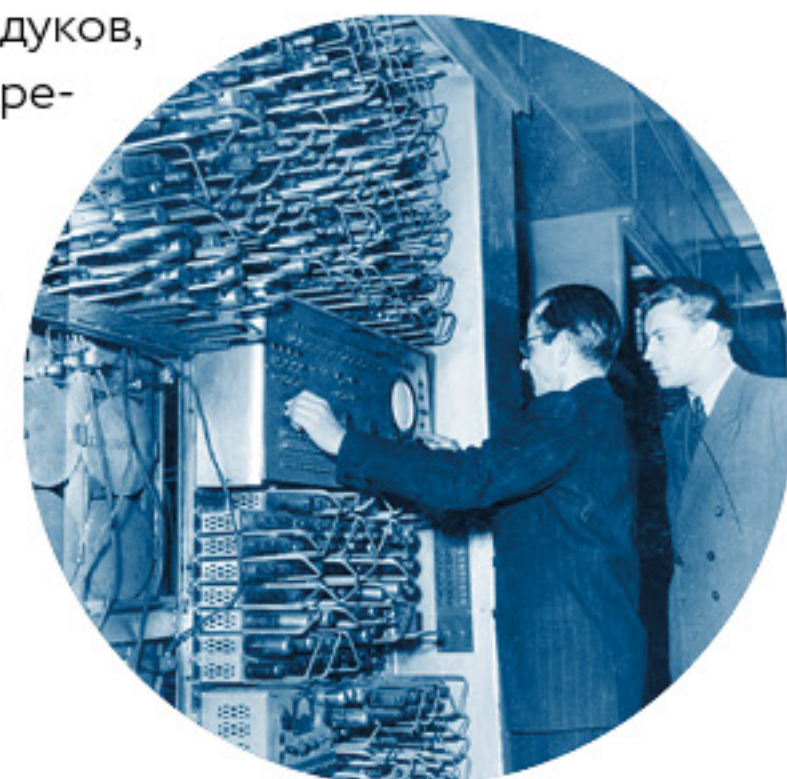


1917 ГОД — КОНЕЦ 1920-Х ГГ. КОРЕННАЯ РЕОРГАНИЗАЦИЯ СИСТЕМЫ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

В том числе и реорганизация криптографических служб после революции 1917 года. Создание советской криптографической службы — Спецотдела при ВЧК 5 мая 1921 года.

ВТОРАЯ ПОЛОВИНА 1940-Х ГОДОВ — 1989 ГОД ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫЕ МАШИНЫ

Во второй половине 1950-х годов при осуществлении криптографической деятельности в СССР начинают активно применяться электронно-вычислительные машины (ЭВМ), поступают новые образцы шифровальной техники различного назначения, создаются шифрмашины нового поколения — электронные шифраторы с использованием интегральных микросхем. [Астрахан, 1996], [Дадуков, 2006-1], [Кузьмин, 1998-2]. Развивается и укрепляется отечественная радиоэлектронная разведка, «она в 50-е — первой половине 80-х годов прошлого столетия организационно и технически превратилась из фронтовой в стратегическую» [Бурнусов, 2009]. Криптографическая деятельность в этот период является исключительной прерогативой государства.



ЧАСТЬ 1

ИСТОКИ



В IX веке в результате объединения новгородских и киевских земель образовалось единое русское государство — Киевская Русь. Эффективное управление весьма обширной территорией было невозможно без организации надежной связи между столицей в Киеве с подчиненными территориями и войсками, несущими сторожевую службу на границах Руси, а также находящимися в походе. Основным средством связи в то время были специальные княжеские гонцы — «люди пешие и конные» и «верные головы» (люди из княжеской дружины), которые со скоростью 200 и более верст в сутки передвигались от одного пункта до

другого, передавая как устные, так и письменные сообщения» [Астрахан, 1996, с. 10]. Использовались и другие способы связи: оптическая сигнализация с помощью костров и дымов, почтовые голуби, на поле боя управление осуществлялось с помощью сигнальных труб и свистков [Астрахан, 1996], [История, 1984], [Кудрявцев, 2002].

ОТ ПОВОЗА...

Расширение территории древнерусского государства, а также развитие системы государственного управления требовали совершенствования системы связи. В 920 году повелением киевского князя был учрежден своеобразный про-

образ современной почты — повоз. «Повозная повинность обязывала весь люд (кроме духовенства и бояр) по первому требованию княжеских людей (и в первую очередь гонцов) предоставлять им безвозмездно лошадей, корм, повозки и даже лодки с гребцами, что способствовало ускорению передачи государственных и ратных вестей» [Астрахан, 1996, с. 11]. Вообще следует отметить, что первая треть XII века стала для Руси периодом наивысшего расцвета политической и военной мощи государства, экономики, науки и культуры.

...К ЯМСКОЙ ГОНЬБЕ

К сожалению, в XII веке на Руси наступил период феодальной раздробленно-

ОДНАКО СКОРОСТЬ ПЕРЕДАЧИ ГОСУДАРСТВЕННОЙ И ВОЕННОЙ ИНФОРМАЦИИ БЫЛА МЕДЛЕННОЙ. ТРЕБОВАЛАСЬ ПОСТОЯННАЯ, НАДЕЖНАЯ, БОЛЕЕ БЫСТРОДЕЙСТВУЮЩАЯ СВЯЗЬ

сти. Отдельные княжества фактически превратились в независимые государства, которые проводили самостоятельную внешнюю и оборонную политику. Дипломатическая деятельность стала включать не только сношения с зарубежными государствами, но и отношения с соседними русскими княжествами. В каждом княжестве создавался свой государственный аппарат. Появлялись люди и службы, отвечающие за княжеский двор, хозяйство, финансы, суд, войско и т.п. В крупных княжествах (Киевское, Новгородское, Владимирское и др.) появились собственные дипломатические «службы», при князьях состоял целый штат переводчиков, которых тогда называли толмачами, и дипломатов, способных отстаивать интересы своих земель при осуществлении посольств и приема иноземных делегаций у себя, имелась также и служба разведки. Система связи была хорошо поставлена во многих княжествах, что позволяло уже во время выдвижения противника к границам княжества готовить войска к отражению нападения. Однако скорость передачи государственной и военной информации была медленной. Требовалась постоянная, надежная, более быстродействующая связь [Астрахан, 1996], [Кудрявцев, 2002].

В начале XIII века на смену повозу пришла ямская гоньба, которая представляла собой конную эстафету и была организована в каждом княжестве. В результате договоренностей между князьями ямская гоньба обеспечивала связь на территории всей Руси. В начальный период монголо-татарского нашествия этот способ связи использовался для координации действий русских князей. К сожалению, вскоре большая часть русских земель оказалась под монголо-татарским игом, которое за-

держало политическое, экономическое и культурное развитие Руси на столетия [Астрахан, 1996].

ТАРАБАРЩИНА

Для обеспечения конфиденциальности передаваемой информации использовались различные методы. Наиболее важные сообщения заучивались гонцом наизусть. При этом часто использовались намеки, иносказания условные слова. Суть данного метода заключается в том, что смысл передаваемого сообщения мог понять только посвященный человек. Впоследствии в криптографии такой способ обеспечения секретности получил название «жаргонного кода» и применяется до сих пор. Так, например, на жаргоне многих разведок слово БОЛЕТЬ означает «арест» или «заключение под стражу»; БОЛЬНИЦА — тюрьма; ДОКТОР — контрразведка. Тогда сообщение «Майкл арестован контрразведкой. Ему грозит заключение в тюрьму», принимает следующий «невинный» вид: Майкл заболел. Вчера был доктор и посоветовал ему лечиться в больнице» [Гольев, 2008], [Полмар, 1999].

Использовался и так называемый «тарабарский язык»¹, когда в устное сообщение вставлялись частицы-паразиты. Например, фраза «возьми суму» звучала так: «тараВОбараЗЬМИтараСУбараМУ». Причем фраза произносилась как можно быстрее, человеку непривычному к такому способу общения понять смысл сказанного было крайне затруднительно. Подобные способы защиты информации с древних времен были распространены не только у государственных служб, но и среди пред-

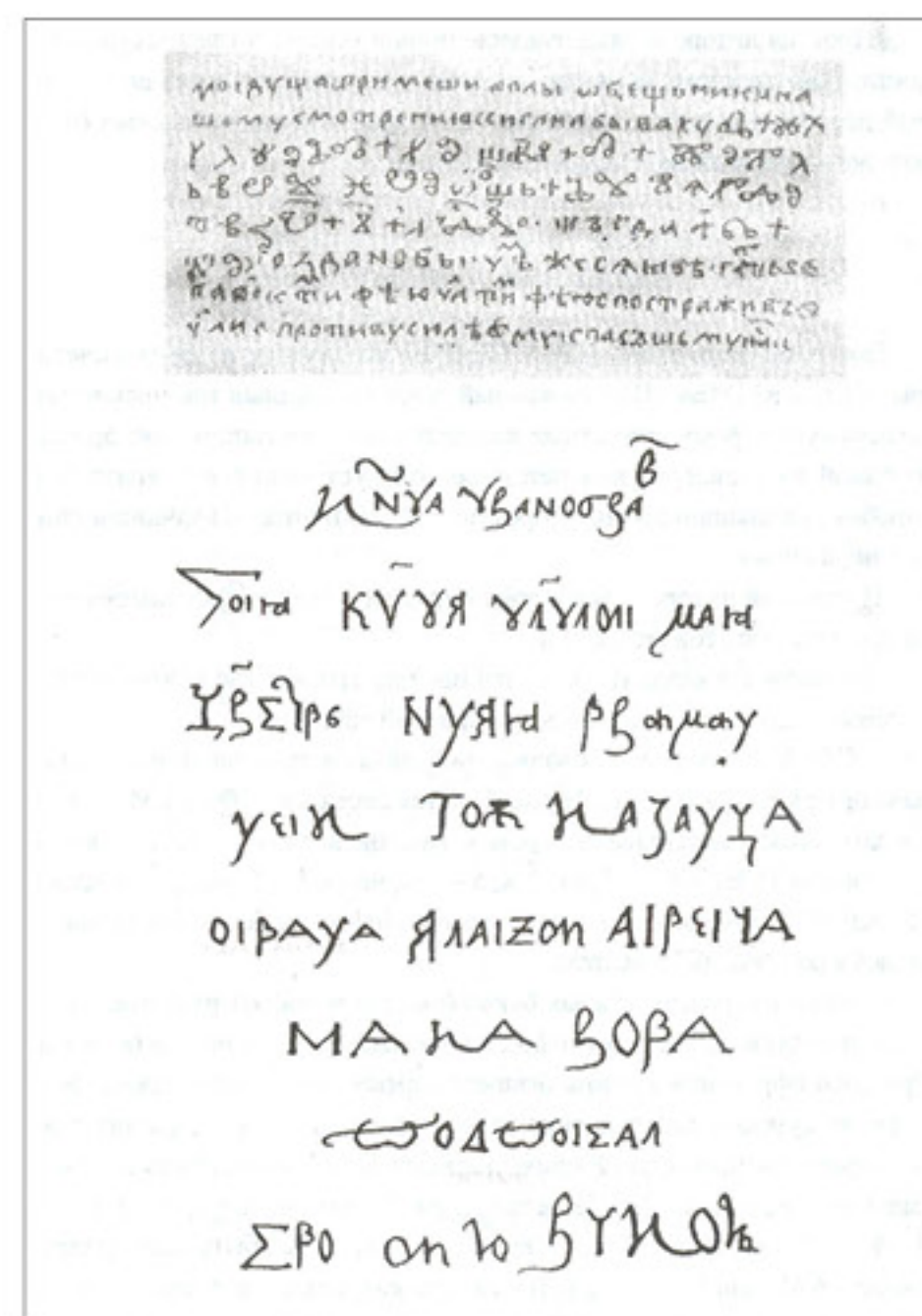


Рисунок 1. Глаголица

ставителей криминального мира в различных странах, в том числе и в России.

Для защиты письменных сообщений использовалась физическая защита, стеганография и шифрование. В качестве гонцов использовались физически крепкие люди, они были хорошо вооружены, нередко гонец следовал в сопровождении охраны. Сами письма скручивались в свитки, которые опечатывались специальными печатями, на которых была надпись «ДЬНЕСЛОВО», что переводится как «скрытое, тайное слово». Такие печати были у многих русских князей, в том числе и у Александра Невского [Соболева, 2002, с. 43].

Стеганографический метод заключался в запрытывании сообщений, депеши зашивались в одежду, помещались в подошвы и каблуки обуви и т.д. Об этом, в частности, говорилось в одной из древних новгородских грамот «...человиком грамотку пришли тайно...» [Бабаш, 2002, с. 207].

«ИНЬЕ ПИСЬМЕНА»

Шифрование. К сожалению, шифрованные документы, относящиеся к эпохе Древней Руси и содержащие информацию государственного характера, пока не обнаружены. Однако сохранился ряд памятников русской письменности, в которых имеются зашифрованные фрагменты. В основном это летописи и тексты религиозного содер-

¹ Интересно отметить, что зашифрованные записи в Древней Руси называли «тарабарской грамотой»

Русские буквы.	Пермские письма.	Русские буквы.	Пермские письма.
А	Ɑ Ɱ Ɐ Ɒ	О	Ɱ Ɐ [Ɒ]
Б	ⱱ Ⱳ ⱳ ⱴ	П	Ⱶ ⱶ ⱷ ⱸ
Г	ⱹ ⱺ ⱻ ⱼ	Р	ⱽ Ȿ Ɀ Ɀ[Ɀ]
Д	ⱽ Ȿ Ɀ Ɀ	С	Ɀ Ɀ Ɀ Ɀ
Е	Ɀ Ɀ Ɀ Ɀ	Т	Ɀ Ɀ Ɀ Ɀ
Ж	Ɀ Ɀ Ɀ Ɀ	У, В	Ɀ Ɀ Ɀ Ɀ
ДЖ	Ɀ Ɀ Ɀ Ɀ	Ц	Ɀ Ɀ
З	Ɀ Ɀ Ɀ Ɀ	Ч	Ɀ Ɀ Ɀ Ɀ
ДЗ	Ɀ Ɀ Ɀ Ɀ	Ш	Ɀ Ɀ Ɀ Ɀ
И	Ɀ Ɀ Ɀ Ɀ	Ы	Ɀ Ɀ Ɀ Ɀ
К	Ɀ Ɀ Ɀ Ɀ	Ю	Ɀ Ɀ Ɀ Ɀ
Л	Ɀ Ɀ Ɀ Ɀ	Ю	Ɀ Ɀ Ɀ Ɀ
М	Ɀ Ɀ Ɀ Ɀ	О	Ɀ Ɀ Ɀ Ɀ
Н	Ɀ Ɀ Ɀ Ɀ	Я	Ɀ

Рисунок 2. Пермские письма

жания. В этих источниках тайнопись применяется не столько для обеспечения секретности, сколько для того, чтобы подчеркнуть важность того или иного фрагмента, а также увековечить имя автора или переписчика. Именно эти документы дают возможность описать древнерусские системы шифрования.

С древних времен до конца XVII века основным средством шифрования на Руси были различные варианты шифра простой замены (получившие название «иные письма»). Буквы открытого текста заменялись на знаки малоиспользуемых алфавитов (глаголица, пермская азбука) или чаще на специально придуманные знаки (рис. 1, 2, 3).

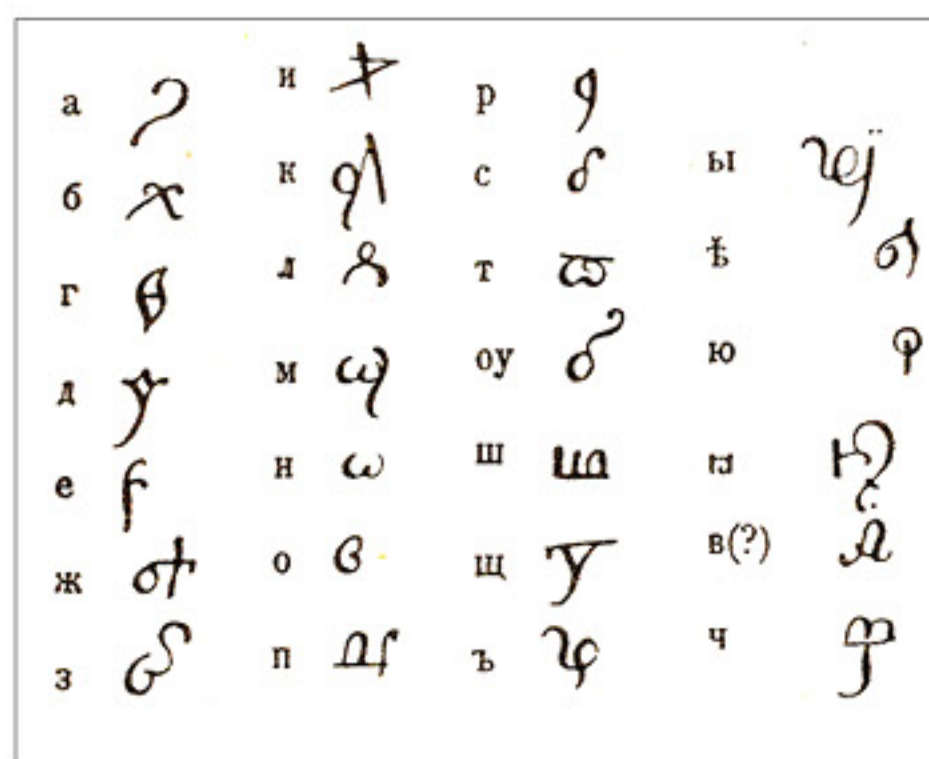


Рисунок 3. Пример простой замены

Обеспечение секретности было необходимо для следующих видов сообщений.

Информация, необходимая для организации государственного управления. Княжеские указы и распоряжения, отчеты с мест и т.п. В процессе становления русской государственности система управления постоянно совершенствовалась. Киевскому князю подчинялись другие князья (в современном понимании — руководители регионов). Создавались различные службы, регулировавшие разные области человеческой деятельности (торговлю, ремесла, сбор налогов и податей и т.п.). Разумеется, в рамках деятельности по управлению государством постоянно возникает необходимость передачи секретной, тайной информации, и наиболее эффективными методами защиты правительственной информации являются криптографические.

Военная информация. В первую очередь передача «ратной вести, сво-

временном уведомлении о появлении неприятеля, проведении сборов войск» [Астрахан, 1996, с. 10], а также организация управления войсками во время боевых действий и в мирное время.

Дипломатическая информация. После становления древнерусского государства происходило налаживание связей с другими странами, в первую очередь, с соседями. Основным внешнеполитическим партнером древней Руси была Византия (хотя при этом русские князья неоднократно воевали с этим государством), дипломатические отношения периодически поддерживались также с рядом стран Европы, Хазарией и викингами.

В процессе становления и развития русского государства в IX–XVI веках криптографическая деятельность играла весьма важную роль в организации системы государственного управления, передачи военной, дипломатической и разведывательной информации. Главным достижением данного периода является создание на Руси достаточно надежной и эффективной системы связи — повоза, а впоследствии ямской гоньбы. Можно сделать однозначный вывод, что ямская гоньба сыграла существенную роль в процессе преодоления феодальной раздробленности на Руси и создания Московского государства. Она была одним из ведущих средств государственного управления.

ЛИТЕРАТУРА

- [Андреев, 1998] Андреев Н. Н. «Россия остается в числе лидеров мировой криптографии». Защита информации. Конфидент, 1998, № 5, с. 12–17.
- [Астрахан, 1996] Астрахан В. И., Гусев В. В., Павлов В. В., Чернявский Б. Г. Становление и развитие правительственной связи в России, Орел: ВИПС, 1996.
- [Астрахан, 2001] Астрахан В. И., Павлов В. В., Чернега В. Г., Чернявский Б. Г. Правительственная электросвязь в истории России. Часть I (1917–1945). М., Наука, 2001.
- [Гольев, 2008–1] Гольев Ю. И., Ларин Д. А., Тришин А. Е., Шанкин Г. П. Криптография: страницы истории тайных операций. М.: Гелиос АРВ, 2008.
- [История, 1984] История военной связи. Под общей редакцией А. И. Белова. М.: Воениздат, 1984.
- [Кан, 2004] Кан Д. Война кодов и шифров. М.: РИПОЛ КЛАССИК, 2004.
- [Кудрявцев, 2002] Кудрявцев Н. А. Государево Око. Тайная дипломатия и разведка на службе России. М., ОЛМА-ПРЕСС, 2002.
- [Очерки, 1996–2006] Очерки истории российской внешней разведки в 6 томах, под ред. Е. М. Примакова и С. Н. Лебедева, М., «Международные отношения», 1996–1999. Второе издание: История российской внешней разведки в 6 томах. М., «Международные отношения», 2014.
- [Соболева, 2002] Соболева Т. А. История шифровального дела в России. М.: ОЛМА-ПРЕСС-Образование, 2002.



Борис СТОЛПАКОВ
историк криптографии,
кандидат физико-
математических наук

«МИР НИКОГДА НЕ УЗНАЕТ, ЧТО МЫ СДЕЛАЛИ С НИМИ»

ЕКАТЕРИНБУРГСКАЯ ТРАГЕДИЯ

17.07.1918: КРИПТОГРАФИЧЕСКИЙ КЛЮЧ
К РАССЛЕДОВАНИЮ



Дом Ипатьева в Екатеринбурге, в подвале которого была расстреляна Царская семья

Сто лет назад, в ночь на 17 июля 1918 года в Екатеринбурге свершилось убийство Царской семьи и их верных слуг, а спустя сутки в полутора сотнях километров от Екатеринбурга, в окрестностях Алапаевска, в заброшенной шахте были заживо погребены великая княгиня Елизавета Фёдоровна и другие представители династии Романовых.

Подробности этих злодеяний стали широко известны после опубликования материалов расследования следователя Н. А. Соколова. Книга

«Убийство Царской Семьи. Из записок судебного следователя Н. А. Соколова» вышла в свет в 1925 году в Берлине, уже после безвременной смерти Соколова.

Опираясь на материалы следствия, Соколов указал на Свердлова и Голощёкина как на главных соучастников убийства.

Как известно, центральное место в обосновании такой позиции принадлежит зашифрованной телеграмме, переданной из Екатеринбурга в Москву 17 июля 1918 года (илл. 2). Ныне эта



Иллюстрация 1. Судебный следователь по особо важным делам Омского окружного суда Н. А. Соколов.

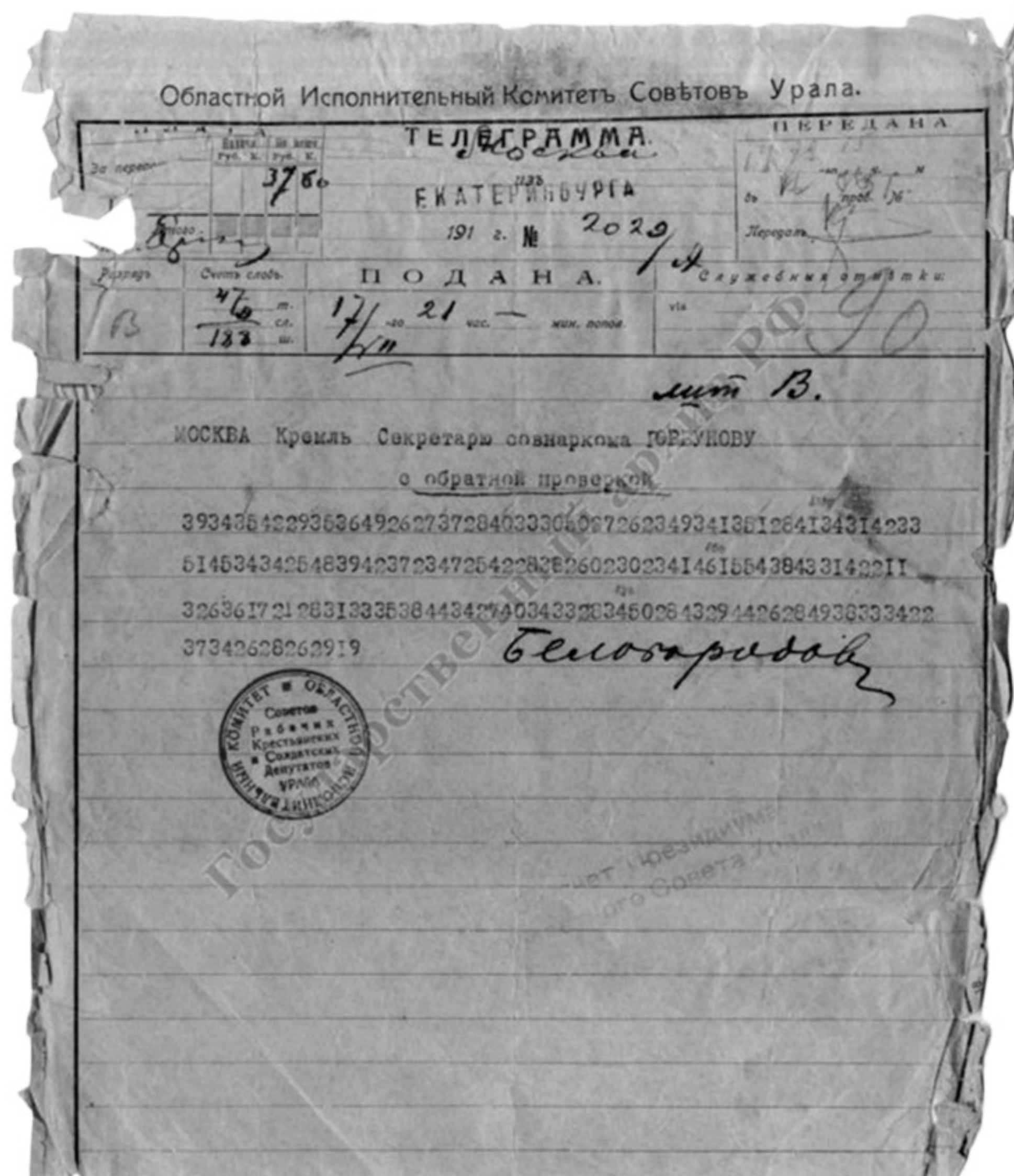


Иллюстрация 2. Телеграмма, переданная из Екатеринбурга 17 июля 1918 года

телеграмма хранится в Государственном архиве РФ. Вот что сообщил о ней следователь.

«Скажу о ней более подробно. Она сразу приковала к себе мое внимание и отняла у меня много времени и хлопот... 24 февраля (1919 года — авт.) я передал ее содержанию опытному лицу при Штабе Верховного Главнокомандующего, 28 февраля — в Министерство Иностранных Дел, позднее — Главнокомандующему союзными войсками генералу Жанену. Результаты были плачевны. В Европе мне удалось найти то русское лицо, о котором всегда было известно как о человеке совершенно исключительных способностей и опыта в этой области. 25 августа 1920 года он получил содержание телеграммы. 15 сентября того же года я имел ее у себя расшифрованной.

Все люди обывательской среды, незнакомые с техникой следственного дела, обычно рассуждают по одному шаблону: всякое, самое простое преступление им кажется чрезвычайно загадочным, пока оно не вскрыто, и каждое самое загадочное преступление им ка-

жется чрезвычайно простым, когда оно вскрыто. Обычно и встречаешься всегда с рассуждениями: как преступники могли оставить неуничтоженным такой ценный предмет? Достоверно ли это?

Большевики — люди, и, как все люди, они подвержены всем людским слабостям и ошибкам. Я им отдаю должное. Они совершили преступление, особенно вторую его часть, уничтожение трупов, так тщательно, как могли.

Они лгали, отдаю им должное, умело. Но они иногда переоценивали самих себя и свою осторожность. Комиссар Войков, снабжавший рудник серной кислотой, всегда отличался склонностью к театральным жестам, глупостью и излишней болтовней, особенно в дамском обществе. Его там однажды спросили о судьбе царской семьи. Он напыщенно ответил: «Мир никогда не узнает, что мы сделали с ними».

В нашем следственном деле нет чудес. Терпением и энергией подходим мы к истине. 25 августа 1920 года мне была абсолютно ясна идея большевистской лжи: «Мы расстреляли только Царя, но не семью». Они надели на себя революционную личину и подсовывали под преступление моральный принцип. Этим принципом они оправдывали убийство Царя. Но какая мораль может оправдать убийство детей? Им оставалось только одно средство: лгать, и они лгали. Но они лгали для мира. Для себя и между собой они должны были говорить правдиво. В содержание этой правды не могло не войти, должно было войти слово «семья». В числе других, оно было дано мною 25 августа 1920 года. Специалист-техник с колоссальным опытом и из ряда вон выдающимися способностями раскрыл смысл таинственной телеграммы».

«В ЕВРОПЕ МНЕ УДАЛОСЬ НАЙТИ ТО РУССКОЕ ЛИЦО, О КОТОРОМ ВСЕГДА БЫЛО ИЗВЕСТНО КАК О ЧЕЛОВЕКЕ СОВЕРШЕННО ИСКЛЮЧИТЕЛЬНЫХ СПОСОБНОСТЕЙ И ОПЫТА. 25 АВГУСТА ОН ПОЛУЧИЛ СОДЕРЖАНИЕ ТЕЛЕГРАММЫ. 15 СЕНТЯБРЯ Я ИМЕЛ ЕЕ У СЕБЯ РАСШИФРОВАННОЙ»

Далее Соколов сообщил некоторые подробности о способе расшифровки телеграммы, прежде всего о ключе шифра. Ключом является слово «ЕКАТЕРИНБУРГ», имеющее 12 букв. Телеграмма расшифровывается следующим образом. Весь зашифрованный текст делим на участки по двенадцать двузначных групп. Затем последовательно записываем их как строки таблицы из 12 колонок, располагая один под другим. Тогда зашифрованный текст принимает вид, указанный в табл. 1.

Для расшифрования используем шифровальную таблицу, приведённую на илл. 2. Каждый из 12 столбцов зашифрованного текста расшифруем с помощью столбца шифровальной таблицы с тем же номером: двузначные группы первого столбца зашифрованного текста посредством первого столбца шифровальной таблицы, группы второго столбца посредством второго столбца и т.д. Вот с сохранением орфографии содержание телеграммы: «Передайте Свердлову что все семейство постигла та же участь что и главу официально семья погибнет при эвакуации».

Всего в распоряжении следствия оказалось 65 подлинных шифрованных телеграмм, захваченных в Екатеринбурге, в том числе и другие телеграммы, зашифрованные тем же самым ключом.

На основе результатов следствия, Соколов выдвинул тезис: «Судьба Царской семьи была решена не в Екатеринбурге, а в Москве». В подтверждение его справедливости следователь предложил следующую цепь доводов. Проследим её кратко.

«Когда Юровский внедрился в дом Ипатьева, Голощекин отсутствовал из Екатеринбурга. Он в это время находился в Москве и жил на квартире у Свердлова. Но Белобородов в тот же день сообщил ему телеграфно о происшедшей в доме Ипатьева перемене:

**Председателю ЦИК Свердлову
для Голощекина**

Авдеев сменен его помощник Мошкин арестован вместо Авдеева Юровский внутренний караул весь сменен заменяется другим точкой.

4 июля 1918 г. Белобородов»

1	2	3	4	5	6	7	8	9	10	11	12
39	34	35	42	29	35	36	49	26	27	37	28
40	33	30	50	27	26	23	49	34	13	51	28
41	34	31	42	33	51	45	34	34	25	48	39
42	37	23	47	25	42	28	38	26	02	30	23
41	46	15	54	38	43	31	42	21	13	26	36
17	21	28	31	33	35	38	44	34	27	40	34
33	28	34	50	28	43	29	44	26	28	49	38
33	34	22	37	34	26	28	26	29	19		

Таблица 1. Зашифрованный текст

	1	2	3	4	5	6	7	8	9	10	11	12
У-	16	20	11	28	16	26	19	23	12	02	26	14
Ф-	17	21	12	29	17	27	20	24	13	03	27	15
Х-	18	22	13	30	18	28	21	25	14	04	28	16
Ц-	19	23	14	31	19	29	22	26	15	05	29	17
Ч-	20	24	15	32	20	30	23	27	16	06	30	18
Ш-	21	25	16	33	21	31	24	28	17	07	31	19
Щ-	22	26	17	34	22	32	25	29	18	08	32	20
Ю-	23	27	18	35	23	33	26	30	19	09	33	21
Я-	24	28	19	36	24	34	27	31	20	10	34	22
А-	25	29	20	37	25	35	28	32	21	11	35	23
Б-	26	30	21	38	26	36	29	33	22	12	36	24
В-	27	31	22	39	27	37	30	34	23	13	37	25
Г-	28	32	23	40	28	38	31	35	24	14	38	26
Д-	29	33	24	41	29	39	32	36	25	15	39	27
Е-	30	34	25	42	30	40	33	37	26	16	40	28
Ж-	31	35	26	43	31	41	34	38	27	17	41	29
З-	32	36	27	44	32	42	35	39	28	18	42	30
И-	33	37	28	45	33	43	36	40	29	19	43	31
К-	34	38	29	46	34	44	37	41	30	20	44	32
Л-	35	39	30	47	35	45	38	42	31	21	45	33
М-	36	40	31	48	36	46	39	43	32	22	46	34
Н-	37	41	32	49	37	47	40	44	33	23	47	35
О-	38	42	33	50	38	48	41	45	34	24	48	36
П-	39	43	34	51	39	49	42	46	35	25	49	37
Р-	40	44	35	52	40	50	43	47	36	26	50	38
С-	41	45	36	53	41	51	44	48	37	27	51	39
Т-	42	46	37	54	42	52	45	49	38	28	52	40

Таблица 2. Шифровальная таблица



Иллюстрация 3. Царская семья в 1913 году

«21 июля официальное большевистское «Бюро Печати» отправило из Москвы в Екатеринбург областному совету телеграмму № 6153. Она датирована 19 июля. Вот ее содержание:

19 июля.

Состоявшемся 18 июля первом заседании президиума ЦИК советов Председатель Свердлов сообщает полученное прямому проводу сообщение от областного Уральского совета расстреле бывшего царя Николая Романова точка Последние дни столице красного Урала Екатеринбург угрожала опасность приближения чехословацких банд точка То же время был раскрыт новый заговор контрреволюционеров имеющий целью вы-

рвать рук Советвласти коронованного палача точка Ввиду всех этих обстоятельств президиум Уральского областного совета постановил расстрелять Николая Романова что было приведено в исполнение 16 июля точка Жена сын Николая отправлены надежное место точка Документы раскрытом заговоре посланы Москву специальным курьером точка Сделав это сообщение Свердлов напоминает историю перевода Романова из Тобольска Екатеринбург когда была раскрыта такая же организация белогвардейцев целях устройства побега Романова точка Последнее время предполагалось предать бывшего царя суду все его преступления против народа только развернувшиеся сейчас события помешали

осуществлению этого суда точка Президиум обсудив все обстоятельства заставившие Уральский областной совет принять решение расстреле Романова постановил ЦИК лице своего президиума признать решение Уральского областного совета правильным точка Затем председатель сообщает что распоряжении ЦИК находятся сейчас важный материал документы Николая Романова его собственноручные дневники которые он вел последнего времени дневники его жены детей переписка Романова точка Имеются между прочим письма Григория Распутина Романову его семье точка Все эти материалы будут разобраны опубликованы ближайшее время точка продолжение следует».



Иллюстрация 4. Подвал дома Ипатьева в Екатеринбурге, где была расстреляна царская семья

Итак, 18 июля 1918 года в Москве Свердлов первый сообщил в присутствии президиума ЦИКа о судьбе царской семьи. 19 июля в Москве появились об этом печатные сообщения. Та же самая картина и в Екатеринбурге. 20 июля здесь Голощекин первый сообщил в присутствии президиума областного совета о судьбе царской семьи. 21 июля в городе были расклеены в разных местах печатные об этом сообщения. Основная идея и Москвы, и Екатеринбурга была одна и та же: Царь «казнен по воле народа», жизнь семьи сохранена. Свердлов и Голощекин лгали одинаково...

Почему Москва первая сообщила о смерти Царя, а Екатеринбург, где он был убит, сообщил об этом только через два дня? Большевики... оставили на телеграфе и свои подлинные телеграммы, и свои подлинные телеграфные ленты. Одна из них содержит переговоры Свердлова, которые он вел 20 июля 1918 года из Москвы с неуказанным в ленте лицом из Екатеринбурга. В ней на вопрос Свердлова: «Что у вас слышно?» — неизвестный отвечает:

«Положение на фронте несколько лучше, чем казалось вчера. Выясняется, что противник оголил все фронты и бросил все силы на Екатеринбург; удержим ли долго Екатеринбург, трудно

сказать. Принимаем все меры к удержанию. Все лишнее из Екатеринбурга эвакуировалось. Вчера выехал к вам курьер с интересующими вас документами. Сообщите решение ЦИК, и можем ли мы оповестить население известным вам текстом?»

Свердлов отвечает:

«В заседании президиума ЦИК от 18-го постановлено признать решение Ур. Обл. Совдепа правильным. Можете публиковать свой текст. У нас вчера во всех газетах было помещено соответствующее сообщение. Сейчас послал за точным текстом и передам его тебе...».

Дальше идет текст большевистской телеграммы «Бюро Печати» за № 6153. Запись вскрывает причину, почему о смерти Царя Москва заговорила раньше Екатеринбурга: Екатеринбург не смел сам говорить об этом без разрешения Москвы. Как же он сам мог осмелиться убить, когда без позволения Москвы он не смел даже сказать об этом?

Кто говорил со Свердловым? Этот человек знает состояние фронта. Голощекин знал фронт, так как он был областной «военный» комиссар. Бурцев (разоблачитель руководителя боевиков-эсеров Азефа, как полицейского агента — авт.) показывает: «И Свердлова, и Голощекина я знаю лично. Между собою они „на ты“».

18 июля Свердлов сказал, что из Екатеринбурга выслан в Москву специальный курьер с документами о раскрытом заговоре контрреволюционеров, намеревавшихся спасти Императора, и что в распоряжении ЦИКа уже имеются дневники и письма царской семьи. Документы о заговоре никогда не отправлялись к Свердлову из Екатеринбурга по той причине, что такого заговора не существовало. Дневники же и письма царской семьи были действительно доставлены к Свердлову, но 18 июля он их у себя не имел и никак иметь не мог. Дневники и письма царской семьи были при ней в доме Ипатьева. Эти письма взяли у Царя, перешагнув через его труп. Убийство случилось в ночь на 17 июля. 18 июля Свердлов не мог иметь у себя ни дневников, ни писем царской семьи. Чтобы это понять, надо только посмотреть на географическую карту России: там обозначено, сколько верст от Екатеринбурга до Москвы. Эти весьма ценные предметы были отправлены к Свердлову с особым курьером. Им был Юровский, выехавший с ними из Екатеринбурга 19 июля. Его отвозил на вокзал из дома Ипатьева кучер Елькин. Он так описывает отъезд Юровского: «В последний раз я подал Юровскому лошадь 19 июля к дому Ипатьева. Из дому вышли молодые люди и с помощью старшего красноармейца вынесли и положили ко мне в экипаж семь мест багажа; на одном из них, представлявшем из себя средних размеров чемодан черной кожи, была сургучная печать».

* * *

Что же означает ложь Свердлова? Между 4 и 14 июля, когда Голощекин был в Москве и жил в квартире Свердлова, судьба царской семьи была решена. Свердлов тогда же приказал Голощекину доставить к нему после убийства семьи все интимные документы. Несомненно, было решено, что их доставит надежный специальный курьер. 18 июля Свердлов получил шифрованную телеграмму... и в радости сердца опрометчиво похвастал тем, чем еще не обладал. Этой своей оплошностью он сам определил свое место: самого главного среди других соучастников убийства.

СОВЕТСКИЙ КРИПТОГРАФ ИВАН ВЕРЧЕНКО



Дмитрий ЛАРИН
кандидат
технических наук,
ЗАО «Лаборатория
«СКАТ»

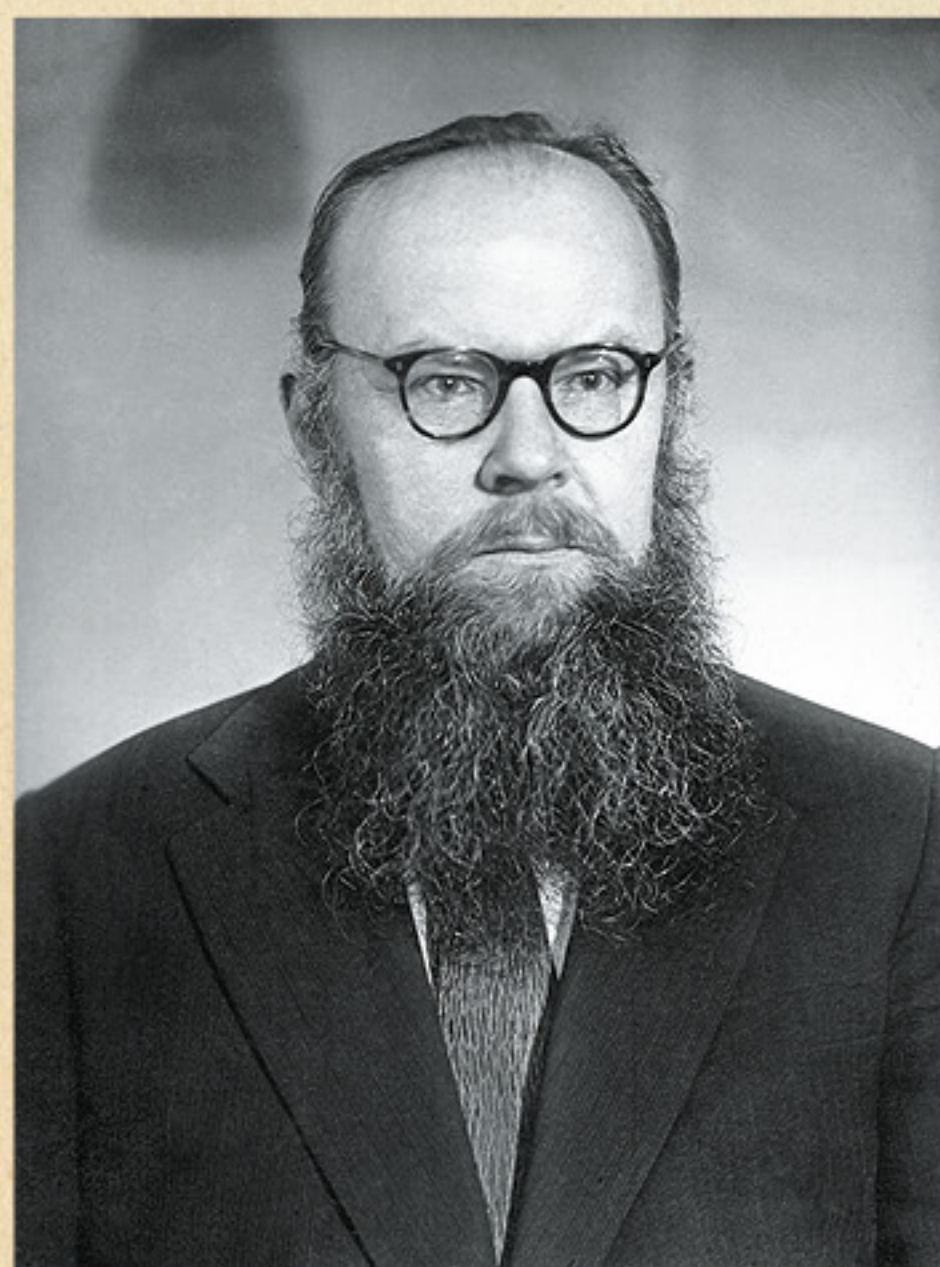


**Геннадий
ЕМЕЛЬЯНОВ**
член-корреспондент
Академии
криптографии РФ

В предыдущих номерах мы рассказали о криптографах В. С. Полине, Г. И. Пондопуло, М. И. Соколове, М. С. Одноробове и других, немало сделавших для реорганизации и развития советской криптографической службы во время Великой Отечественной войны и сразу после нее. В этом списке с полным правом находится и имя И. Я. Верченко, хотя во время войны его деятельность только начиналась, а ее расцвет приходится на более позднее время.

ИВАН ИЗ-ПОД ЛУГАНСКА

Иван Яковлевич Верченко родился 11 сентября 1907 г. в селе Ивановка Славяносербского уезда Екатеринославской губернии (позже Ворошиловградской, ныне Луганской области). Учился в трудовой школе, в 1922–



1925 гг. — в фабрично-заводском училище при Государственном Динамитном заводе в Донбассе. По окончании работал лаборантом химической лаборатории Динамитного завода. В 1926–1928 гг. — переписчик на Мариупольском заводе им. Ильича.

СТУДЕНТ И ПРЕПОДАВАТЕЛЬ В ОДНОМ ЛИЦЕ

В 1929 г. поступает в МГУ им. М. В. Ломоносова на механико-математический факультет. В период обучения одновременно работает два года преподавателем математики в Институте подготовки кадров для Красной Профессуры и один год техником в ЦАГИ. По окончании университета поступает в аспирантуру научно-исследовательского института математики при МГУ.

Будучи аспирантом, работает ассистентом на механико-математическом факультете МГУ, а также ведет серьезные научные исследования по теории функций под руководством профессора А. Н. Колмогорова. В 1937 году по окончании аспирантуры и защиты диссертации на ученую степень кандидата физико-математических наук направляется на работу в Ростовский-на-Дону Государственный Университет.

В 1941 г. в связи с эвакуацией вынужден оставить работу в университете и переехать в г. Баку. С ноября 1941 г. по ноябрь 1943 г. работает инженером-конструктором на заводе в Баку, а затем в Москве. В ноябре 1943 г. возвращается к научной работе, поступив в докторантуру Математического института им. В. А. Стеклова АН СССР. Будучи докторантом, также препода-

ет математику в Военной Академии им. И. В. Сталина и является доцентом Московского Механического Института. За время прохождения докторантуры получил ряд фундаментальных научных результатов по теории функций многих переменных и по математическому анализу, которые вошли в его докторскую диссертацию. Защита состоялась в 1949 г.

ПРИГЛАШЕНИЕ В МГБ

В 1947 г., в связи с усилением в стране работ по развитию систем закрытой связи и привлечением к этим работам высококвалифицированных специалистов в области математики, физики и техники, И. Я. Верченко приглашается на работу в органы МГБ СССР. В июле 1947 г. он зачислен в центральный аппарат Министерства сначала на должность старшего оперуполномоченного с присвоением воинского звания старшего лейтенанта, а затем на должность заместителя начальника 1 отделения 6 Управления МГБ СССР.

С учетом высокой квалификации специалиста-математика был направлен на наиболее важный и сложный участок исследовательской работы по дешифрованию машинных шифрсистем. За сравнительно короткий срок он в полной мере и научно глубоко воспринял криптографическое наследие дешифровальной службы и с пониманием дела взялся за разработку первоочередных проблем дешифрования машинных шифрсистем с привлечением математического аппарата. В июле 1949 г. Верченко присваивают звание капитана, а в августе того же года досрочно — звание майора.

Следует отметить, что после войны началась большая работа по реорганизации криптографической службы с целью вывести ее на более высокий научно-технический уровень. Так, 21 января 1948 г. в МГБ была создана так называемая Марфинская лаборатория для разработки аппаратуры засекречивания телефонных переговоров гарантированной стойкости. Предполагалось, что в ее работе наряду с опытными специалистами отдела правительственной связи и отдела оперативной техники МГБ будут использованы и заключенные [Калачев, 2000].

МАРФИНСКАЯ ЛАБОРАТОРИЯ

К концу 1948 г. в Марфинской лаборатории работало 490 человек, в том числе 280 заключенных. Вместе с тем в ней явно не хватало специалистов-криптографов, без которых трудно было решить вопросы стойкости разрабатываемой аппаратуры. В связи с этим руководитель лаборатории обратился к руководству МГБ с просьбой о временном прикомандировании к ним специалистов 6 Управления. Одним из таких прикомандированных оказался И. Я. Верченко.

Он был назначен руководителем созданной в 6 Управлении группы из 29 человек для анализа и экспертизы шифраторов, разрабатываемых в лаборатории. Группа работала в тесном контакте с инженерами-разработчиками лаборатории. В результате была решена сложнейшая научно-техническая проблема создания стойкой аппаратуры для засекречивания телефонных переговоров на линиях ВЧ-связи. 29 июля 1950 г. правительственная комиссия приняла опытные образцы, что стало значительным успехом отечественной криптографии.

В 1950 г. создается НИИ-1 ГУСС, и И. Я. Верченко назначается туда заместителем начальника по научной работе. В составе НИИ-1 предусма-

ПОСЛЕ ВОЙНЫ НАЧАЛАСЬ БОЛЬШАЯ РАБОТА ПО РЕОРГАНИЗАЦИИ КРИПТОГРАФИЧЕСКОЙ СЛУЖБЫ С ЦЕЛЬЮ ВЫВЕСТИ ЕЕ НА БОЛЕЕ ВЫСОКИЙ НАУЧНО-ТЕХНИЧЕСКИЙ УРОВЕНЬ

тривались ученый совет, аспирантура и специальная научно-техническая библиотека. Первый набор в аспирантуру состоялся в октябре 1955 г.

ПО УКАЗАНИЮ БЕРИИ

В 1953 г. после смерти И. В. Сталина началась новая реорганизация Специальной службы страны. ГУСС было упразднено, некоторые его подразделения переданы обратно в МГБ СССР. Функции НИИ-1 были переданы сначала 8 Управлению МВД СССР, а в 1954 г., в связи с образованием Комитета государственной безопасности при СМ СССР, — 8 Главному Управлению КГБ.

По словам самого И. Я. Верченко, он в апреле 1953 г. на одном из совещаний в присутствии Л. П. Берия послал в президиум записку по вопросу о существовании абсолютно стойких шифров. После этого по указанию Л. П. Берии он был освобожден от работы в органах госбезопасности в связи с переходом на педагогическую работу по специальности.

С 1953 г. работал профессором, а затем завкафедрой математического анализа в Московском Городском педагогическом институте им. В. П. Потемкина. В 1960 г. становится профессором кафедры математического анализа МГПИ им. В. И. Ленина. Работая в педагогических вузах, активно сочетает учебно-педагогическую практику с научной.

ВОЗВРАЩЕНИЕ В КГБ

В 1962 г. И. Я. Верченко при содействии Отдела науки ЦК КПСС удалось вер-

нуть на работу в органы КГБ — он был назначен на должность начальника кафедры высшей математики технического факультета Высшей школы КГБ, а в мае 1963 г. — на должность начальника технического факультета при условии совмещения с должностью начальника кафедры. Обе эти должности он занимал в течение последующих 10 лет.

В январе 1968 г. по представлению Высшей Школы КГБ и при поддержке МГУ им. М. В. Ломоносова и МГПИ им. В. И. Ленина он был избран членом-корреспондентом Академии педагогических наук СССР. В 1971 г. награжден Орденом Трудового Красного Знамени.

В январе 1972 г. И. Я. Верченко был уволен с должности начальника факультета, а в январе 1973 г. — с должности начальника кафедры высшей математики в связи с переходом на работу в Академию педагогических наук СССР. С 1972 г. по 1986 г. Иван Яковлевич работал заведующим кафедрой Высшей математики и читал лекции по математическому анализу в Московском институте электронного машиностроения. Частично в этот период, а также и после 1986 г. он читал лекции по математическому анализу и на родном ему техническом факультете Высшей Школы КГБ.

Иван Яковлевич Верченко скончался 15 ноября 1995 года [Код 2007].

ЛИТЕРАТУРА

- [Бутырский, 2012] Бутырский Л. С., Ларин Д. А., Шанкин Г. П. Криптографический фронт Великой Отечественной. Монография. М.: Гелиос АРВ, 2012. 2 изд. исправл. и дополн. М. 2013.
- [Калачев, 2000] Калачев Константин. В круге третьем. Воспоминания и размышления о работе Марфинской лаборатории в 1948–1951 годах. М.: Элиас рекордз, 2000.
- [Код 2007] Код Верченко. Документальный фильм. Производство ЗАО «Видео-пресс», 2007.
- [Кузьмин, 1998–1] Кузьмин Л. А. Не забывать своих героев // Защита информации. Конфидент № 1, 1998, с. 83–85.
- [Кузьмин, 1998–2] Кузьмин Л. А. ГУСС — этап в развитии советской криптографии // Защита информации. Конфидент. № 4, 1998, с. 89–94.
- [Кузьмин, 1999] Кузьмин Л. А. Становление кафедры криптографии // Защита информации. Конфидент. № 1–2, 1999, с. 85–90.
- [Энциклопедия, 2004] Энциклопедия секретных служб России. М.: Астрель, 2004.

КОМУ СУШИТЬ СУХАРИ?

ПРО БИЗНЕС БЕЗ БЕЗОПАСНИКОВ

Искусственный интеллект, аутсорсинг и классические поползновения ИТ на поляну ИБ регулярно смущают умы специалистов и руководителей по ИБ: а что если нас заменят? Предупрежден — значит, вооружен. Давайте проведем кабинетный эксперимент по замене службы ИБ на современные технологии. Задача проста — свести количество и качество безопасников в организации к минимуму. Благо, что бизнес будет только рад снять с себя лишнее бремя.

НОМЕНКЛАТУРА ФУНКЦИЙ СЛУЖБЫ ИБ

Перед началом анализа необходимо определиться с функциями службы ИБ. Для этого используем фундаментально свежий и полный NIST CyberSecurity Framework — руководство по информационной безопасности критической информационной инфраструктуры США (далее Руководство).

Руководство включает в себя 5 доменов, без каждого из которых мощную и адаптивную систему ИБ не построить:

- ◆ Идентификация
- ◆ Защита
- ◆ Мониторинг
- ◆ Реагирование
- ◆ Восстановление

ИДЕНТИФИКАЦИЯ

Домен включает в себя 5 организационных способностей (capabilities) — Управление активами, Анализ бизнес-среды, Корпоративное управление ИБ, Оценка рисков и Управление рисками.

Уже из названий организационных способностей специалисту понятно, что нейронная сеть тут не очень поможет, так как нужно договариваться с другими руководителями функций организации. Аутсорсинг возможен лишь частично — принятие управленческих решений невозможно отдать «наружу».

Да и ИТ будет покусаться на такую «поляну» осторожно — работа вроде «бумажная» (не очень почетная), а ответственности много.

ЗАЩИТА

Домен включает в себя 6 организационных способностей — Управление доступом, Повышение осведомленности, Защита данных, Процессы и политики ИБ, Безопасная поддержка и Защитные технологии.

Защита — домен для анализа более сложный, чем предыдущий. К примеру, Защитные технологии убедительно и почти повсеместно закрываются «облачными» и аутсорсинговыми подходами, а настройка любого ИТ-средства (в том числе средства защиты информации) с каждым годом становится все проще, иные производители встраивают элементы искусственного интеллекта даже для формирования подсказки, какой диапазон Wi-Fi сигнала выбрать администратору при установке или настройке Wi-Fi-точки.

Управление доступом и Повышение осведомленности в теории хорошо автоматизируются, но на практике их автоматизация приводит только к росту численности службы ИБ — это понятные бизнесу процессы, и они с каждым годом становятся все более крупными и развитыми. Защита данных как задача эффективно упрощается автоматизацией (к примеру, автоматической классификацией чувствительной информации), а вот Безопасная поддержка и Политики и процедуры аналогичны домену Идентификация — автоматизировать сложно, передать ответственность — невозможно.

Итого, только Защитные технологии и Защита данных под ударом — 2 из 6 организационных способностей.

МОНИТОРИНГ

Домен включает в себя 3 организационные способности — Аномалии и События, Непрерывный мониторинг и Процесс мониторинга.

Как математическая задача мониторинг фундаментально слаб перед нейронными сетями, а как в целом рутинная и повторяющаяся задача — перед аутсорсингом.

Все 3 процесса в зоне риска.

РЕАГИРОВАНИЕ

Домен включает в себя 5 организационных способностей — Планирование реагирования, Коммуникации, Анализ, Снижение риска и Улучшения.

В отличие от Мониторинга домен Реагирование требует принятия решений, которые могут прямо повлиять на работоспособность сети организации. Тут в полный рост встает вопрос ответственности с вытекающими сложностью автоматизации и передачи «наружу».

ВОССТАНОВЛЕНИЕ

Домен включает в себя 3 организационные способности — Планирование восстановления, Улучшения и Коммуникации.

Так как реализация всех трех способностей требует детального знания внутренних процессов и политики организации, а также многочасовых переговоров и обсуждений, все 3 организационные способности оказываются вне зоны риска.

Итоговой зоной риска стали технические области внедрения, эксплуатации, поддержки и мониторинга средств защиты информации и мониторинга ИБ. Сейчас такие специалисты востребованы, но фундаментально их позиции уязвимы, поэтому им нужно искать запасной вариант профессионального развития или банально копить деньги — формировать запас, который пригодится в случае реализации пессимистичного сценария. Ведь полноценная профессиональная переподготовка — дело не одного дня или недели, иным специалистам может понадобиться и год.



РКИ-Форум Россия

г. Санкт-Петербург
25–27 сентября 2018 года

www.pki-forum.ru



Встречаемся в Питере!

АВАНГАРД

медиа группа



Организация
мероприятий



Отраслевой
журнал



Интернет-
телекомпания



Книжное
издательство

ib-bank.ru